C/2026/6013

17.11.2026

COMUNICARE A COMISIEI

Orientări ale Comisiei referitoare la aplicarea Regulamentului (UE) 2024/2847 (Regulamentul privind reziliența cibernetică)

(C/2026/6013)

Cuprins

Pagina

1. INTRODUCERE 3
   - 1.1. Regulamentul privind reziliența cibernetică 3
   - 1.2. Scopul prezentelor orientări 3
2. DOMENIUL DE APLICARE 4
   - 2.1. Introducerea pe piață 4
   - 2.2. Software ca produs cu elemente digitale 5
   - 2.3. Codul informatic 6
   - 2.4. Combinație de hardware și software care formează un produs cu elemente digitale 7
   - 2.5. Conexiune de date 8
   - 2.6. Sisteme complexe 8
   - 2.7. Produse cu elemente digitale concepute înainte de intrarea în vigoare a CRA 9
3. SOFTWARE LIBER ȘI CU SURSĂ DESCHISĂ 11
   - 3.1. Stabilirea responsabilității unei persoane pentru un software liber și cu sursă deschisă 12
   - 3.2. Stabilirea plasării unui software liber și cu sursă deschisă pe piața UE 13
     - 3.2.1. Perceperea unui preț 13
     - 3.2.2. Monetizarea altor servicii sau solicitarea prelucrării datelor cu caracter personal 13
     - 3.2.3. Servicii de asistență 14
     - 3.2.4. Donații 15
     - 3.2.5. Finanțarea unui software liber și cu sursă deschisă 15
     - 3.2.6. Entități non-profit înființate pentru a atinge obiective non-profit 16
     - 3.2.7. Integrarea de alți producători 16
   - 3.3. Administratori de software cu sursă deschisă 16
     - 3.3.1. Asistență susținută și asigurarea viabilității FOSS 17
   - 3.4. Contribuitori și utilizări în aval 18
   - 3.5. Scenarii ilustrative 19
4. MODIFICĂRI SUBSTANȚIALE ȘI PIESE DE SCHIMB 21
   - 4.1. Reparații fizice 22
   - 4.2. Piese de schimb 23
   - 4.3. Actualizări de software ca modificări substanțiale 24

4.4. Consecințele unei modificări substanțiale 27
4.4.1. Modificări substanțiale efectuate de o altă persoană decât producătorul de origine 28
4.4.2. Modificări substanțiale efectuate de producătorul de origine 29
5. PERIOADA DE ASISTENȚĂ 29
5.1. Modificări substanțiale și perioada de asistență 31
6. Produse importante și critice cu elemente digitale 32
6.1. Funcționalitatea de bază 33
6.2. Evaluarea conformității pentru produsele importante și critice cu elemente digitale 36
6.3. Implicații pentru prezumția de conformitate 38
7. EVALUAREA RISCURILOR ÎN MATERIE DE SECURITATE CIBERNETICĂ ȘI INTEGRAREA PRODUSELOR CU ELEMENTE DIGITALE ȘI COMPONENTE 41
7.1. În ceea ce privește evaluarea și abordarea riscurilor în materie de securitate cibernetică 41
7.2. În ceea ce privește proiectarea, dezvoltarea și fabricarea de produse cu elemente digitale astfel încât să asigure un nivel adecvat de securitate cibernetică bazat pe riscuri 42
7.3. Evaluarea riscurilor și diligența necesară în ceea ce privește dependențele externe și componentele integrate 42
7.4. Reutilizarea evaluărilor riscurilor și a documentației de conformitate pentru familiile de produse cu elemente digitale 44
8. PRELUCRAREA DATELOR LA DISTANȚĂ 44
8.1. Ce se consideră a fi o soluție de prelucrare a datelor la distanță pentru un produs cu elemente digitale? 45
8.1.1. Noțiunea „la distanță” 46
8.1.2. Absența unei astfel de prelucrări a datelor ar împiedica produsul cu elemente digitale să își îndeplinească vreuna dintre funcții? 46
8.1.3. Software-ul a fost proiectat și dezvoltat de producător sau sub responsabilitatea acestuia? 47
8.2. Implicațiile practice și tehnice ale soluțiilor de prelucrare a datelor la distanță și dependența de soluțiile oferite de terți 49
8.3. Cazuri de utilizare pentru soluții de prelucrare a datelor la distanță 50
8.3.1. Aplicația pentru servicii bancare prin telefonul mobil 51
8.3.2. Termostat inteligent 52
8.3.3. e-Reader 53
8.3.4. Robot industrial 53
8.3.5. Rețeaua celulară 53
9. ELEMENTE SUPLIMENTARE 54
9.1. Obligații de raportare 54
9.2. Gestionarea vulnerabilităților 56
9.2.1. Raportarea în amonte și partajarea soluțiilor de securitate 56
9.2.2. Vulnerabilități exploatabile cunoscute 57
9.2.3. Teste și reexaminări eficace și periodice 58
9.3. Interacțiunea cu alte reglementări 59
9.3.1. Regulamentul (UE) 2019/2144 și Regulamentul (UE) nr. 168/2013 59
9.3.2. Valabilitatea certificatelor de examinare UE de tip [articolul 69 alineatul (1)] 59

1. **INTRODUCERE**

1.1. **Regulamentul privind reziliența cibernetică**

1. Regulamentul (UE) 2024/2847 al Parlamentului European și al Consiliului din 23 octombrie 2024 privind cerințele orizontale în materie de securitate cibernetică pentru produsele cu elemente digitale și de modificare a Regulamentelor (UE) nr. 168/2013 și (UE) 2019/1020, precum și a Directivei (UE) 2020/1828 (Regulamentul privind reziliența cibernetică) ([1]) a intrat în vigoare la 10 decembrie 2024. Regulamentul urmărește să consolideze abordarea Uniunii în materie de securitate cibernetică, să abordeze reziliența cibernetică la nivelul Uniunii și să 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, precum și pe parcursul ciclului de viață al unui produs cu elemente digitale.

2. Regulamentul privind reziliența cibernetică (*Cyber Resilience Act* – CRA) se întemeiază pe noul cadru legislativ al UE (NCL) prevăzut în 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 și în 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 ([2]).

3. Supravegherea pieței și asigurarea respectării legislației sunt realizate de autoritățile naționale de supraveghere a pieței. Produsele cu elemente digitale care fac obiectul domeniului de aplicare al CRA intră sub incidența Regulamentului (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. Comisia și Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) sprijină operatorii economici și statele membre în aplicarea CRA.

1.2. **Scopul prezentelor orientări**

4. Potrivit articolului 26 alineatul (1) din CRA, Comisia publică orientări pentru a ajuta operatorii economici în aplicarea regulamentului, acordând o atenție deosebită facilitării respectării sale de către microîntreprinderi și întreprinderile mici și mijlocii. Articolul 26 alineatul (2) stabilește aspectele minime care ar trebui abordate în orientări. Printre acestea se numără: (i) domeniul de aplicare al CRA (în special soluții de prelucrare a datelor la distanță și software liber și cu sursă deschisă); (ii) noțiunea de „perioade de asistență”; (iii) interacțiunea dintre CRA și alte acte legislative ale UE și (iv) conceptul de „modificare substanțială”.

5. La 3 decembrie 2025, Comisia a publicat o serie de întrebări frecvente (FAQ), menite să ajute operatorii economici să se pregătească pentru punerea în aplicare a CRA ([3]).

6. Prezentele orientări sunt menite să ajute operatorii economici să respecte CRA și să sprijine activitățile autorităților de supraveghere a pieței, ale autorităților de notificare și ale organismelor notificate, cu scopul de a asigura aplicarea armonizată a CRA în întreaga Uniune. Prezentele orientări nu sunt menite să acopere întregul domeniu de aplicare al CRA, ci mai degrabă să ofere clarificări cu privire la justificarea anumitor dispoziții-cheie și la modul în care acestea ar putea fi puse în practică. Prezentele orientări vizează CRA și nu se aplică altor acte legislative ale UE.

([1]) JO L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj.

([2]) Programul de lucru al Comisiei pentru 2026 prevede prezentarea unui „Act legislativ european privind produsele”, care să actualizeze NCL și normele privind supravegherea pieței și standardizarea: https://eur-lex.europa.eu/legal-content/RO/TXT/?uri=CELEX:52025DC0870.

([3]) Întrebările frecvente pot fi descărcate prin intermediul site-ului web al Comisiei privind punerea în aplicare a CRA, de pe pagina web dedicată întrebărilor frecvente.

7. Părțile interesate au fost consultate pe larg în contextul elaborării prezentelor orientări, inclusiv Grupul de experți privind securitatea cibernetică a produselor cu elemente digitale ([4]) și prin intermediul unei consultări publice desfășurate în perioada 3 martie-13 aprilie 2026 ([5]).

8. Prezentele orientări nu au caracter obligatoriu pentru operatorii economici sau pentru alți actori care intră sub incidența CRA. Doar Curtea de Justiție a Uniunii Europene poate să ofere o interpretare cu valoare de autoritate a Regulamentului privind reziliența cibernetică. Cu toate acestea, prezentele orientări stabilesc interpretarea pe care Comisia o dă CRA, cu scopul de a sprijini conformitatea și de a contribui la punerea în aplicare efectivă a regulamentului. În plus, orientările conțin o serie de exemple pentru a ilustra aplicarea unor dispoziții specifice. Totuși, aceste exemple nu sunt menite să înlocuiască o evaluare de la caz la caz, care va fi întotdeauna necesară pentru a ține seama de particularitățile fiecărui caz în parte.

9. În conformitate cu articolul 26 din CRA, Comisia poate lua în considerare emiterea de orientări suplimentare, inclusiv orientări destinate producătorilor cărora li se aplică CRA și alte acte legislative de armonizare ale Uniunii sau alte acte juridice conexe ale Uniunii. Aceste orientări pot aborda, de exemplu, aspecte privind interacțiunea dintre CRA și Regulamentul (UE) 2024/1689 de stabilire a unor norme armonizate privind inteligența artificială (Regulamentul privind IA) și Regulamentul (UE) 2022/2554 privind reziliența operațională digitală a sectorului financiar (DORA).

2. **DOMENIUL DE APLICARE**

2.1. **Introducerea pe piață**

10. CRA se aplică produselor cu elemente digitale care sunt puse la dispoziție pe piața UE. Conceptul de punere la dispoziție pe piață este definit la articolul 3 punctul 22 din CRA ca fiind „furnizarea unui produs cu elemente digitale pentru distribuție sau utilizare pe piața Uniunii, în cadrul unei activități comerciale, contra cost sau gratuit”. În conformitate cu articolul 3 punctul 21, un produs cu elemente digitale este introdus pe piața UE atunci când este pus la dispoziție pentru prima dată.

11. Cea mai recentă ediție a „Ghidului albastru referitor la punerea în aplicare a normelor UE privind produsele”, publicat în 2022 (denumit în continuare „Ghidul albastru”) ([6]), oferă orientări care facilitează înțelegerea normelor UE privind produsele și aplicarea lor uniformă în diferitele cadre juridice sectoriale aliniate la noul cadru legislativ (NCL), cum ar fi CRA. În conformitate cu Ghidul albastru, conceptele de „introducere pe piață” și de „punere la dispoziție” trebuie înțelese ca aplicându-se „fiecărui produs individual și nu unui tip de produs, indiferent dacă acesta a fost fabricat ca o unitate individuală sau în serie (secțiunea 2.3).

12. Pentru produsele mai „tradiționale” cu elemente digitale care fac obiectul NCL, cum ar fi hardware-ul sub formă de produse asimilate mașinilor sau de echipamente radio cu elemente digitale, conceptul de „introducere pe piață” este bine stabilit, iar Ghidul albastru oferă orientări suplimentare pentru a clarifica situațiile în care astfel de produse sunt considerate a fi introduse pe piață. „Exemplele sintetizate” cuprinse în secțiunea 2.12 din Ghidul albastru oferă exemple suplimentare ale conceptului de „introducere pe piață”.

13. Cu toate acestea, având în vedere natura produselor necorporale cu elemente digitale, cum ar fi software-ul de sine stătător, sunt necesare orientări suplimentare cu privire la momentul în care astfel de produse cu elemente digitale sunt considerate introduse pe piață. Odată ce etapa de fabricație a software-ului este finalizată, iar produsul cu elemente digitale este oferit potențialilor utilizatori de pe piața UE, se poate considera că producătorul său a fabricat mai multe copii ale aceluiași produs software cu elemente digitale și le-a furnizat în vederea distribuției sau utilizării. În fapt, spre deosebire de produsele tangibile cu elemente digitale, software-ul de sine stătător nu face

([4]) Grupul de experți privind securitatea cibernetică a produselor cu elemente digitale înscris în registrul grupurilor de experți al Comisiei și al altor entități similare.
([5]) Consultare publică privind proiectul de orientări ale Comisiei referitoare la Regulamentul privind reziliența cibernetică.
([6]) Comunicare a Comisiei „Ghidul albastru” din 2022 referitor la punerea în aplicare a normelor UE privind produsele 2022/C 247/01 (JO C 247, 29.6.2022, p. 1).

obiectul unor limitări ale producției fizice sau ale stocurilor: fiecare acțiune de punere la dispoziție a software-ului pentru descărcare sau distribuție are ca rezultat crearea unei noi copii identice pentru utilizator. Atât timp cât această versiune a software-ului nu este modificată într-un mod care afectează conformitatea cu CRA, se consideră că introducerea pe piața UE a avut loc în momentul primei oferte pentru distribuție sau utilizare. Prin urmare, posibilitatea descărcării sau a distribuirii ulterioare a acestei versiuni a produsului software cu elemente digitale trebuie considerată un caz în care acest produs software cu elemente digitale este pus la dispoziție ([7]).

14. Prin urmare, ar trebui să se considere că un produs software de sine stătător cu elemente digitale a fost introdus pe piață odată ce etapa de fabricație este finalizată și software-ul respectiv este furnizat pentru prima dată în vederea distribuției sau utilizării pe piața UE în cadrul unei activități comerciale. Ar trebui să se considere că producătorul a introdus pe piață mai multe copii ale aceluiași produs software cu elemente digitale în același timp. Prin urmare, deși mai multe copii ale aceluiași software rămân produse individuale cu elemente digitale, acestea sunt considerate a fi introduse pe piață în același timp, indiferent de momentul în care deținerea sau utilizarea fiecărei copii individuale este transferată unei alte persoane fizice sau juridice. În același timp, în cazul în care producătorul pune la dispoziție software în diverse variante care diferă în ceea ce privește componentele incluse, configurațiile sau funcționalitățile activate (de exemplu, dezvoltă sisteme de operare diferite sau pachete cu seturi de caracteristici diferite), aceste variante nu pot fi considerate copii multiple ale aceluiași produs software cu elemente digitale. Prin urmare, acestea ar trebui tratate ca produse distincte cu elemente digitale în scopul introducerii pe piață.

Exemplul 1: La 1 ianuarie 2028, societatea A efectuează primele livrări în vederea distribuirii prin intermediul site-ului său internet a versiunii 1.0.0 a software-ului său X. În aceeași zi, clientul 1 achiziționează o copie a versiunii 1.0.0 a software-ului X. La 15 ianuarie 2028, clientul 2 achiziționează o copie a versiunii 1.0.0 a software-ului X. Ambele copii ale versiunii 1.0.0 a software-ului X sunt introduse pe piață la 1 ianuarie 2028.

15. Având în vedere caracterul iterativ al dezvoltării de software, ar trebui clarificat în continuare faptul că iterațiile ulterioare ale unui produs software cu elemente digitale sunt considerate a fi nou introduse pe piață atunci când iterațiile respective se califică drept „modificare substanțială” a unui produs software cu elemente digitale deja introdus pe piață, astfel cum se indică la considerentul 41 din CRA. Iterațiile care nu se califică drept modificări substanțiale nu impun producătorului să efectueze o nouă procedură de evaluare a conformității și, prin urmare, nu modifică data introducerii pe piață a software-ului respectiv. Pentru mai multe informații privind conceptul de modificări substanțiale, a se vedea secțiunea *4 Modificări substanțiale*.

Exemplul 2: La 1 ianuarie 2028, societatea A efectuează primele livrări în vederea distribuirii prin intermediul site-ului său internet a versiunii 1.0.0 a software-ului X. În aceeași zi, clientul 1 achiziționează o copie a versiunii 1.0.0 a software-ului X. La 15 ianuarie 2028, societatea A emite o versiune actualizată 1.0.1 a software-ului X care nu constituie o modificare substanțială. La 30 ianuarie 2028, clientul 2 achiziționează o copie a versiunii 1.0.1 a software-ului X. Ambele copii ale versiunilor 1.0.0 și 1.0.1 ale software-ului X sunt considerate a fi introduse pe piață la 1 ianuarie 2028.

16. Orientările prevăzute la punctele 13, 14 și 15 se aplică exclusiv în măsura în care produsul cu elemente digitale este un software de sine stătător. Acestea nu se aplică, de exemplu, atunci când software-ul este combinat cu hardware, astfel cum se discută în secțiunea *2.4 Combinație de hardware și software care formează un produs*.

2.2. **Software ca produs cu elemente digitale**

17. Articolul 3 punctul 1 din CRA definește un produs cu elemente digitale ca fiind „un produs software sau hardware și soluțiile sale de prelucrare de date la distanță, inclusiv componentele software sau hardware introduse pe piață separat”. Astfel de produse cu elemente digitale intră în domeniul de aplicare al CRA în cazul în care scopul lor preconizat sau utilizarea lor previzibilă în mod rezonabil include o conexiune de date logică sau fizică directă sau indirectă la un dispozitiv sau la o rețea.

([7]) În conformitate cu articolul 13 alineatul (11), producătorii pot întreține arhive software publice care să îmbunătățească accesul utilizatorilor la versiunile istorice. În astfel de cazuri, utilizatorii sunt informați într-un mod clar și ușor accesibil, cu privire la riscurile asociate utilizării software-ului care nu beneficiază de asistență.

18. Prin urmare, CRA poate viza o serie de produse cu elemente digitale, printre acestea: (i) software de sine stătător, cum ar fi aplicațiile și programele informatice, indiferent dacă sunt distribuite digital sau fizic; (ii) hardware cu software încorporat (de exemplu, dispozitive, laptopuri, tablete pentru internetul obiectelor); (iii) hardware de sine stătător (de exemplu, circuite integrate, plăci de bază) și (iv) orice combinație de hardware și software furnizate separat, dar destinate să funcționeze împreună.

19. Prin urmare, software-ul de sine stătător intră în domeniul de aplicare al CRA în cazul în care este introdus pe piață ca produs cu elemente digitale. Este util să se facă distincția între produsele software cu elemente digitale care fac obiectul CRA și furnizarea la distanță de servicii care nu intră în domeniul de aplicare al CRA.

20. Pentru ca un software să intre în domeniul de aplicare al CRA, un produs software cu elemente digitale trebuie să fie furnizat unui utilizator, obținut de utilizatorul respectiv și utilizat în cadrul sau ca parte a unui sistem electronic de informații din partea utilizatorului. Software-ul care este descărcat, instalat sau furnizat în alt mod utilizatorului și care execută pe sistemul electronic de informații al utilizatorului îndeplinește aceste criterii, inclusiv, de exemplu, în cazul în care ia forma unei extensii a browserului sau a unei aplicații dezvoltate utilizând tehnologii web, dar furnizate pentru execuție locală.

21. În schimb, software-ul care execută de la distanță și care este doar accesat de utilizator nu este, doar pe această bază, un produs cu elemente digitale. În fapt, considerentele 11 și 12 din CRA fac această distincție, explicând că prelucrarea sau stocarea la distanță intră sub incidența CRA numai în măsura în care este necesar ca un produs cu elemente digitale să își îndeplinească funcțiile (și anume prin conceptul de prelucrare de date la distanță, astfel cum este definit la articolul 3 punctul 2), și nu în sine ca produs cu elemente digitale. Acesta este, de regulă, cazul aplicațiilor web, inclusiv al aplicațiilor web progresive, în cazul cărora acestea sunt accesate exclusiv prin intermediul unui browser web. Același lucru este valabil și pentru site-urile web: deși site-urile web pot, într-o măsură limitată, să funcționeze și să execute din punct de vedere tehnic pe dispozitivul utilizatorului, din considerentul 12 din CRA reiese că site-urile web nu trebuie considerate ele însele produse cu elemente digitale și intră în domeniul de aplicare al CRA numai în cazul în care sprijină funcționalitatea unui produs cu elemente digitale, și anume în măsura în care se califică drept prelucrare de date la distanță (astfel cum se explică în continuare în secțiunea *8* și, în special, *8.1.2 Absența unei astfel de prelucrări a datelor ar împiedica produsul cu elemente digitale să își îndeplinească vreuna dintre funcții?*).

Exemplul 3: o aplicație mobilă pe care un utilizator o descarcă dintr-un magazin de aplicații și o instalează pe telefonul său inteligent este furnizată utilizatorului și este executată pe dispozitivul utilizatorului și, prin urmare, este un produs cu elemente digitale. În cazul în care este introdusă pe piață în cadrul unei activități comerciale, aceasta poate intra în domeniul de aplicare al CRA.

Exemplul 4: o aplicație desktop construită utilizând tehnologii web, dar destinată unei instalări locale, este furnizată utilizatorului și se execută pe dispozitivul utilizatorului și, prin urmare, este un produs cu elemente digitale. În cazul în care este introdusă pe piață în cadrul unei activități comerciale, aceasta poate intra în domeniul de aplicare al CRA.

Exemplul 5: o aplicație web accesată de utilizator exclusiv prin intermediul unui browser web nu este un produs cu elemente digitale. Cu excepția cazului în care sprijină funcționalitatea unui produs cu elemente digitale, aceasta nu intră în domeniul de aplicare al CRA. În schimb, o aplicație furnizată utilizatorului în calitate de client instalat local care execută pe dispozitivul utilizatorului este un produs cu elemente digitale. În cazul în care este introdusă pe piață în cadrul unei activități comerciale, aceasta poate intra în domeniul de aplicare al CRA.

În cazul în care clientul respectiv se bazează, pentru a îndeplini una sau mai multe dintre funcțiile sale, pe o prelucrare de date la distanță care se încadrează în definiția prelucrării de date la distanță, această prelucrare de date la distanță face parte, de asemenea, din produsul cu elemente digitale.

Exemplul 6: un site internet care doar prezintă informații vizitatorilor săi și nu sprijină funcționalitatea unui produs cu elemente digitale nu este în sine un produs cu elemente digitale. Prin urmare, acesta nu intră în domeniul de aplicare al CRA.

2.3. **Codul informatic**

22. De asemenea, este util să se clarifice dacă, în ceea ce privește codul sursă, acesta poate constitui un produs software cu elemente digitale. CRA definește software-ul ca fiind „acea parte a unui sistem informatic electronic care constă într-un cod informatic” (articolul 3 punctul 4). Codul informatic poate lua forma (i) codului mașină, care este setul de instrucțiuni executate direct de procesorul computerului, scris în format binar; sau a (ii) codului sursă, adică setul de instrucțiuni și declarații scrise într-un limbaj de programare, care trebuie compilate sau interpretate pentru a fi executate de un calculator. Definiția software-ului prevăzută în CRA le acoperă pe ambele.

23. O întrebare separată este dacă o anumită furnizare de coduri informatice echivalează cu introducerea unui produs cu elemente digitale pe piața UE, ceea ce necesită furnizarea în cadrul unei activități comerciale. Adesea, este posibil ca acest fapt să nu fie valabil pentru codul sursă. De exemplu, o persoană fizică sau juridică ce partajează un cod informatic gratuit și cu sursă deschisă în depozite accesibile publicului nu este, în general, considerată a introduce codul respectiv pe piața UE în scopul CRA (astfel cum se discută mai detaliat în secțiunea *3 Software liber și cu sursă deschisă*). De asemenea, codul nefinalizat partajat în faza de proiectare și dezvoltare a unui produs cu elemente digitale (de exemplu, pentru testare sau reexaminare) nu este considerat a fi introdus pe piață în scopul CRA, deoarece faza sa de fabricație nu este finalizată. În mod similar, nici eșantionul sau codul demo furnizat ca parte a tutorialelor sau a materialelor de formare nu este considerat a fi introdus pe piață în scopul CRA ([8]).

24. Pe de altă parte, atunci când un producător furnizează clienților săi un cod informatic ca produs cu elemente digitale, acest cod este considerat a fi introdus pe piață, indiferent dacă este vorba despre codul mașină sau despre codul sursă ([9]).

Exemplul 7: Societatea A acordă societății B licența de cod sursă pentru o platformă internă personalizabilă și furnizează acest cod sursă într-un fișier text. Chiar dacă acest cod sursă necesită adaptări și compilări suplimentare din partea societății B înainte de a fi utilizat, societatea A introduce acest cod sursă pe piață și, prin urmare, face obiectul CRA. Societatea A nu este responsabilă pentru respectarea CRA a adaptărilor ulterioare și a compilării codului respectiv de către societatea B.

2.4. **Combinație de hardware și software care formează un produs cu elemente digitale**

25. Faptul că software-ul face parte dintr-un produs cu elemente digitale nu ar trebui să fie determinat de modul sau de momentul în care software-ul respectiv este livrat utilizatorului, ci de faptul dacă, având în vedere scopul preconizat al produsului și utilizarea previzibilă în mod rezonabil, software-ul este necesar pentru ca produsul cu elemente digitale să își îndeplinească funcțiile preconizate. În cazul în care un produs hardware cu elemente digitale este conceput să funcționeze împreună cu un software specific furnizat de același producător pentru a-și îndeplini funcțiile, hardware-ul și software-ul respectiv constituie împreună produsul cu elemente digitale. Software-ul necesar pentru operarea, configurarea, controlul sau utilizarea unui produs cu elemente digitale în conformitate cu scopul său preconizat face parte, prin urmare, din produsul cu elemente digitale, chiar dacă este obținut printr-un canal separat (de exemplu, un magazin de aplicații, un link de descărcare sau un alt canal digital după introducerea pe piață a produsului hardware cu elemente digitale). Prin urmare, introducerea sa pe piață are loc în același moment în care unitățile produselor hardware cu elemente digitale sunt introduse pe piață.

Exemplul 8: O imprimantă de rețea este introdusă pe piață ca produs hardware cu elemente digitale, în timp ce driverele de software care trebuie să trimită comenzi de imprimare, să configureze dispozitivul și să gestioneze funcționarea acestuia sunt puse la dispoziție pentru descărcare de pe site-ul producătorului. Deși imprimanta și driverele sunt furnizate prin canale diferite, acestea constituie împreună un singur produs cu elemente digitale, deoarece imprimanta nu își poate îndeplini scopul preconizat fără drivere.

Exemplul 9: Un dispozitiv purtabil pentru monitorizarea condiției fizice este introdus pe piață pentru a măsura frecvența cardiacă și activitatea unui utilizator, în timp ce o aplicație pentru telefoane inteligente furnizată de producător este necesară pentru a afișa măsurătorile, a prezenta istoricul și a permite configurația dispozitivului. Deși aplicația este descărcată separat prin intermediul unui magazin de aplicații, dispozitivul purtabil și aplicația constituie împreună un singur produs cu elemente digitale, deoarece sunt concepute și destinate să funcționeze împreună pentru a asigura funcționalitatea produsului cu elemente digitale.

([8]) De asemenea, ar trebui reamintit faptul că articolul 4 alineatul (3) permite producătorilor să pună la dispoziție pe piață un software nefinalizat care nu este conform cu regulamentul, cum ar fi versiunile alfa, beta sau aplicațiile candidate la lansare, cu condiția ca software-ul nefinalizat să fie pus la dispoziție numai pentru perioada necesară pentru a-l testa și pentru a primi feedback.

([9]) Pe de altă parte, ar trebui remarcat faptul că, în sensul legislației privind răspunderea pentru produsele cu defecte, codul informatic în sine nu constituie un produs și, prin urmare, producătorii care introduc un astfel de cod pe piață nu pot fi considerați răspunzători în temeiul Directivei (UE) 2024/2853 (Directiva privind răspunderea pentru produsele cu defecte). Considerentul 13 din directiva menționată prevede că „[c]u toate acestea, informațiile nu trebuie considerate produse și, prin urmare, normele privind răspunderea pentru produsele cu defecte nu ar trebui să se aplice conținutului fișierelor digitale, cum ar fi fișierele media sau cărțile electronice ori simplul cod sursă al software-ului”. Acest aspect nu exclude posibilitatea ca producătorii să fie răspunzători în temeiul legislației naționale în domeniul răspunderii civile.

2.5. **Conexiune de date**

26. Potrivit articolului 2 alineatul (1), CRA „se aplică produselor cu elemente digitale puse la dispoziție pe piață al căror scop preconizat sau a căror utilizare previzibilă în mod rezonabil include o conexiune de date logică sau fizică directă sau indirectă la un dispozitiv sau la o rețea”. Prin urmare, domeniul de aplicare al CRA nu este ancorat în simpla prezență a produselor electronice, ci în capacitatea unui produs cu elemente digitale de a face schimb de informații digitale.

27. Deși termenii „conexiune logică” și „conexiune fizică” sunt definiți la articolul 3, CRA nu definește termenii „conexiune de date” sau „date digitale”. Prin urmare, este util să se stabilească o interpretare a ceea ce este o conexiune de date, pentru a clarifica limitele domeniului de aplicare al CRA. Această limită este deosebit de importantă pentru a distinge produsele cu elemente digitale care utilizează doar semnale electrice de cele care participă la comunicarea digitală și, prin urmare, sunt expuse riscurilor de securitate cibernetică.

28. La nivelul său cel mai elementar, o conexiune de date implică transmiterea de informații în format binar, și anume într-o secvență de 0 și 1. Simpla activare și dezactivare a unei ieșiri (și anume 0/1) nu constituie în sine o conexiune de date dacă aceste stări nu sunt destinate să reprezinte date sau nu sunt citite de o intrare numerică. Pentru a exista o conexiune de date, stările binare trebuie să fie codificate în mod deliberat ca informații de către o sursă și trebuie să poată fi decodate ca informații la destinație. Cu alte cuvinte, trebuie să existe un expeditor care generează în mod deliberat simboluri digitale în conformitate cu un sistem definit și un receptor capabil să interpreteze aceste simboluri ca date. În cazul în care semnalele electrice sau electronice sunt utilizate exclusiv pentru a declanșa sau a alimenta o funcție, fără a transmite informații codificate digital, nu există nicio conexiune de date în scopul CRA și, prin urmare, produsul cu elemente digitale nu intră în domeniul de aplicare al articolului 2 alineatul (1).

2.6. **Sisteme complexe**

29. Produsele cu elemente digitale care intră în domeniul de aplicare al CRA pot consta nu numai în dispozitive unice sau componente software, ci și în sisteme complexe, inclusiv sisteme compuse din mai multe elemente hardware și software care funcționează împreună pentru a îndeplini o anumită funcție. În cazul în care un astfel de sistem este introdus pe piață ca produs unic cu elemente digitale, acesta constituie un produs cu elemente digitale în înțelesul CRA.

30. Astfel de sisteme complexe sunt adesea caracterizate de cicluri lungi de proiectare și dezvoltare, cu contracte care este posibil să fi fost semnate înainte de aplicarea CRA, durate de viață operaționale prelungite și un grad ridicat de complexitate tehnică și organizațională. Astfel de sisteme, care urmează să fie introduse pe piață după intrarea în vigoare a CRA, se pot baza pe componente introduse pe piață înainte de intrarea în vigoare a CRA, pe arhitecturi consacrate sau pe standarde de interoperabilitate utilizate pe scară largă, inclusiv pe standardele menționate în alte acte legislative ale UE sau în cadrele sectoriale. Prin urmare, anumite caracteristici tehnice ale sistemelor respective pot fi dificil sau disproporționat de modificat fără a afecta scopul preconizat, siguranța, fiabilitatea sau interoperabilitatea acestora cu infrastructura existentă.

31. Aceste caracteristici nu exclud, în sine, sistemele complexe din domeniul de aplicare al CRA. Mai degrabă, acestea ilustrează aplicarea abordării bazate pe riscuri a CRA, care permite demonstrarea conformității în moduri diferite, în funcție de caracteristicile și constrângerile produsului cu elemente digitale, în conformitate cu articolul 13 alineatul (3) din CRA. Aceste caracteristici fac parte din scopul preconizat și din contextul operațional și, prin urmare, sunt relevante atunci când se evaluează conformitatea cu cerințele esențiale de securitate cibernetică (denumite în continuare „cerințele esențiale”). În special, considerentul 55 recunoaște în mod explicit că este posibil ca anumite cerințe esențiale să nu fie pe deplin compatibile cu natura unui produs cu elemente digitale. De exemplu, acest lucru se poate întâmpla în cazul în care conformitatea ar submina cerințele obligatorii de interoperabilitate sau buna funcționare a sistemului.

32. În consecință, producătorii au obligația de a aborda riscurile în materie de securitate cibernetică pe baza evaluării riscurilor în materie de securitate cibernetică menționate la articolul 13 alineatul (2). Astfel cum se explică, de asemenea, la considerentul 55, în unele cazuri, cerințele esențiale specifice nu sunt aplicabile sau nu pot fi

îndeplinite prin punerea în aplicare a unor măsuri de securitate de ultimă generație din cauza, de exemplu, a scopului preconizat al sistemului, care impune ca produsul cu elemente digitale să interacționeze cu dependențele existente sau să respecte anumite cerințe de interoperabilitate. În astfel de cazuri, producătorii ar trebui să identifice și să documenteze aceste constrângeri specifice, să evalueze riscurile asociate și să pună în aplicare măsuri alternative sau compensatorii adecvate de atenuare a riscurilor, astfel încât să nu submineze securitatea produsului cu elemente digitale. În acest scop, atât documentația tehnică menționată la articolul 31, cât și informațiile și instrucțiunile pentru utilizator menționate în anexa II joacă un rol esențial în descrierea transparentă a constrângerilor identificate, a riscurilor de securitate cibernetică asociate și a măsurilor de atenuare a riscurilor puse în aplicare. În conformitate cu obligația de a actualiza evaluarea riscurilor în cursul perioadei de sprijin, producătorii ar trebui, de asemenea, să reevalueze periodic dacă astfel de constrângeri continuă să existe. În cazul în care astfel de constrângeri pot fi eliminate sau reduse în timp, producătorii ar trebui să actualizeze produsul cu elemente digitale în consecință, astfel încât acesta să poată evolua către un nivel adecvat de securitate cibernetică ([10]).

Exemplul 10: Un producător introduce pe piață un produs cu elemente digitale care comunică cu sistemele externe utilizând un protocol de rețea. În contextul aplicării cerințelor esențiale, producătorul stabilește, pe baza evaluării riscurilor în materie de securitate cibernetică, că utilizarea unui protocol de comunicare securizat este necesară pentru a asigura confidențialitatea și integritatea datelor care fac obiectul schimbului de către produsul cu elemente digitale.

Cu toate acestea, scopul său preconizat include interoperabilitatea cu sistemele existente care permit doar un protocol mai vechi sau mai puțin sigur. În astfel de cazuri, producătorul poate pune în aplicare protocolul respectiv atunci când acest lucru este necesar pentru realizarea interoperabilității, cu condiția ca riscurile în materie de securitate cibernetică asociate să fie identificate și atenuate prin alte mijloace.

În cazul în care este fezabil din punct de vedere tehnic ca produsul cu elemente digitale să suporte atât protocolul securizat, cât și protocolul mai puțin securizat, se preconizează că producătorul va pune în aplicare protocolul securizat și va permite utilizarea implicită a acestuia. Protocolul mai puțin securizat ar fi permis numai în cazul în care este necesar pentru interoperabilitate.

Exemplul 11: Un producător al unui sistem de automatizare industrială achiziționează unele microcontrolere înainte de intrarea în vigoare a CRA. Producătorul efectuează evaluarea riscurilor în materie de securitate cibernetică pentru sistemul său de automatizare industrială care urmează să fie introdus pe piață după intrarea în vigoare a CRA. Pe baza respectivei evaluări a riscurilor în materie de securitate cibernetică, producătorul nu identifică riscuri specifice în materie de securitate cibernetică asociate cu utilizarea unuia dintre aceste microcontrolere. Producătorul îl integrează în sistemul său de automatizare industrială și se asigură că produsul cu elemente digitale în ansamblu (sistemul de automatizare industrială) îndeplinește cerințele esențiale.

2.7. **Produse cu elemente digitale concepute înainte de intrarea în vigoare a CRA**

33. În unele cazuri, un producător va introduce pe piață, după intrarea în vigoare a CRA la 11 decembrie 2027, unități ale unui produs cu elemente digitale fabricate în conformitate cu un tip sau model proiectat și dezvoltat înainte de data aplicării CRA. În astfel de cazuri, conformitatea cu prezentul regulament nu impune neapărat ca unitățile respective ale produsului cu elemente digitale să fie reproiectate. Producătorul trebuie să efectueze o evaluare a riscurilor în materie de securitate cibernetică în conformitate cu articolul 13 alineatul (2) din CRA pentru a stabili, pe baza scopului preconizat și a utilizării previzibile în mod rezonabil a produsului cu elemente digitale, care dintre cerințele esențiale prevăzute în anexa I partea I sunt aplicabile produsului cu elemente digitale respectiv și modul în care sunt puse în aplicare cerințele respective.

34. În cazul în care rezultatul respectivei evaluări a riscurilor demonstrează că produsul cu elemente digitale include deja măsuri de securitate adecvate și eficace care abordează riscurile relevante, producătorul se poate baza pe măsurile existente respective pentru a demonstra conformitatea cu CRA. CRA nu impune, în sine, obligația de a introduce noi elemente de securitate sau de a reproiecta produsul cu elemente digitale în cazul în care acest lucru nu este necesar pentru a aborda riscurile identificate.

([10]) Ar trebui remarcat faptul că, după caz, considerațiile prevăzute la prezentul alineat pot fi aplicabile tuturor produselor cu elemente digitale care intră în domeniul de aplicare al CRA, și nu doar „sistemelor complexe”.

35. Cu toate acestea, producătorul intră în continuare sub incidența obligațiilor prevăzute în CRA. Printre acestea se numără asigurarea, înainte ca produsul cu elemente digitale să fie introdus pe piață, a faptului că procedura aplicabilă de evaluare a conformității a fost efectuată, că declarația de conformitate UE a fost întocmită și că marcajul CE a fost aplicat. Conformitatea cu aceste cerințe este independentă de necesitatea modificării proiectării produsului cu elemente digitale ca urmare a evaluării riscurilor. În cazul produselor cu elemente digitale proiectate înainte de data aplicării CRA, dar introduse pe piață după această dată, atunci când producătorul nu poate demonstra modul în care evaluarea riscurilor a fost avută în vedere în faza de proiectare și dezvoltare a produsului cu elemente digitale, obligația prevăzută la articolul 13 alineatul (2) ar trebui înțeleasă ca impunând producătorilor să efectueze o evaluare a riscurilor în materie de securitate cibernetică și să demonstreze, pe această bază, că produsul cu elemente digitale încorporează măsuri de securitate adecvate în vederea reducerii la minimum a riscurilor de securitate cibernetică, a prevenirii incidentelor și a reducerii la minimum a impactului acestora, inclusiv în ceea ce privește sănătatea și siguranța utilizatorilor.

36. În consecință, produsele cu elemente digitale proiectate înainte de intrarea în vigoare a CRA ar putea fi introduse pe piață în temeiul CRA fără reproiectare, cu condiția ca producătorul să poată demonstra, prin evaluarea riscurilor în materie de securitate cibernetică și prin documentația tehnică, că produsul cu elemente digitale atinge un nivel adecvat de securitate cibernetică având în vedere scopul său preconizat și utilizarea sa previzibilă în mod rezonabil și respectă cerințele esențiale de securitate cibernetică.

37. În plus, este util să se clarifice aplicarea obligațiilor de evaluare a conformității pentru producătorii de produse cu elemente digitale care sunt introduse pe piață după intrarea în vigoare a CRA, dar sunt fabricate în conformitate cu un tip sau model proiectat și dezvoltat înainte de data respectivă. În conformitate cu articolul 13 alineatul (12), producătorul trebuie să demonstreze, prin intermediul procedurii relevante de evaluare a conformității, că produsul său cu elemente digitale este conform cu cerințele esențiale aplicabile și să includă dovezi în acest sens în documentația tehnică a produsului (punctul 6 din anexa VII).

38. Cu toate acestea, aplicarea unor astfel de cerințe trebuie interpretată în lumina evaluării riscurilor în materie de securitate cibernetică și a profilului de risc în materie de securitate cibernetică al produsului cu elemente digitale. În special în cazul produselor cu elemente digitale proiectate înainte de data aplicării CRA (dar introduse pe piață după data respectivă) și care fac obiectul procedurilor de evaluare a conformității prevăzute la articolul 32 alineatul (1), în cazul în care evaluarea riscurilor demonstrează că produsul cu elemente digitale încorporează deja măsuri de securitate adecvate și eficace care abordează riscurile produsului respectiv, obligația de a furniza dovezi în cadrul procedurii de evaluare a conformității nu ar trebui înțeleasă ca impunând producătorului să furnizeze rezultate ale testelor care să acopere etapele inițiale de proiectare și dezvoltare ale unor astfel de produse cu elemente digitale. Acest fapt nu ar fi necesar, deoarece nu ar contribui la creșterea securității produsului cu elemente digitale în sine. În cazul în care testele pot fi totuși necesare, producătorii nu trebuie să furnizeze dovezi ale testelor efectuate asupra tuturor variantelor de produs, ci pot grupa astfel de teste pe familii de produse cu elemente digitale, astfel cum se discută în continuare în secțiunea *7.4 Reutilizarea evaluărilor riscurilor și a documentației de conformitate pentru familiile de produse cu elemente digitale*.

39. Cu toate acestea, producătorul ar trebui să furnizeze dovezi cu privire la modul în care respectă procesele de gestionare a vulnerabilităților prevăzute în anexa I partea II, ar trebui să își actualizeze evaluarea riscurilor în conformitate cu articolul 13 alineatul (3), precum și să îndeplinească toate celelalte obligații prevăzute în CRA, inclusiv prin furnizarea de informații și instrucțiuni utilizatorilor în conformitate cu articolul 13 alineatul (18).

Exemplul 12: Un producător introduce pe piață un microcontroler care a fost proiectat și dezvoltat înainte de data aplicării CRA. Microcontrolerul este destinat să fie integrat într-o serie de produse electronice cu elemente digitale, inclusiv produse cu elemente digitale cu funcționalități de conectivitate.

Înainte de a introduce pe piață noi unități ale microcontrolerului după aplicarea CRA, producătorul efectuează o evaluare a riscurilor în materie de securitate cibernetică în conformitate cu articolul 13 alineatul (2). Pe baza scopului preconizat al microcontrolerului și a utilizării sale previzibile în mod rezonabil, producătorul identifică riscurile relevante în materie de securitate cibernetică, cum ar fi accesul neautorizat, manipularea software-ului sau a datelor și utilizarea abuzivă a interfețelor disponibile.

Rezultatul evaluării riscurilor arată că microcontrolerul, astfel cum a fost conceput inițial, include deja măsuri de securitate adecvate și eficace care abordează riscurile identificate. Prin urmare, producătorul concluzionează că produsul cu elemente digitale îndeplinește cerințele esențiale relevante prevăzute în anexa I partea I și că nu este necesară reproiectarea sau introducerea unor funcționalități de securitate suplimentare.

În cazul în care nu este posibil să se demonstreze modul în care o evaluare a riscurilor în materie de securitate cibernetică a fost luată în considerare în faza inițială de proiectare și dezvoltare, producătorul documentează o evaluare actuală a riscurilor în materie de securitate cibernetică și explică modul în care proiectarea și măsurile existente atenuează riscurile identificate. Producătorul nu este obligat să recreeze documentația istorică de proiectare sau de testare, deoarece aceasta nu ar contribui la îmbunătățirea securității cibernetice a produsului cu elemente digitale. În cazul în care mai multe variante ale microcontrolerului se bazează pe același model și au același profil de risc în materie de securitate cibernetică, producătorul se poate baza, de asemenea, pe dovezi reprezentative care acoperă familia de produse relevantă.

Producătorul asigură, de asemenea, respectarea cerințelor de gestionare a vulnerabilităților prevăzute în anexa I partea II, inclusiv prin menținerea proceselor de abordare și remediere a vulnerabilităților și prin reexaminarea evaluării riscurilor în materie de securitate cibernetică în conformitate cu articolul 13 alineatul (3).

În aceste circumstanțe, microcontrolerul proiectat înainte de data aplicării CRA poate fi introdus pe piață fără reproiectare, cu condiția ca producătorul să poată demonstra, prin evaluarea riscurilor în materie de securitate cibernetică și prin documentația tehnică, că atinge un nivel adecvat de securitate cibernetică având în vedere scopul său preconizat și utilizarea sa previzibilă în mod rezonabil și că respectă cerințele esențiale aplicabile.

3. **SOFTWARE LIBER ȘI CU SURSĂ DESCHISĂ**

40. Astfel cum s-a reamintit în secțiunea *2.1 Introducerea pe piață*, CRA se aplică produselor cu elemente digitale care sunt puse la dispoziție pe piața UE în cadrul unei activități comerciale pentru prima dată (și anume „introduse pe piață"), precum și oricărui caz ulterior care constituie punerea la dispoziție pe piață a aceluiași produs cu elemente digitale. Ghidul albastru (secțiunea 2.2) clarifică faptul că prin „activitate comercială" se înțelege furnizarea de bunuri, contra cost sau gratuit, într-un context comercial și nu poate fi evaluată decât pentru fiecare caz în parte, ținând cont de regularitatea furnizărilor, de caracteristicile produsului, de intențiile furnizorului etc.

41. Furnizarea în cadrul unei activități comerciale se caracterizează printr-o serie de circumstanțe, documentate pe larg în Ghidul albastru și reamintite la considerentul 15 din CRA. Acestea pot include perceperea directă a unui preț, precum și „perceperea unui preț pentru serviciile de asistență tehnică, în cazul în care acestea nu servesc doar la recuperarea costurilor reale, prin intenția de monetizare, de exemplu prin furnizarea unei platforme software prin intermediul căreia producătorul monetizează alte servicii, prin impunerea ca o condiție de utilizare a prelucrării datelor cu caracter personal din alte motive decât exclusiv pentru îmbunătățirea securității, compatibilității sau interoperabilității software-ului, sau prin acceptarea unor donații care depășesc costurile asociate cu proiectarea, dezvoltarea și furnizarea unui produs cu elemente digitale" (considerentul 15) ([11]).

42. Cu toate acestea, CRA recunoaște particularitățile diferitelor modalități de dezvoltare și publicare a „software-ului liber și cu sursă deschisă" (FOSS) și oferă unele orientări pentru a contribui la identificarea FOSS ca fiind un produs cu elemente digitale introdus pe piață (și anume în cadrul unei activități comerciale) în înțelesul CRA. Astfel cum se explică la considerentul 18, „circumstanțele în care a fost dezvoltat produsul cu elementele digitale sau modul în care a fost finanțată dezvoltarea nu ar trebui […] să fie luate în considerare atunci când se stabilește natura comercială sau necomercială a activității respective". Mai precis, „pentru a se asigura că există o distincție clară între etapele de dezvoltare și de furnizare, furnizarea de produse cu elemente digitale care se califică drept software gratuit și cu sursă deschisă care nu sunt monetizate de producătorii lor nu ar trebui să fie considerată a fi o activitate comercială".

([11]) De asemenea, ar trebui reamintit faptul că, deși adesea produsele cu elemente digitale sunt monetizate (și) prin prelucrarea datelor cu caracter personal, protecția datelor cu caracter personal este un drept fundamental și, așadar, datele cu caracter personal nu pot fi considerate o marfă, astfel cum se indică la considerentul 24 din Directiva (UE) 2019/770 a Parlamentului European și a Consiliului din 20 mai 2019 privind anumite aspecte referitoare la contractele de furnizare de conținut digital și de servicii digitale (JO L 136, 22.5.2019, p. 1, ELI: http://data.europa.eu/eli/dir/2019/770/oj).

43. Prin urmare, este util (i) să se clarifice ce este FOSS; (ii) să se indice în ce condiții se consideră că un FOSS intră în sfera de responsabilitate a unei persoane fizice sau juridice și (iii) să se furnizeze exemple pentru a ajuta părțile interesate să înțeleagă când distribuția de FOSS constituie introducere pe piață. În cazul în care FOSS nu este introdus pe piață, acesta nu intră în domeniul de aplicare al CRA, cu excepția cazului în care entitatea care îl publică este o persoană juridică ce se încadrează în definiția „administratorului de software cu sursă deschisă" (denumit în continuare „administratorul") în temeiul articolului 3 punctul 14. În acest caz, se supune numai obligațiilor prevăzute la articolul 24.

44. Articolul 3 punctul 48 definește FOSS ca fiind „un software al cărui cod sursă este partajat în mod deschis și care este pus la dispoziție sub licență liberă și cu sursă deschisă ce prevede toate drepturile necesare pentru ca software-ul să fie accesibil, utilizabil, modificabil și redistribuibil în mod liber". Deși prezentele orientări nu identifică licențe libere și cu sursă deschisă specifice care sunt compatibile cu definiția prevăzută la articolul 3 punctul 48, din formularea dispoziției respective rezultă că numai software-ul care îndeplinește cumulativ două condiții se califică drept FOSS în sensul CRA: (i) software-ul trebuie să fie pus la dispoziție sub licență liberă și cu sursă deschisă care acordă setul complet de drepturi menționate la articolul 3 punctul 48 și (ii) codul său sursă trebuie să fie partajat în mod deschis.

45. Cerința ca licența să prevadă ca software-ul să fie „accesibil, utilizabil, modificabil și redistribuibil în mod liber" reflectă interpretarea tradițională a FOSS, și anume că utilizatorii trebuie să poată accesa codul sursă, să îl utilizeze fără restricții nejustificate, să îl modifice și să redistribuie versiunile originale sau modificate. Accesul la codul sursă este, prin urmare, o condiție prealabilă necesară pentru exercitarea celorlalte drepturi: fără acces la codul sursă, nu este posibil din punct de vedere practic să se modifice sau să se reutilizeze în mod semnificativ software-ul.

46. Cu toate acestea, articolul 3 punctul 48 nu se referă numai la condițiile licenței, întrucât impune în mod expres ca respectivul cod sursă „să fie partajat în mod deschis". Noțiunea de „partajat în mod deschis" indică faptul că respectivul cod sursă trebuie să fie pus la dispoziția publicului (fie „în amonte", fie „în aval"), și nu doar furnizat în mod restricționat sau condiționat. În consecință, software-ul distribuit sub licență liberă și cu sursă deschisă, dar al cărui cod sursă este partajat (sau este permis să fie partajat) numai cu clienți plătitori sau cu un grup limitat de utilizatori nu trebuie considerat FOSS în înțelesul articolului 3 punctul 48. În sensul CRA, numai software-ul al cărui cod sursă este disponibil public și care face obiectul unei licențe libere și cu sursă deschisă care acordă setul complet de drepturi menționate la articolul 3 punctul 48 ar trebui, prin urmare, să se califice drept FOSS.

3.1. **Stabilirea responsabilității unei persoane pentru un software liber și cu sursă deschisă**

47. CRA atribuie responsabilități esențiale operatorilor economici care furnizează produse cu elemente digitale pe piața UE. Acesta definește producătorul ca fiind persoana fizică sau juridică ce furnizează un produs cu elemente digitale sub numele sau marca sa și în cadrul unei activități comerciale (introducându-l astfel pe piață). În mod similar, un importator este persoana fizică sau juridică stabilită în UE care furnizează produsul cu elemente digitale unei persoane stabilite în afara UE, în cadrul unei activități comerciale (introducându-l astfel pe piață). Obligațiile administratorilor se aplică persoanei juridice care furnizează un FOSS destinat activităților comerciale ([12]), dar nu îl introduce pe piață în înțelesul CRA.

48. Prin urmare, pentru a stabili dacă o persoană fizică sau juridică introduce FOSS pe piața UE, mai întâi trebuie să se clarifice dacă persoana fizică sau juridică respectivă furnizează efectiv FOSS. Pentru a stabili în mod corect obligațiile aplicabile în temeiul CRA, este esențial să se stabilească dacă persoana fizică sau juridică efectuează într-adevăr acțiunea de furnizare a unui FOSS. În fapt, astfel cum se reamintește la considerentul 18, CRA nu se aplică persoanelor fizice sau juridice care contribuie cu cod sursă la produse cu elemente digitale care se califică drept FOSS și care nu se află în responsabilitatea lor.

([12]) Aceasta este o condiție necesară, dar nu suficientă pentru ca o persoană juridică să se califice drept administrator de software cu sursă deschisă, deoarece definiția prevăzută la articolul 3 punctul 14 stabilește condiții suplimentare pentru ca o persoană juridică să se califice drept administrator de software cu sursă deschisă.

49. Având în vedere particularitățile dezvoltării FOSS, care implică adesea mai mulți contribuitori, modele de colaborare descentralizată și o separare între contribuție și procesul decizional, este util să se clarifice faptul că FOSS este considerat a intra „în sfera de responsabilitate" a persoanelor fizice sau juridice care îl publică și exercită controlul primar asupra deciziilor în materie de dezvoltare, versiuni și distribuție a acestuia (denumiți adesea „operatori de întreținere"). Persoanele care contribuie cu codul sursă, dar nu controlează deciziile în materie de versiuni, foi de parcurs sau guvernanță sunt considerate „contribuitori"; în astfel de cazuri, FOSS nu intră în sfera lor de responsabilitate, chiar dacă au contribuit cu coduri la acesta. Simpla existență a unor autorizații tehnice, cum ar fi angajarea accesului, nu este suficientă pentru a stabili că FOSS intră în sfera de responsabilitate a persoanei respective; responsabilitatea le revine celor care publică și controlează FOSS.

Exemplul 13: Un dezvoltator individual sau un angajat al unei societăți depune o solicitare de tip „pull" sau „merge" care conține o corecție de securitate sau o nouă caracteristică a unui proiect FOSS. Operatorii de întreținere ai proiectului reexaminează, acceptă și fuzionează codul în depozitul principal, incluzându-l ulterior într-o nouă versiune. În acest scenariu, persoana care a depus solicitarea de tip „pull" este un „contribuitor" și nu face obiectul CRA. Deși această persoană a contribuit cu un cod sursă, ea nu exercită un control primar asupra deciziilor în materie de dezvoltare, versiuni sau distribuție.

3.2. **Stabilirea plasării unui software liber și cu sursă deschisă pe piața UE**

50. Odată ce se stabilește că un FOSS intră în responsabilitatea unei persoane fizice sau juridice, trebuie să se stabilească dacă persoana respectivă îl furnizează în cadrul unei activități comerciale, constituind astfel o plasare pe piață.

3.2.1. *Perceperea unui preț*

51. În cazul în care persoana fizică sau juridică ce furnizează un FOSS percepe un preț pentru software-ul în sine (de exemplu, prin perceperea unui preț pentru sistemele binare precompilate), persoana respectivă plasează pe piață un produs cu elemente digitale. Prin urmare, persoana care plasează pe piață un FOSS este un producător în temeiul CRA.

52. Adesea, producătorii de FOSS furnizează versiuni gratuite ale acestui software (denumite adesea versiuni „comunitare"), a căror bază de cod este (aproape) identică cu versiunea plătită. Totuși, aceste produse cu elemente digitale sunt produse diferite: versiunea plătită este monetizată într-un anumit mod (de exemplu, fie prin perceperea unui preț, fie prin alte mijloace, astfel cum se discută în prezenta secțiune) și, prin urmare, este considerată a fi introdusă pe piață, ceea ce declanșează obligațiile producătorului. Versiunea furnizată gratuit (sau versiunea comunitară) nu este monetizată și, prin urmare, nu este considerată a fi introdusă pe piață în scopul CRA. Acest aspect este valabil și în cazul în care versiunea plătită este o versiune comercială „îmbunătățită", care extinde baza de cod a versiunii furnizate în mod gratuit sau încorporează versiunea respectivă într-un produs mai amplu cu elemente digitale (de exemplu, ca în cazul modelului „open core").

53. În cazul în care persoana care furnizează versiunea comunitară este o persoană juridică, respectiva persoană juridică este supusă și obligațiilor care revin administratorilor pentru versiunea pe care o furnizează în mod gratuit (versiunea comunitară). Dacă entitatea este o persoană fizică, versiunea furnizată gratuit (versiunea comunitară) nu intră în domeniul de aplicare al CRA.

3.2.2. *Monetizarea altor servicii sau solicitarea prelucrării datelor cu caracter personal*

54. O persoană fizică sau juridică ce publică un FOSS poate, de asemenea, să îl plaseze pe piață (și anume să îl furnizeze în cadrul unei activități comerciale) în cazul în care furnizează software-ul prin care monetizează alte produse cu elemente sau servicii digitale sau în cazul în care impune drept condiție de utilizare prelucrarea datelor cu caracter personal din alte motive decât exclusiv pentru îmbunătățirea securității, a compatibilității sau a interoperabilității software-ului.

Exemplul 14: O persoană fizică sau juridică publică o aplicație pe piață liberă și cu sursă deschisă. Aplicația este disponibilă gratuit și le permite utilizatorilor să achiziționeze bunuri sau servicii prin intermediul său. Aplicația permite persoanei care a publicat-o să monetizeze alte produse cu elemente digitale și servicii oferite prin intermediul său (de exemplu, prin anunțuri publicitare, comisioane sau taxe de abonament). Prin urmare, aplicația este considerată introdusă pe piață în cadrul unei activități comerciale.

Exemplul 15: O persoană fizică sau juridică publică un VPN liber și cu sursă deschisă. Aplicația este disponibilă gratuit, dar permite utilizatorilor să plătească pentru a accesa servere suplimentare sau adrese IP dedicate. Această aplicație permite persoanei respective să monetizeze alte servicii oferite prin intermediul său și, prin urmare, este considerată introdusă pe piață în cadrul unei activități comerciale.

Exemplul 16: O persoană fizică sau juridică publică o aplicație liberă și cu sursă deschisă pentru monitorizarea condiției fizice. Aplicația este disponibilă gratuit, dar utilizarea sa este condiționată de prelucrarea datelor cu caracter personal ale utilizatorilor în scopuri precum publicitatea direcționată sau analiza care nu au legătură cu securitatea, compatibilitatea sau interoperabilitatea software-ului. Prin urmare, prin impunerea unei astfel de prelucrări a datelor ca o condiție de utilizare, aplicația este considerată introdusă pe piață în cadrul unei activități comerciale.

3.2.3. *Servicii de asistență*

55. Simplul fapt că o persoană fizică sau juridică ce publică un FOSS oferă totodată servicii de asistență plătite legate de acesta nu înseamnă, ca atare, că produsul cu elemente digitale este furnizat în cadrul unei activități comerciale. Serviciile de asistență pot include activități precum consultanța, formarea sau serviciile profesionale legate de utilizarea, documentarea, configurarea și implementarea software-ului de către un client.

56. Factorul decisiv este dacă accesul la FOSS în sine (și anume furnizarea produsului cu elemente digitale), inclusiv întreținerea acestuia, este condiționat mai degrabă de o remunerație decât de simpla ofertă de servicii profesionale care vizează un produs cu elemente digitale disponibil gratuit, astfel cum se indică la considerentul 18 din CRA („furnizarea de produse cu elemente digitale care se califică drept software gratuit și cu sursă deschisă care nu sunt monetizate de producătorii lor nu ar trebui să fie considerată a fi o activitate comercială”). În cazul în care FOSS poate fi descărcat și instalat în mod liber, iar utilizatorii pot alege opțional să achiziționeze servicii profesionale separat, FOSS respectiv nu este considerat a fi introdus pe piață.

57. În schimb, în unele cazuri, accesul la o anumită versiune a produsului cu elemente digitale, inclusiv la anumite beneficii, cum ar fi asistența tehnică sau optimizarea performanței, este condiționat de remunerare. În astfel de cazuri, dispoziția respectivă constituie o furnizare monetizată a unui produs cu elemente digitale furnizat în cadrul unei activități comerciale și, prin urmare, este considerat introdus pe piață. Aceasta include cazurile în care o ediție plătită sau o versiune comercială este pusă la dispoziție în temeiul unui acord comercial, indiferent dacă software-ul echivalent din punct de vedere funcțional este, de asemenea, disponibil gratuit în baza unei licențe libere și cu sursă deschisă.

Exemplul 17: O persoană fizică sau juridică publică un sistem de operare liber și cu sursă deschisă, oferind o versiune plătită a sistemului de operare respectiv, care include servicii de asistență, cum ar fi asistența tehnică sau optimizarea performanței. Versiunea plătită a sistemului de operare este considerată introdusă pe piață în cadrul unei activități comerciale.

Exemplul 18: O persoană fizică sau juridică publică un instrument de linie de comandă liber și cu sursă deschisă. Instrumentul este accesibil gratuit și poate fi descărcat și instalat de orice persoană. Persoana fizică sau juridică respectivă oferă separat servicii profesionale, cum ar fi servicii opționale de consultanță pentru formarea utilizatorilor și sprijinirea acestora în ceea ce privește instalarea și utilizarea instrumentului. Acest FOSS nu este considerat introdus pe piață în înțelesul CRA.

58. În special în cazul persoanelor fizice care publică FOSS, oferirea de asistență tehnică grupată direct cu accesul la produsul cu elemente digitale tot nu s-ar califica drept activitate comercială dacă, astfel cum se indică la considerentul 15 din CRA, prețul perceput servește doar la recuperarea costurilor reale. Astfel de costuri reale includ o varietate de costuri legate de proiectarea, dezvoltarea și întreținerea software-ului respectiv, inclusiv cheltuielile de subzistență rezonabile ale persoanei. Prin urmare, o persoană fizică ce publică un FOSS și oferă asistență tehnică pentru a-și acoperi costurile și pentru a obține o remunerație echitabilă nu trebuie considerată, numai pe această bază, ca introducând software-ul respectiv pe piața UE.

59. Nu se consideră că o persoană fizică sau juridică ce oferă asistență tehnică legată de un FOSS și care nu se află în responsabilitatea sa introduce software-ul respectiv pe piață, cu excepția cazului în care persoana respectivă modifică substanțial FOSS, în conformitate cu articolul 22, în contextul furnizării unei astfel de asistențe.

Exemplul 19: Un prestator de servicii nu publică un FOSS, dar ajută un client să îl instaleze pe serverul clientului la sediu. Această acțiune este întreprinsă fără a efectua o modificare substanțială a respectivului FOSS. Prin urmare, se consideră că prestatorul de servicii nu introduce FOSS pe piață.

3.2.4. *Donații*

60. Persoanele fizice sau juridice care publică proiecte FOSS includ în mod obișnuit modalități prin care utilizatorii software-ului respectiv pot dona în mod voluntar bani pentru a mulțumi editorului (editorilor) proiectului și, de asemenea, pentru a se asigura că proiectul este întreținut în mod activ.

61. Astfel cum se indică la considerentul 15 din CRA, „acceptarea de donații fără intenția de a realiza un profit nu ar trebui să fie considerată o activitate comercială”. Simplul fapt de a include un link către o platformă de donații sau instrumente similare de colectare a donațiilor nu ar trebui considerat o intenție de a realiza un profit, chiar și în cazul în care suma colectată din donații depășește simplele costuri asociate proiectării, dezvoltării și furnizării unui produs cu elemente digitale. Aceasta include o compensație rezonabilă pentru contribuitorii angajați de o persoană juridică și/sau cheltuielile de subzistență rezonabile ale unei persoane fizice. Donațiile, prin însăși natura lor, fluctuează în timp și, prin urmare, trebuie exercitat un anumit grad de flexibilitate atunci când se evaluează dacă un FOSS monetizat exclusiv prin donații este considerat a fi introdus pe piață. Prin urmare, este puțin probabil ca un FOSS susținut numai prin donații să fie considerat introdus pe piață în înțelesul CRA.

Exemplul 20: O persoană fizică sau juridică publică un instrument FOSS într-un depozit public online, permițând oricui să îl descarce, să îl utilizeze, să îl modifice și să îl redistribuie sub o licență liberă și cu sursă deschisă. Editorul invită utilizatorii să efectueze donații voluntare prin intermediul unei platforme de donații pentru a susține dezvoltarea și întreținerea permanentă a proiectului. Accesul la software, la codul sursă și la actualizările acestuia nu este condiționat de efectuarea unei donații. Acest FOSS nu este considerat a fi furnizat în cadrul unei activități comerciale și nu este considerat a fi introdus pe piață în înțelesul CRA.

62. Cu toate acestea, există cazuri în care un FOSS susținut prin donații poate fi considerat introdus pe piață. Acest aspect este valabil în cazul în care, pe baza unei evaluări generale a circumstanțelor, donațiile sunt echivalente de facto cu perceperea unui preț pentru accesul la produsul cu elemente digitale sau la anumite funcționalități ale acestuia. Această situație poate surveni, în special, în cazul în care accesul la FOSS, la funcționalitățile esențiale sau la actualizări este condiționat în practică de efectuarea unei donații sau în cazul în care donațiile sunt asociate cu beneficii contractuale sau avantaje exclusive care depășesc sfera comunității.

Exemplul 21: O persoană fizică sau juridică publică un produs software cu elemente digitale în baza unei licențe libere și cu sursă deschisă, dar furnizează versiuni care pot fi descărcate și actualizări de securitate exclusiv utilizatorilor care efectuează o donație. Utilizatorii care nu efectuează donații nu au acces la versiunea actuală a software-ului.

În acest caz, donațiile reprezintă de facto o condiție pentru accesul la produsul cu elemente digitale și, prin urmare, echivalează cu perceperea unui preț. Prin urmare, se consideră că respectivul FOSS este introdus pe piață în înțelesul CRA.

Exemplul 22: O persoană fizică sau juridică pune codul sursă al unui FOSS la dispoziția publicului, însă furnizează binare precompilate, actualizări periodice și soluții de securitate garantate exclusiv donatorilor. În acest caz, donațiile sunt legate de accesul la aspecte esențiale ale produsului cu elemente digitale și constituie o remunerație pentru furnizarea produsului respectiv. Prin urmare, se consideră că acest FOSS este introdus pe piață în cadrul unei activități comerciale.

3.2.5. *Finanțarea unui software liber și cu sursă deschisă*

63. Simplul fapt că un terț a plătit, a sponsorizat sau a finanțat în alt mod dezvoltarea unui FOSS nu stabilește în sine dacă FOSS respectiv este introdus pe piață. Este o practică obișnuită în ecosistemul FOSS ca dezvoltatorii individuali, fundațiile sau comunitățile să primească finanțare din partea întreprinderilor, a organismelor publice sau a altor sponsori pentru a lucra la caracteristici specifice, a remedia erorile sau a menține componente critice. Această finanțare poate lua multe forme, inclusiv granturi, programe de stimulare a identificării bug-urilor, sponsorizări, contracte de servicii sau activități de dezvoltare remunerate.

64. Astfel cum s-a reamintit deja, considerentul 18 din CRA clarifică faptul că circumstanțele în care a fost dezvoltat produsul cu elementele digitale sau modul în care a fost finanțată dezvoltarea nu ar trebui să fie luate în considerare atunci când se stabilește natura comercială a activității respective.

65. Prin urmare, în cazul în care FOSS este partajat în mod deschis și pus la dispoziția tuturor în mod gratuit pentru a fi accesat, utilizat, modificat și redistribuit, faptul că este posibil ca o entitate comercială să fi plătit pentru proiectul respectiv nu ar trebui să contribuie la stabilirea introducerii sau nu pe piață a software-ului. În fapt, dacă respectivul FOSS nu este monetizat în alt mod, acesta nu trebuie considerat introdus pe piață. În cazul în care întreprinderea care a finanțat dezvoltarea FOSS (precum și orice altă întreprindere) îl integrează în produsul său cu elemente digitale, întreprinderea respectivă trebuie să exercite diligența necesară în conformitate cu articolul 13 alineatul (5) din CRA.

Exemplul 23: Un dezvoltator individual publică un proiect de FOSS și îl întreține în mod activ. Producătorul A solicită dezvoltatorului individual să adauge o caracteristică specifică pentru respectivul FOSS și finanțează dezvoltarea în cauză. Dezvoltatorul adaugă caracteristica respectivă la baza de cod a FOSS, partajând-o în mod deschis și punând-o la dispoziția tuturor în mod gratuit pentru a fi accesată, utilizată, modificată și redistribuită. Se consideră că dezvoltatorul individual nu a introdus pe piață respectivul FOSS. În cazul în care producătorul integrează FOSS în produsul său cu elemente digitale, acesta trebuie să exercite diligența necesară în conformitate cu articolul 13 alineatul (5).

3.2.6. *Entități non-profit înființate pentru a atinge obiective non-profit*

66. În cazul în care o persoană juridică ce publică un FOSS este o organizație non-profit „înființată astfel încât să se asigure că toate veniturile după costuri sunt utilizate pentru a atinge obiective non-profit” (considerentul 18 din CRA), FOSS pe care îl publică nu este considerat introdus pe piață. În cazul în care persoana juridică respectivă se încadrează în definiția „administratorului”, aceasta este supusă obligațiilor corespunzătoare (articolul 24 din CRA).

Exemplul 24: O persoană juridică publică un browser liber și cu sursă deschisă care este monetizat direct prin intermediul parteneriatelor cu motoare de căutare, dar toate veniturile sale după costuri sunt utilizate pentru obiective non-profit. Browserul nu este considerat a fi introdus pe piață în înțelesul CRA. Persoana juridică ce îl publică este supusă obligațiilor aplicabile administratorilor.

3.2.7. *Integrarea de alți producători*

67. În unele cazuri, un FOSS este publicat de o persoană fizică sau juridică ușor de identificat, însă acest FOSS este „destinat integrării de către alți producători în propriile produse cu elemente digitale”. În astfel de cazuri, FOSS respectiv nu este considerat a fi introdus pe piața UE, cu excepția cazului în care este, de asemenea, monetizat de persoana care îl publică (și anume producătorul de origine), în conformitate cu secțiunile anterioare ale prezentelor orientări.

68. În cazul în care respectivul FOSS nu este introdus pe piață, persoana juridică ce îl publică ar fi supusă obligațiilor administratorilor, dacă oferă sprijin în mod susținut, în conformitate cu definiția „administratorului”.

Exemplul 25: O persoană juridică publică o bibliotecă FOSS pentru construirea interfețelor pentru utilizatori. Aceasta nu monetizează oferta bibliotecii respective, ci o integrează într-unul dintre produsele sale cu elemente digitale (care, la rândul său, este introdus pe piață). Biblioteca nu este considerată ca fiind introdusă pe piață în înțelesul CRA, dar este destinată integrării în produse cu elemente digitale. Persoana juridică ce o publică este administratorul acesteia.

Exemplul 26: O persoană juridică introduce pe piață un sistem de operare și publică, de asemenea, biblioteci FOSS pentru a servi drept implementări de referință pentru utilizatorii sistemului de operare respectiv. Persoana juridică nu monetizează bibliotecile FOSS, care sunt destinate integrării în alte produse cu elemente digitale. Persoana juridică ce le publică este un administrator al acestor biblioteci FOSS.

3.3. **Administratori de software cu sursă deschisă**

69. CRA introduce noua categorie juridică de „administratori de software cu sursă deschisă”, având în vedere „importanța pentru securitatea cibernetică a multor produse cu elemente digitale care se califică drept software gratuit și cu sursă deschisă care sunt publicate, dar nu sunt puse la dispoziție pe piață în înțelesul [CRA]” (considerentul 19 din CRA).

70. În unele cazuri, un FOSS este publicat, dar nu este pus la dispoziție pe piață în înțelesul CRA de către o persoană juridică, care „are scopul sau obiectivul de a oferi în mod sistematic și durabil sprijin pentru dezvoltarea de [FOSS] [...] destinate unor activități comerciale, și care asigură viabilitatea produselor respective” (articolul 3 punctul 14 din CRA). În astfel de cazuri, persoana juridică respectivă este supusă obligațiilor administratorilor.

71. Un administrator este definit ca fiind „o persoană juridică, alta decât un producător”, deoarece un producător, prin definiție, este persoana fizică sau juridică ce introduce pe piață produse cu elemente digitale („le comercializează”) sub numele sau marca sa. O persoană juridică poate fi un administrator numai pentru produsele cu elemente digitale care se califică drept FOSS care sunt publicate, dar nu sunt puse la dispoziție pe piață în înțelesul CRA. Prin urmare, conceptul de administrator se aplică unor cazuri specifice de FOSS care „sunt în cele din urmă destinate activităților comerciale, cum ar fi integrarea în servicii comerciale sau în produse monetizate cu elemente digitale” [considerentul 19 din CRA ([13])], dar care nu sunt puse la dispoziție pe piață în înțelesul CRA și pentru care persoana juridică ce publică FOSS respectiv asigură un sprijin sistematic.

72. Calitatea de administrator pentru un anumit FOSS nu înseamnă că persoana juridică respectivă este neapărat administrator și pentru alte FOSS pe care le publică. În mod similar, calitatea de producător pentru un anumit FOSS nu înseamnă că persoana juridică nu poate fi administrator pentru alt FOSS. Aceasta include furnizarea de versiuni „comunitare” ale aceluiași FOSS, astfel cum se descrie în secțiunea *3.2.1 Perceperea unui preț*.

73. Prin urmare, o persoană juridică poate fi simultan un administrator pentru un anumit FOSS (în cazul în care administratorul oferă în mod sistematic sprijin în mod susținut și asigură viabilitatea software-ului) și un producător pentru un alt FOSS specific (în cazul în care îl introduce pe piață). Cu alte cuvinte, aceeași entitate juridică poate fi obligată să îndeplinească roluri diferite pentru proiecte FOSS diferite.

74. Pentru fiecare FOSS specific pe care îl publică, persoana juridică va trebui să verifice dacă respectivul FOSS este considerat a fi introdus pe piață în înțelesul CRA. În caz afirmativ, entitatea juridică este producătorul software-ului. În cazul în care se consideră că FOSS nu este introdus pe piață, persoana juridică poate fi administratorul acestuia, dacă software-ul este destinat activităților comerciale și dacă persoana juridică îl susține în conformitate cu definiția administratorului ([14]).

3.3.1. *Asistență susținută și asigurarea viabilității FOSS*

75. Considerentul 19 explică faptul că furnizarea de asistență susținută pentru dezvoltarea unui produs cu elemente digitale poate include (fără a se limita la acestea): (i) găzduirea și gestionarea platformelor de colaborare pentru dezvoltarea de software; (ii) găzduirea de coduri sursă sau software; (iii) reglementarea sau gestionarea produselor cu elemente digitale care se califică drept FOSS și (iv) coordonarea dezvoltării unor astfel de produse cu elemente digitale.

76. Această situație poate surveni, de exemplu, în cazul unei entități juridice care dezvoltă FOSS în vederea integrării în propriile produse cu elemente digitale și apoi îl publică fără a-l introduce pe piață. Acest aspect este discutat, de asemenea, în secțiunea *3.2.7 Integrarea de alți producători*. În acest caz, entitatea juridică nu este un producător al software-ului, ci poate fi un administrator al acestuia. În plus, astfel cum s-a explicat și în secțiunile anterioare, o entitate juridică ce publică o versiune gratuită (sau comunitară) și o versiune monetizată a aceluiași FOSS este considerată un administrator pentru versiunea gratuită (sau comunitară) și un producător pentru versiunea monetizată.

77. În mod similar, o entitate juridică ce monetizează un FOSS, dar este o entitate non-profit ale cărei venituri după costuri sunt utilizate pentru a atinge obiective non-profit (și, prin urmare, FOSS nu este introdus pe piață în înțelesul CRA, astfel cum se discută în secțiunea *3.2.6 Entități non-profit*) este un administrator al FOSS pe care îl publică.

78. În plus, anumite fundații oferă platforme de colaborare cu diferite forme de guvernanță care permit producătorilor să contribuie în mod regulat la dezvoltarea FOSS și/sau care sunt finanțate în mod regulat de producători. Astfel de fundații trebuie considerate administratori în ceea ce privește FOSS specifice care sunt destinate activităților comerciale și pentru care fundația oferă asistență susținută. Cu toate acestea, astfel cum s-a explicat în secțiunea *3.3 Administratori de software cu sursă deschisă*, este posibil ca o astfel de fundație să nu facă obiectul niciunei obligații în temeiul CRA pentru alte FOSS specifice pe care le găzduiește, în cazurile în care nu oferă sprijin sistematic pentru un anumit FOSS, nu îi asigură viabilitatea și/sau software-ul specific nu este destinat activităților comerciale.

([13]) Această noțiune este inclusă, de asemenea, în formularea „destinate activităților comerciale” inclusă în definiția „administratorului de software cu sursă deschisă” prevăzută la articolul 3 punctul 14 din CRA.

([14]) De asemenea, persoana juridică nu poate fi supusă niciunei obligații în temeiul CRA, în cazurile în care: (i) un anumit FOSS nu este introdus pe piață în înțelesul CRA și (ii) entitatea juridică nu se încadrează în definiția administratorului judiciar în legătură cu respectivul FOSS specific.

79. Tipul de „asistență susținută” pe care fundațiile și organizațiile similare îl acordă proiectelor FOSS specifice poate varia în mare măsură. De exemplu, anumite entități juridice oferă doar sprijin fără caracter tehnic, cum ar fi gestionarea brandingului proiectelor, stabilirea normelor de guvernanță, organizarea de evenimente comunitare sau colectarea de donații. Alte entități furnizează, de asemenea, infrastructura informatică subiacentă necesară pentru desfășurarea proiectului, cum ar fi găzduirea registrelor de coduri sursă, furnizarea de sisteme de control al versiunilor sau generarea de chei de semnare. Altele merg mai departe în ceea ce privește tipul de asistență pe care îl oferă, contribuind activ la proiect cu resurse în materie de inginerie, de exemplu prin angajarea de dezvoltatori, coordonarea activităților de dezvoltare, reexaminarea sau fuzionarea codurilor, gestionarea versiunilor sau gestionarea rapoartelor de vulnerabilitate și a corecțiilor de securitate. Deși toate entitățile juridice care se califică drept administratori în temeiul CRA trebuie să respecte obligațiile prevăzute la articolul 24 alineatele (1) și (2), măsura în care obligațiile prevăzute la articolul 14 alineatele (1), (3) și (8) se aplică entităților juridice respective variază în funcție de tipul de asistență pe care îl acordă, în conformitate cu articolul 24 alineatul (3).

80. De exemplu, un administrator care oferă doar sprijin fără caracter tehnic nu este, prin definiție, implicat în dezvoltarea produsului cu elemente digitale și, prin urmare, nu este obligat să raporteze vulnerabilitățile exploatate activ. De asemenea, administratorul respectiv nu furnizează nicio rețea și niciun sistem informatic pentru dezvoltarea unor astfel de produse cu elemente digitale și, prin urmare, nu este obligat să raporteze incidentele grave către ENISA și CSIRT sau către utilizatorii afectați. Cu toate acestea, în cazul în care administratorul ia cunoștință de o vulnerabilitate exploatată activ (de exemplu, prin intermediul unui raport din surse externe, cum ar fi cercetătorii în domeniul securității), acesta ar trebui să partajeze informațiile cu operatorii de întreținere ai produsului cu elemente digitale, în conformitate cu politica sa de securitate cibernetică. Operatorii de întreținere ai produselor cu elemente digitale și/sau administratorii ar trebui, de asemenea, să ia în considerare raportarea vulnerabilității în mod voluntar, în conformitate cu articolul 15.

81. Pe de altă parte, în cazul în care un administrator furnizează infrastructura informatică subiacentă pentru anumite produse cu elemente digitale, acesta are obligația de a notifica ENISA și CSIRT, în conformitate cu articolul 14 alineatul (3), orice incidente grave legate de infrastructura respectivă care afectează securitatea produselor cu elemente digitale. De asemenea, se impune, după caz, informarea tuturor utilizatorilor (de exemplu, printr-un anunț general). Astfel cum se indică la punctul anterior, deși administratorul nu este obligat să raporteze vulnerabilitățile exploatate activ de care ia cunoștință, acesta ar trebui să promoveze gestionarea corectă a vulnerabilităților și ar trebui să ia în considerare raportarea voluntară în conformitate cu articolul 15.

82. În cele din urmă, în cazul în care un administrator furnizează, de asemenea, resurse în materie de inginerie pentru produse specifice cu elemente digitale, acesta trebuie: (i) să notifice, în conformitate cu articolul 14 alineatul (1), vulnerabilitățile exploatate activ de care ia cunoștință și (ii) după caz, să informeze toți utilizatorii. În măsura în care administratorul are, de asemenea, o relație directă cu utilizatorii afectați, acesta are totodată obligația de a-i informa în mod direct, în conformitate cu articolul 14 alineatul (8).

83. În cazul în care o entitate încetează să mai ofere sprijin în mod sistematic și durabil pentru un anumit FOSS, este posibil ca aceasta să nu se mai încadreze în definiția administratorului și, prin urmare, să nu mai facă obiectul obligațiilor corespunzătoare. În astfel de cazuri, entitatea respectivă este încurajată să comunice în mod clar modificarea statutului său pentru respectivul FOSS.

84. În anumite situații, o entitate care a fost administrator pentru un anumit proiect poate decide să monetizeze direct proiectul respectiv, introducând astfel pe piață produsul cu elemente digitale și declanșând obligațiile producătorului în temeiul CRA. În astfel de circumstanțe, entitatea respectivă se califică drept producător al produsului cu elemente digitale de la data la care îl introduce pe piață (dar nu în ceea ce privește versiunile anterioare pentru care a acționat în calitate de administrator).

3.4. **Contribuitori și utilizări în aval**

85. Astfel cum s-a menționat deja în secțiunea *3.1 Stabilirea responsabilității unei persoane pentru un software liber și cu sursă deschisă*, CRA clarifică faptul că nu se aplică „persoanelor fizice sau juridice care contribuie cu cod sursă la produse cu elemente digitale care se califică drept software gratuit și cu sursă deschisă care nu se află în responsabilitatea lor” (considerentul 18).

86. Nici producătorii de produse cu elemente digitale care integrează componente FOSS în propriile produse cu elemente digitale nu devin responsabili pentru conformitatea individuală a acestor componente cu CRA, chiar și în cazul în care producătorii contribuie cu codul sursă la întreținerea lor.

87. În mod similar, simplul fapt că producătorii integrează componente FOSS în propriile produse (monetizate) cu elemente digitale nu are niciun impact asupra statutului respectivei componente FOSS în cadrul CRA. Operatorii de întreținere ai componentelor FOSS care nu sunt introduse pe piață nu au obligații în raport cu alte entități care pot integra astfel de componente în produsele lor cu elemente digitale. Aplicarea CRA în raport cu o anumită componentă a FOSS depinde exclusiv de introducerea sa pe piață de către persoana fizică sau juridică ce o publică.

88. Cu toate acestea, producătorii de produse cu elemente digitale care integrează componente FOSS au obligația de a respecta CRA pentru propriile produse cu elemente digitale. De asemenea, acestora le revine o obligație de diligență, în conformitate cu articolul 13 alineatul (5), față de componentele FOSS pe care le integrează. În plus, aceștia au obligația de a raporta vulnerabilitățile componentelor integrate și de a partaja soluțiile de securitate în conformitate cu articolul 13 alineatul (6). Pentru mai multe informații pe această temă, a se vedea secțiunea *9.2.1 Raportarea în amonte și partajarea soluțiilor de securitate*.

3.5. **Scenarii ilustrative**

89. Exemplele prezentate mai jos sunt complet ipotetice și sunt menite doar să ilustreze diferite cazuri, astfel cum sunt explicate în secțiunile de mai sus.

Exemplul 27: Dezvoltatorul individual A a dezvoltat un FOSS. Dezvoltatorul A publică FOSS sub numele sau marca sa, dar nu percepe un preț pentru utilizarea acestuia. Software-ul este partajat în mod deschis și disponibil tuturor în mod gratuit pentru a fi accesat, utilizat, modificat și redistribuit. Dezvoltatorul A include, de asemenea, un link către o platformă de colectare a donațiilor voluntare.

Societățile B, C și D integrează acest FOSS în propriile produse cu elemente digitale. Pentru a sprijini întreținerea permanentă, societățile B, C și D efectuează donații voluntare către dezvoltatorul A. Aceste donații permit dezvoltatorului A să întrețină proiectul în mod activ.

Acest FOSS nu este introdus pe piață în înțelesul CRA. Dezvoltatorului A nu îi revin obligații în temeiul CRA. Societățile B, C și D trebuie să exercite diligența necesară în conformitate cu articolul 13 alineatul (5) atunci când integrează respectivul FOSS în propriile produse cu elemente digitale.

Exemplul 28: Fundația non-profit F publică o componentă FOSS pentru integrarea în alte produse comerciale cu elemente digitale. Fundația F se angajează să ofere asistență susținută respectivului FOSS, pentru a asigura viabilitatea și adoptarea acestuia. Societățile A, B și C integrează acest FOSS în propriile produse cu elemente digitale. Societățile A și B contribuie în mod voluntar cu o parte din timpul dezvoltatorilor lor la dezvoltarea și întreținerea proiectelor FOSS în cadrul fundației F, inclusiv pentru FOSS respectiv.

Întrucât fundația F este o entitate non-profit înființată astfel încât veniturile sale după costuri sunt utilizate pentru a atinge obiective non-profit, FOSS nu este considerat introdus pe piață în înțelesul CRA. Fundația F este administratorul FOSS și face obiectul obligațiilor corespunzătoare prevăzute la articolul 24. Societățile A, B și C trebuie să exercite diligența necesară în conformitate cu articolul 13 alineatul (5) atunci când integrează respectivul FOSS în propriile produse cu elemente digitale.

Exemplul 29: Societatea A a dezvoltat o componentă FOSS pentru integrarea în propriile produse cu elemente digitale. De asemenea, aceasta publică FOSS separat sub numele sau marca sa și îl întreține în mod activ. Cu toate acestea, nu percepe taxe pentru utilizarea sa și nici nu monetizează în alte moduri. Societățile B, C și D integrează acest FOSS în propriile produse cu elemente digitale și contribuie în mod voluntar la întreținerea acestuia cu o parte din timpul dezvoltatorilor lor.

FOSS în cauză nu este considerat a fi introdus pe piață în înțelesul CRA. Societatea A nu este producătorul său, ci administratorul său. Societățile B, C și D trebuie să exercite diligența necesară în conformitate cu articolul 13 alineatul (5) atunci când integrează respectivul FOSS în propriile produse cu elemente digitale.

Exemplul 30: Întreprinderea A publică un FOSS sub numele sau marca sa și îl oferă ca versiune plătită, care include anumite beneficii, cum ar fi asistența tehnică sau optimizarea performanței. Dezvoltatorii din cadrul societăților B, C și D contribuie la întreținerea FOSS, dar acesta rămâne sub controlul societății A.

Societatea A este considerată producător al respectivului FOSS ([15]). Societățile B, C și D nu sunt supuse obligațiilor în temeiul CRA pentru respectivul FOSS. În cazul în care integrează respectivul FOSS în propriile produse cu elemente digitale, acestea au obligația de a exercita diligența necesară în conformitate cu articolul 13 alineatul (5).

Exemplul 31: Societatea A publică un FOSS sub numele sau marca sa și asigură întreținerea permanentă pentru a-i asigura viabilitatea pe termen lung, pentru a permite integrarea software-ului respectiv în produsele cu elemente digitale ale altor societăți. Societatea A nu percepe taxe pentru utilizarea sa, nu prelucrează datele cu caracter personal pe care le colectează prin intermediul produsului cu elemente digitale și nu vinde servicii de asistență asociate cu publicarea FOSS.

Societatea B contribuie cu codul și timpul dezvoltatorilor la întreținerea FOSS, dar nu îl distribuie din punct de vedere comercial. Societatea B oferă servicii de asistență tehnică independent de distribuția FOSS. Societatea A este considerată a fi administratorul respectivului FOSS, în timp ce societății B nu îi revin obligații în temeiul CRA pentru FOSS în cauză.

Exemplul 32: O componentă FOSS este publicată de o entitate non-profit înființată astfel încât să se asigure că toate veniturile după costuri sunt utilizate pentru a atinge obiective non-profit. Entitatea oferă asistență susținută pentru a asigura viabilitatea pe termen lung a proiectului. Întreținerea este finanțată din fonduri publice, cum ar fi granturile pentru cercetare. Evoluțiile suplimentare, inclusiv noile caracteristici, sunt finanțate prin donații și proiecte specifice, desfășurate în parteneriat cu producătorii care integrează FOSS respectiv în produsele lor cu elemente digitale. Astfel de caracteristici sunt încorporate în baza de cod a FOSS.

Entitatea non-profit care publică FOSS este considerată administratorul respectivei componente FOSS. Un producător care a contribuit la dezvoltarea anumitor caracteristici nu devine producătorul respectivei componente FOSS. În cazul în care producătorul integrează respectiva componentă FOSS în propriul produs cu elemente digitale, acesta trebuie să exercite diligența necesară în conformitate cu articolul 13 alineatul (5).

Exemplul 33: O entitate non-profit înființată astfel încât să se asigure că toate veniturile după costuri sunt utilizate pentru a atinge obiective non-profit publică un kit de dezvoltare de software FOSS (SDK) și asigură întreținerea continuă a acestuia. SDK este partajat în mod deschis și este disponibil tuturor în mod gratuit pentru a fi accesat, utilizat, modificat și redistribuit. Finanțarea este asigurată prin cotizațiile de membru plătite entității non-profit, iar dezvoltatorii angajați de organizațiile membre contribuie cu coduri și alte resurse la dezvoltarea SDK. Producătorii utilizează SDK ca o componentă pentru a construi alte produse cu elemente digitale.

Entitatea non-profit care publică SDK este administratorul respectivei componente. Membrii fundației nu sunt responsabili pentru respectarea CRA de către SDK. În cazul în care producătorii utilizează SDK pentru a-și construi propriul produs cu elemente digitale, aceștia trebuie să exercite diligența necesară în conformitate cu articolul 13 alineatul (5).

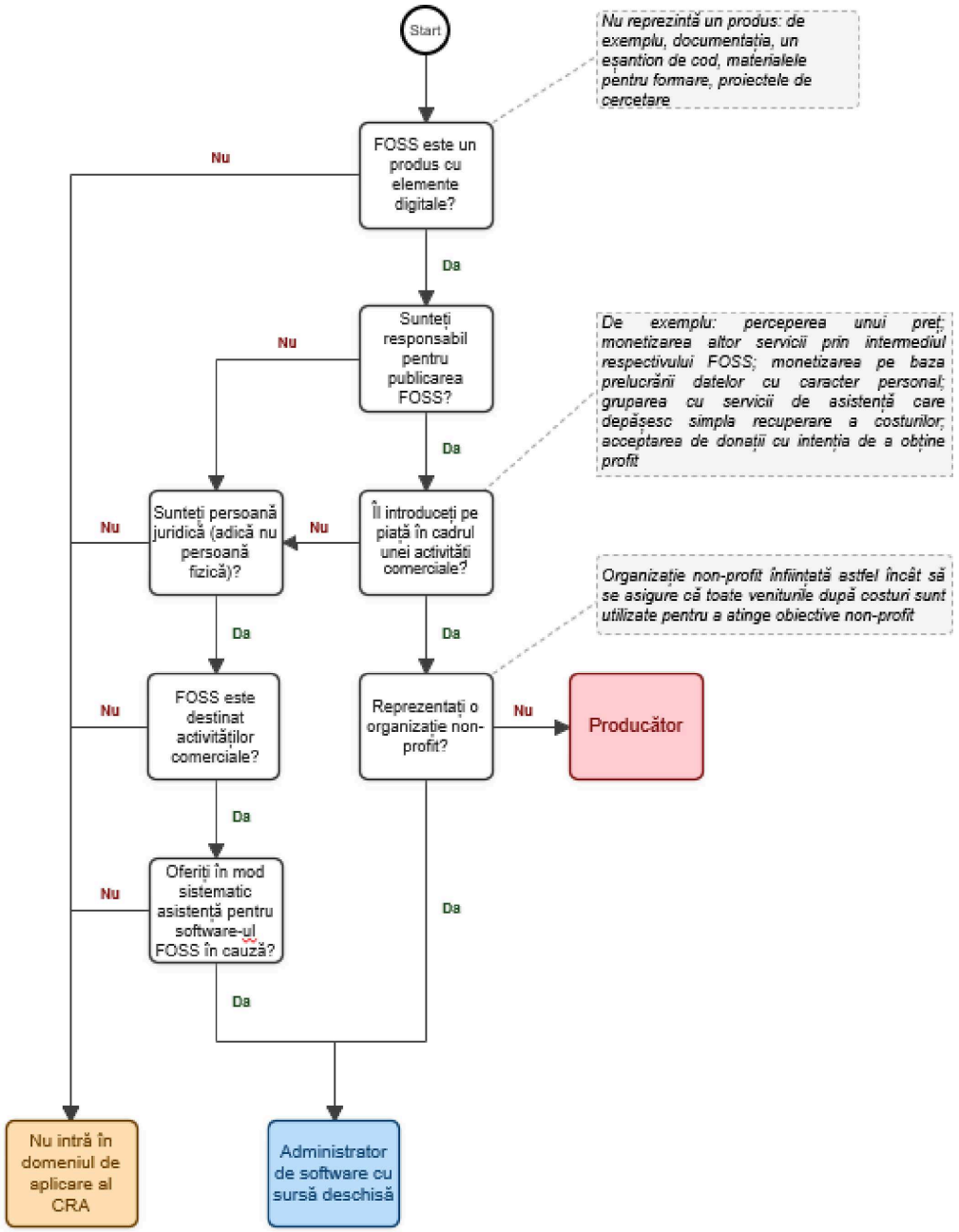
Exemplul 34: Un dezvoltator individual publică o bibliotecă FOSS într-un depozit public de pachete pentru un anumit limbaj de programare și o întreține în mod activ. În documentația pachetului, dezvoltatorul adaugă un link pentru colectarea donațiilor. Un producător descarcă gratuit biblioteca respectivă din depozit și o integrează în propriul produs cu elemente digitale.

Dezvoltatorul individual și depozitul de pachete nu au obligații în temeiul CRA. Producătorul care integrează biblioteca trebuie să exercite diligența necesară în conformitate cu articolul 13 alineatul (5).

([15]) Cu excepția cazului în care societatea A este o entitate non-profit înființată astfel încât să se asigure că toate veniturile după costuri sunt utilizate pentru a atinge obiective non-profit, caz în care ar fi administrator al FOSS respectiv.

Figura 1

Diagramă stilizată privind reglementarea de către CRA a software-ului liber și cu sursă deschisă



4. **MODIFICĂRI SUBSTANȚIALE ȘI PIESE DE SCHIMB**

90. Articolul 3 punctul 30 din CRA definește o „modificare substanțială” ca fiind o modificare a produsului cu elemente digitale în urma introducerii sale pe piață care (i) afectează conformitatea produsului cu elemente digitale cu cerințele esențiale prevăzute în anexa I partea I; sau (ii) care are ca rezultat o modificare a scopului preconizat pentru care a fost evaluat respectivul produs cu elemente digitale.

91. Noțiunea de modificare substanțială este relevantă pentru stabilirea obligațiilor CRA într-o serie de cazuri, inclusiv următoarele:

(a) în conformitate cu articolul 21, un importator sau un distribuitor care efectuează o modificare substanțială a unui produs cu elemente digitale deja introdus pe piață este considerat a fi producătorul său;

(b) în conformitate cu articolul 22, orice persoană fizică sau juridică ce efectuează o modificare substanțială a unui produs cu elemente digitale și îl pune la dispoziție pe piață este considerată producătorul acestuia;

(c) în conformitate cu articolul 69 alineatul (2), orice persoană fizică sau juridică ce efectuează o modificare substanțială după 11 decembrie 2027 a unui produs cu elemente digitale care a fost introdus pe piață înainte de 11 decembrie 2027 și îl introduce pe piață este considerată a fi producătorul acestuia;

(d) pentru producătorii de produse cu elemente digitale introduse pe piață după 11 decembrie 2027, pentru a stabili dacă un produs cu elemente digitale trebuie să facă obiectul unei noi proceduri de evaluare a conformității ca urmare a modificărilor efectuate după data respectivă, în special având în vedere caracterul iterativ al dezvoltării de software.

92. Prin urmare, este important să se ofere orientări pentru a ajuta operatorii economici să înțeleagă când se califică modificările hardware-ului sau software-ului drept modificări substanțiale.

4.1. **Reparații fizice**

93. Astfel cum se menționează la considerentul 42 din CRA, „atunci când un produs cu elemente digitale face obiectul «recondiționării», «întreținerii» și «reparării», în sensul definiției de la articolul 2 punctele 18, 19 și 20 din Regulamentul (UE) 2024/1781 al Parlamentului European și al Consiliului, acestea nu conduc neapărat la o modificare substanțială a produsului, de exemplu în cazul în care scopul și funcționalitățile preconizate nu sunt modificate, iar nivelul de risc rămâne neafectat. Cu toate acestea, modernizarea unui produs cu elemente digitale de către producător ar putea duce la modificări ale proiectării și dezvoltării produsului respectiv și ar putea afecta, prin urmare, scopul pentru care a fost conceput și conformitatea produsului cu cerințele stabilite în prezentul regulament”. Acest aspect este în concordanță cu secțiunea 2.1 din Ghidul albastru, care reamintește că „un produs care a făcut obiectul unor modificări importante sau al unor reparații generale după ce a fost pus în funcțiune trebuie considerat produs nou dacă: (i) se modifică performanța, destinația sau tipul original al acestuia, fără ca acest lucru să fie prevăzut în evaluarea inițială a riscurilor; (ii) natura pericolului s-a schimbat sau nivelul de risc a crescut în raport cu legislația de armonizare relevantă a Uniunii; și (iii) produsul este pus la dispoziție (sau pus în funcțiune dacă legislația aplicabilă reglementează și punerea în funcțiune în cadrul domeniului său de aplicare). Acest lucru trebuie evaluat pentru fiecare caz în parte și, în special, în funcție de obiectivul legislației și de tipul de produse vizate de legislația în cauză”.

94. Operațiunile de recondiționare, întreținere sau reparare care au ca rezultat modificări fizice ale produselor cu elemente digitale deja introduse pe piață nu constituie neapărat modificări substanțiale. Prin urmare, ar trebui efectuată o evaluare de la caz la caz pentru a stabili dacă o astfel de modificare fizică afectează conformitatea produsului cu elemente digitale cu cerințele esențiale prevăzute în anexa I partea I sau dacă are ca rezultat o modificare a scopului preconizat al produsului care face obiectul evaluării riscurilor în materie de securitate cibernetică.

95. Înlocuirea pieselor defecte sau a articolelor uzate cu piese care funcționează mai bine (de exemplu, pe fondul progresului tehnic sau deoarece vechea piesă nu mai este produsă) nu declanșează, în sine, o modificare substanțială a produsului reparat cu elemente digitale. Această situație survine numai dacă modificarea performanței sau modul în care funcționează produsul reparat cu elemente digitale (i) afectează conformitatea acestuia cu cerințele esențiale sau (ii) duce la o modificare a scopului preconizat care nu a fost vizată de evaluarea riscurilor.

Exemplul 35: Producătorul unui server efectuează o operațiune de reparare, înlocuind un RAM defect cu unul nou, mai performant. Conformitatea serverului cu cerințele esențiale nu este afectată. Funcționarea serverului este îmbunătățită, dar noua sa performanță se menține în cadrul utilizării preconizate a serverului, astfel cum se prevede în evaluarea riscurilor în materie de securitate cibernetică. Serverul nu este considerat a fi modificat în mod substanțial.

4.2. **Piese de schimb**

96. Articolul 2 alineatul (6) din CRA prevede că piesele de schimb destinate să înlocuiască componente identice și care sunt fabricate în conformitate cu aceleași specificații ca și componentele respective nu fac obiectul CRA. Considerentul 29 prevede, de asemenea, că exceptarea cuprinde atât piesele de schimb pentru produsele cu elemente digitale puse la dispoziție înainte de intrarea în vigoare a CRA, cât și piesele de schimb care au făcut deja obiectul unei proceduri de evaluare a conformității, astfel cum se prevede în regulament.

97. Exceptarea prevăzută la articolul 2 alineatul (6) din CRA ar trebui înțeleasă ca aplicându-se numai în cazul în care piesa de schimb este furnizată în mod specific pentru a repara sau a prelungi durabilitatea unui produs cu elemente digitale deja introdus pe piață (înainte sau după 11 decembrie 2027). În cazul în care un produs cu elemente digitale este furnizat ca produs de sine stătător, fără nicio legătură cu întreținerea sau repararea unui produs preexistent cu elemente digitale, acesta este introdus pe piață în sensul CRA și nu ar trebui să fie considerat o piesă de schimb care intră în domeniul de aplicare al articolului 2 alineatul (6). Scopul întreținerii sau al reparării ar trebui să reiasă în mod clar din contextul furnizării, de exemplu prin identificarea produsului cu elemente digitale sau a familiei de produse în comandă sau în oferta comercială sau prin furnizarea prin canale postvânzare sau de servicii. Dovezile justificative în acest sens ar trebui, de asemenea, să fie puse la dispoziția autorităților de supraveghere a pieței. Faptul că un produs cu elemente digitale ar putea fi utilizat din punct de vedere tehnic pentru a înlocui o componentă nu este, în sine, suficient pentru a-l include în domeniul de aplicare al exceptării în absența unor astfel de elemente.

98. În consecință, în cazul în care o piesă de schimb este identică cu o componentă deja inclusă într-un produs cu elemente digitale care fie a fost introdus pe piață înainte de data aplicării CRA, fie a fost introdus pe piață în conformitate cu CRA, piesa de schimb respectivă nu face ea însăși obiectul CRA.

99. Evaluarea măsurii în care o piesă de schimb ar trebui considerată identică cu o componentă ar trebui să se concentreze asupra rolului său funcțional în cadrul produsului cu elemente digitale și asupra caracteristicilor care pot fi relevante pentru securitatea cibernetică. Deși se impune întotdeauna o evaluare de la caz la caz, diferențele care nu afectează caracteristicile de securitate sau profilul de risc în materie de securitate cibernetică al componentei nu împiedică, în sine, ca piesa de schimb respectivă să intre sub incidența articolului 2 alineatul (6) din CRA.

100. În schimb, diferențele în ceea ce privește caracteristicile relevante pentru securitatea cibernetică a componentei, cum ar fi algoritmii, protocoalele, mecanismele criptografice, caracteristicile de control al accesului sau alte caracteristici relevante pentru securitate, pot însemna că noua piesă nu poate fi considerată identică cu componenta pe care este destinată să o înlocuiască.

101. În cazul în care o piesă de schimb nu este identică cu componenta originală, piesa de schimb respectivă constituie un produs cu elemente digitale de sine stătător și, prin urmare, face obiectul CRA. În astfel de cazuri, respectarea cerințelor esențiale trebuie evaluată în funcție de scopul preconizat al componentei de schimb. Deosebit de relevantă este funcția componentei de schimb de a asigura compatibilitatea sau interoperabilitatea cu un produs existent cu elemente digitale, inclusiv în cazul în care produsul respectiv este un produs cu elemente digitale introdus pe piață înainte de intrarea în vigoare a CRA. În cazul în care anumite cerințe esențiale nu pot fi îndeplinite în mod rezonabil din cauza scopului preconizat sau a constrângerilor tehnice, producătorul trebuie să reflecte acest aspect în evaluarea riscurilor în materie de securitate cibernetică și să pună în aplicare măsuri alternative sau compensatorii adecvate de atenuare a riscurilor, pentru a nu submina securitatea produsului cu elemente digitale. Astfel cum s-a discutat și în secțiunea *2.6 Sisteme complexe*, atât documentația tehnică, cât și informațiile și instrucțiunile pentru utilizator joacă un rol esențial în descrierea transparentă a constrângerilor identificate, a riscurilor de securitate cibernetică asociate și a măsurilor de atenuare a riscurilor puse în aplicare. Astfel cum s-a explicat în secțiunea *4.1 Reparații fizice*, înlocuirea pieselor defecte sau a articolelor uzate cu piese care funcționează mai bine nu declanșează, în sine, o modificare substanțială a produsului reparat cu elemente digitale.

Exemplul 36: Un producător a introdus controlere conectate pe piața UE. Într-un caz, controlerul a fost introdus pe piață în 2026, înainte de data aplicării CRA. Într-un alt caz, controlerul a fost introdus pe piață în 2028, în conformitate cu CRA. În 2028, un modul de comunicare digitală inclus în ambele tipuri de controlere nu mai funcționează. Producătorul furnizează ca piesă de schimb un modul de schimb care este identic și fabricat în conformitate cu aceleași specificații ca și originalul.

În ambele cazuri, modulul de schimb intră în domeniul de aplicare al excepțării prevăzute la articolul 2 alineatul (6). Piesa de schimb nu face în sine obiectul CRA, chiar dacă este un produs cu elemente digitale, deoarece înlocuiește o componentă identică dintr-un produs cu elemente digitale. Repararea nu constituie o modificare substanțială a produsului cu elemente digitale.

Exemplul 37: Un producător a introdus un controler industrial conectat pe piața UE în 2026, înainte de data aplicării CRA. În anul 2028, un cip de comunicare al acestui controler nu mai funcționează. Întrucât producătorul nu mai produce cipul respectiv, acesta furnizează ca piesă de schimb un cip mai nou cu funcționalitate echivalentă, dar cu o implementare criptografică diferită și cu un mecanism de boot securizat actualizat, pentru a menține compatibilitatea și funcționarea permanentă.

În acest caz, cipul de schimb nu poate fi considerat identic, deoarece diferențele în ceea ce privește implementarea criptografică și mecanismul de boot securizat afectează proprietățile de securitate cibernetică ale cipului. Prin urmare, acesta nu beneficiază de exceptarea prevăzută la articolul 2 alineatul (6) și constituie un produs cu elemente digitale care face obiectul CRA. Conformitatea piesei de schimb trebuie evaluată în funcție de scopul său preconizat, inclusiv de rolul său în asigurarea interoperabilității cu produsul cu elemente digitale introdus pe piață înainte de intrarea în vigoare a CRA.

Exemplul 38: Un producător introduce pe piață un controler pentru clădiri inteligente în 2028, în conformitate cu CRA. În 2029, modulul fără fir al acestui controler nu mai funcționează. Întrucât producătorul nu mai fabrică modulul respectiv, acesta furnizează ca piesă de schimb un modul nou care îndeplinește aceeași funcție utilizând aceleași protocoale de comunicare și mecanisme de securitate, dar se bazează pe un chipset diferit și beneficiază de firmware actualizat care nu aduce modificări caracteristicilor care pot avea caracter relevant pentru securitatea cibernetică.

În acest caz, modulul de schimb poate fi considerat identic. Prin urmare, modulul beneficiază de exceptarea prevăzută la articolul 2 alineatul (6) și nu face obiectul CRA.

102. Exceptarea pentru piesele de schimb se aplică indiferent dacă piesa de schimb înlocuiește o componentă din cadrul unui produs cu elemente digitale sau dacă înlocuiește un produs complet cu elemente digitale care, la rândul său, face parte dintr-un produs mai cuprinzător, inclusiv în cazul în care respectivul produs mai cuprinzător cu elemente digitale este compus din mai multe componente integrate, cu condiția ca piesa de schimb să fie furnizată în mod specific ca piesă de schimb, astfel cum se explică la punctele anterioare.

Exemplul 39: În 2027, un producător introduce pe piață un sistem pentru automatizări industriale care încorporează ca una dintre componentele sale un controler logic programabil (PLC). În 2031, unitatea centrală de procesare (CPU) a PLC nu mai funcționează. Producătorul oferă două opțiuni de reparare: (i) livrarea unei unități CPU de înlocuire, care poate fi considerată identică cu CPU instalată inițial; sau (ii) furnizarea unui PLC de înlocuire complet, care poate fi considerat identic cu PLC instalat inițial. În fiecare caz, înlocuirea este furnizată prin intermediul canalului de servicii postvânzare al producătorului ca piesă de schimb, iar sistemul pentru automatizări industriale vizat de înlocuire este identificat în mod clar. În ambele cazuri, înlocuirea intră în domeniul de aplicare al excepțării prevăzute la articolul 2 alineatul (6), indiferent dacă înlocuirea se referă la o componentă din cadrul PLC sau la PLC în ansamblu.

4.3. **Actualizări de software ca modificări substanțiale**

103. Dezvoltarea de software are un caracter iterativ, produsele software cu elemente digitale deja introduse pe piață fiind actualizate în mod frecvent și permanent. În acest context, este util să se ofere mai multe orientări pentru a stabili când trebuie să se considere că software-ul a fost modificat substanțial. Astfel de orientări sunt menite în special să ajute producătorii de produse software cu elemente digitale care aduc modificări propriilor produse să stabilească dacă modificările respective constituie o modificare substanțială.

104. Considerentul 39 indică faptul că un produs cu elemente digitale este modificat substanțial în cazul în care o modificare generează o schimbare a nivelului riscului în materie de securitate cibernetică și în cazul în care un astfel de risc modificat sau suplimentar nu a fost avut în vedere de producător în evaluarea riscurilor și, în consecință, în punerea în aplicare a cerințelor esențiale. Prin urmare, un producător ar trebui să evalueze, de la caz la caz, dacă o actualizare de software introduce riscuri noi sau sporite în materie de securitate cibernetică și dacă astfel de riscuri au fost deja abordate în evaluarea riscurilor.

105. În cazul în care un producător introduce noi funcționalități într-un produs cu elemente digitale care determină o modificare a scopului preconizat al produsului în ansamblu, este probabil ca producătorul să nu fi avut în vedere astfel de modificări în evaluarea riscurilor. În astfel de circumstanțe, modificarea s-ar califica, în general, drept modificare substanțială.

Exemplul 40: Un producător introduce pe piață un tablou de bord care colectează date de la mașini și afișează tendințele și alertele, fără a avea capacitatea de a controla astfel de mașini. Ulterior, producătorul dezvoltă o nouă versiune a tabloului de bord respectiv, introducând funcționalități care îi permit să controleze mașinile, inclusiv prin ajustarea parametrilor de funcționare și repornirea mașinilor în urma unor condiții de defecțiune. Ca urmare a acestor modificări, scopul preconizat al tabloului de bord a evoluat dincolo de ceea ce s-a prevăzut în evaluarea riscurilor, trecând de la un instrument de conștientizare a situației la un produs cu elemente digitale menit să exercite controlul operațional asupra altor dispozitive. Prin urmare, tabloul de bord a fost modificat substanțial.

Exemplul 41: Un producător introduce pe piață o aplicație software destinată consumatorilor, menită să organizeze și să afișeze date cu caracter personal, cum ar fi e-mailuri, mesaje sau documente, precum și să sprijine funcțiile de căutare și filtrare de bază. Ulterior, producătorul introduce o actualizare care permite aplicației să analizeze automat conținutul pentru utilizator pentru a genera profiluri comportamentale și pentru a lua decizii automatizate care afectează prioritizarea, eliminarea sau recomandarea conținutului fără intervenția utilizatorului. Ca urmare a acestei modificări, scopul preconizat al software-ului trece de la un instrument de gestionare a informațiilor controlat de utilizator la un sistem automatizat de luare a deciziilor, care nu a fost avut în vedere în evaluarea riscurilor. Prin urmare, cererea a fost modificată substanțial.

106. Totodată, este posibil totuși ca un producător să introducă treptat noi funcționalități deja incluse în evaluarea riscurilor sau care nu modifică, în sine, profilul de risc în materie de securitate cibernetică al produsului cu elemente digitale. Această situație poate surveni, de exemplu, în cazul în care producătorul a anticipat dezvoltarea funcționalităților respective, a descris și a evaluat deja riscurile asociate și a pus în aplicare măsuri de atenuare adecvate pentru a asigura respectarea în continuare a cerințelor esențiale. Această situație poate fi valabilă și în cazul în care noile funcționalități nu pun în aplicare modificări care introduc riscuri noi sau sporite. Prin urmare, actualizările de acest tip nu ar trebui considerate modificări substanțiale, deoarece nu sporesc riscul în materie de securitate cibernetică și, în consecință, nu modifică punerea în aplicare a cerințelor esențiale.

Exemplul 42: O aplicație de mesagerie este lansată inițial cu funcționalitate limitată la mesageria unu-la-unu. Evaluarea riscurilor efectuată de producător vizează introducerea ulterioară a mesageriei de grup, inclusiv, de exemplu, complexitatea sporită a rutării mesajelor. În cadrul unei actualizări ulterioare, producătorul adaugă o funcționalitate de conversație de grup împreună cu controale administrative și instrumente de moderare care au fost deja prevăzute și evaluate în proiectul inițial. Actualizarea pune în aplicare funcționalități care intră în domeniul de aplicare al scopului preconizat inițial și al evaluării riscurilor. Prin urmare, aplicația de mesagerie nu a fost modificată substanțial.

Exemplul 43: Un sistem de monitorizare a producției este introdus pe piață cu tablouri de bord care permit numai citirea, în timp ce funcțiile de control automatizat sunt prezente în arhitectura de sistem, dar rămân dezactivate. Evaluarea riscurilor efectuată de producător acoperă în mod explicit activarea viitoare a buclelor de control automat, inclusiv riscurile de securitate cibernetică asociate controlului în buclă închisă, precum și garanții, cum ar fi mecanismele de preluare a controlului de către operator și stările de autoprotecție. În cadrul unei actualizări ulterioare, producătorul permite funcțiile de control automat și activează garanțiile, astfel cum au fost evaluate inițial. Prin urmare, sistemul de monitorizare a producției nu a fost modificat în mod substanțial.

107. În schimb, chiar și noile funcționalități limitate sau aparent minore pot introduce riscuri semnificative în materie de securitate cibernetică care afectează conformitatea cu cerințele esențiale. Prin urmare, evaluarea modificării substanțiale nu ar trebui să se bazeze pe amploarea sau complexitatea modificării, ci pe potențialul său impact negativ asupra profilului de risc în materie de securitate cibernetică al produsului cu elemente digitale și, în consecință, pe punerea în aplicare a cerințelor esențiale.

Exemplul 44: Un producător introduce o actualizare a unei aplicații software adăugând o funcție de conectare de tip „remember me” (rămâi autentificat) sau permanentă care stochează tokenurile de autentificare la nivel local pentru a îmbunătăți confortul utilizatorului. Deși funcționalitatea are un domeniu de aplicare limitat, aceasta introduce noi riscuri (legate de furtul de tokenuri, accesul neautorizat și deturnarea sesiunilor) care nu au fost avute în vedere în evaluarea riscurilor. Prin urmare, actualizarea afectează conformitatea cu cerințele esențiale. Aplicația software a fost modificată substanțial.

Exemplul 45: Un producător adaugă o nouă caracteristică de conectare și diagnosticare la un produs software existent cu elemente digitale, permițând exportarea jurnalelor de sistem detaliate în scopul remedierii defecțiunilor tehnice. Deși funcționalitatea pare minoră, aceasta conduce la colectarea și stocarea datelor operaționale sensibile într-un format necriptat, introducând riscuri de expunere a datelor care nu au fost evaluate sau atenuate anterior. Prin urmare, modificarea poate avea un impact semnificativ asupra profilului de risc în materie de securitate cibernetică al produsului cu elemente digitale. Produsul software cu elemente digitale a fost modificat substanțial.

108. În conformitate cu considerentul 39 din CRA, actualizările de securitate nu trebuie considerate, în general, modificări substanțiale, deoarece scopul lor principal este de a reduce nivelul riscului în materie de securitate cibernetică asociat produsului cu elemente digitale. O actualizare de securitate care nu modifică scopul preconizat al produsului respectiv și nu introduce noi riscuri în materie de securitate cibernetică nu ar trebui, prin urmare, să fie considerată o modificare substanțială, chiar și în cazul în care actualizarea respectivă poate genera modificări semnificative de natură tehnică. Aceasta include cazurile în care anumite funcționalități sunt modificate sau limitate exclusiv în scopul atenuării vulnerabilităților identificate și al asigurării conformității în permanență cu cerințele esențiale.

Exemplul 46: Un producător implementează o actualizare de securitate pentru a aborda o vulnerabilitate în baza de cod a unui produs cu elemente digitale prin corectarea unei erori de validare a datelor de intrare care ar putea duce la o supraîncărcare a tamponului sau prin remedierea unei erori de logică ce permite evitarea autentificării prin validarea necorespunzătoare a tokenului de sesiune. Actualizarea modifică implementarea internă a software-ului fără a afecta scopul preconizat al produsului respectiv sau fără a introduce o nouă expunere. O astfel de actualizare este menită exclusiv să reducă riscul în materie de securitate cibernetică. Actualizarea de securitate nu ar trebui considerată o modificare substanțială.

Exemplul 47: Un producător introduce o actualizare de securitate care consolidează configurațiile de securitate existente, cum ar fi înăsprirea regulilor firewall, dezactivarea porturilor de rețea neutilizate, modificarea politicilor implicite privind parolele administratorilor sau impunerea obligativității autentificării multifactor în cazul în care o astfel de funcționalitate era deja disponibilă sau prevăzută. Deși actualizarea poate afecta modul în care utilizatorii configurează sau accesează produsul cu elemente digitale, aceasta nu modifică scopul preconizat al produsului și servește exclusiv la consolidarea poziției sale de securitate. Actualizarea de securitate nu ar trebui considerată o modificare substanțială.

Exemplul 48: Un producător introduce pe piață un produs software cu elemente digitale care asigură comunicațiile utilizând un cadru de criptare configurabil care permite algoritmi criptografici multipli și dimensiuni ale cheilor, astfel cum sunt descrise în documentația tehnică a produsului și în evaluarea riscurilor. Evaluarea riscurilor acoperă toate opțiunile criptografice furnizate în produsul cu elemente digitale și anticipează perimarea în viitor a anumitor algoritmi. Evaluarea riscurilor include, de asemenea, măsuri de atenuare, cum ar fi agilitatea criptografică, gestionarea cheilor interne și testarea compatibilității. Ca răspuns la orientările criptografice emergente, producătorul implementează o actualizare de securitate care dezactivează un algoritm perimat și activează o alternativă mai puternică, care se bucură deja de sprijin, fără a introduce noi dependențe externe sau a modifica fluxurile de date. Întrucât actualizarea pune în aplicare o măsură de securitate care a fost prevăzută și evaluată în contextul proiectării inițiale și nu introduce noi riscuri în materie de securitate cibernetică, actualizarea de securitate nu ar trebui considerată o modificare substanțială.

109. În schimb, o actualizare de securitate se poate califica drept modificare substanțială în cazul în care, în pofida obiectivului său de securitate, actualizarea are ca rezultat modificarea scopului preconizat al produsului cu elemente digitale dincolo de ceea ce a fost prevăzut inițial sau introduce riscuri noi sau sporite în materie de securitate cibernetică. Această situație poate surveni, de exemplu, în cazul în care o actualizare modifică în mod semnificativ limitele sau structura de dependență a produsului respectiv într-un mod care nu este prevăzut în evaluarea riscurilor, de exemplu prin modificarea semnificativă a fluxurilor de date sau prin adăugarea de noi interfețe accesibile din exterior.

Exemplul 49: Un producător introduce pe piață un produs software cu elemente digitale destinat să asigure criptarea locală a fișierelor pentru datele stocate pe dispozitivul unui utilizator, permițând utilizatorilor să cripteze și să decripteze fișiere la cerere. În urma descoperirii unei vulnerabilități în fluxul de lucru pentru criptare, producătorul implementează o actualizare de securitate care elimină funcționalitatea locală de criptare și, în schimb, impune ca toate fișierele să fie încărcate, stocate și prelucrate de un serviciu de criptare la distanță operat de producător. Ca urmare a acestei modificări, produsul cu elemente digitale nu mai efectuează criptarea locală astfel cum s-a prevăzut inițial, funcționând în schimb ca serviciu de criptare și de prelucrare a datelor la distanță. Deși actualizarea este introdusă din motive de securitate, aceasta modifică în mod fundamental scopul preconizat al produsului respectiv într-un mod care nu este prevăzut în evaluarea riscurilor și, prin urmare, se califică drept modificare substanțială.

Exemplul 50: Un producător introduce pe piață un produs software cu elemente digitale care se bazează pe un protocol de criptare stabilit și pe un ciclu de viață al cheilor gestionat intern pentru a securiza comunicațiile dintre componentele produsului cu elemente digitale. Ca răspuns la deficiențele criptografice nou identificate, producătorul introduce o actualizare de securitate care înlocuiește mecanismul de criptare existent cu un protocol diferit care impune utilizarea unui serviciu extern de gestionare a cheilor operat de o parte terță. Ca urmare a acestei modificări, dependențele și fluxurile de date ale produsului cu elemente digitale sunt modificate în mod semnificativ, introducând noi interfețe externe și bazându-se pe servicii furnizate de terți care nu sunt avute în vedere în evaluarea riscurilor. Deși actualizarea se bazează pe securitate, ea introduce noi riscuri în materie de securitate cibernetică și, prin urmare, se califică drept modificare substanțială.

110. Astfel cum s-a menționat la punctul 104 de mai sus, ar trebui să se evalueze de la caz la caz dacă o actualizare a software-ului constituie o modificare substanțială. Atunci când efectuează această evaluare, producătorii pot lua în considerare, în mod neexhaustiv, dacă actualizarea software-ului:

(a) introduce noi vectori de amenințare, cum ar fi interfețe suplimentare, canale de comunicare, medii de executare sau dependențe externe prin care amenințările s-ar putea materializa;

(b) permite noi scenarii de atac, inclusiv, de exemplu, noi moduri în care ar putea surveni în mod plauzibil accesul neautorizat, manipularea, interferența sau utilizarea abuzivă a produsului cu elemente digitale sau a datelor prelucrate de acesta;

(c) modifică probabilitatea unor scenarii de atac identificate anterior, de exemplu prin reducerea efortului sau a expertizei necesare pentru exploatarea acestora, prin creșterea expunerii la actori nedemni de încredere sau prin diminuarea garanțiilor existente;

(d) modifică impactul potențial al scenariilor de atac identificate anterior, inclusiv, de exemplu, domeniul de aplicare al datelor sau funcțiilor afectate, gravitatea consecințelor operaționale, economice sau în materie de siguranță, sau capacitatea de a detecta, de a limita un incident sau de a se redresa în urma unui incident.

111. În unele cazuri, o actualizare a software-ului nu introduce noi vectori de amenințare, nu permite noi scenarii de atac și nu modifică în mod semnificativ probabilitatea sau impactul scenariilor de atac identificate anterior. Acest lucru poate indica faptul că actualizarea nu introduce riscuri noi sau sporite în materie de securitate cibernetică, cu condiția ca ipotezele și măsurile de atenuare pe care se bazează evaluarea riscurilor să rămână valabile și eficace. Prin urmare, este probabil ca actualizarea să nu se califice drept modificare substanțială.

112. În schimb, o actualizare de software poate introduce noi vectori de amenințare, poate permite noi scenarii de atac sau poate modifica semnificativ probabilitatea sau impactul scenariilor de atac existente. În astfel de cazuri, producătorul ar trebui să reevalueze riscurile în materie de securitate cibernetică ale produsului cu elemente digitale și să stabilească dacă cerințele esențiale continuă să fie îndeplinite, inclusiv dacă actualizarea introduce riscuri noi sau sporite care nu sunt prevăzute în evaluarea riscurilor.

113. Actualizarea de software care se califică drept modificare substanțială are caracter relevant atunci când se stabilește dacă se aplică anumite obligații în temeiul CRA, astfel cum se prevede la punctul 91. Cu toate acestea, indiferent de calificarea respectivă, producătorii rămân responsabili de asigurarea securității actualizărilor de software și a produsului lor cu elemente digitale pe durata perioadei sale de asistență, în conformitate cu cerințele de gestionare a vulnerabilităților prevăzute în partea II din anexa I la CRA. În plus, indiferent dacă actualizările de software se califică sau nu drept modificări substanțiale, producătorii au obligația de a menține caracterul exact, complet și actualizat în permanență al evaluării riscurilor și al documentației tehnice, în conformitate cu articolul 13 alineatul (7) și cu articolul 31 alineatul (2).

4.4. **Consecințele unei modificări substanțiale**

114. Consecințele unei modificări substanțiale efectuate de un alt actor decât producătorul de origine al unui produs cu elemente digitale deja introdus pe piață sunt abordate la articolele 21 și 22 din CRA. Articolul 21 se referă la importatori și distribuitori, în timp ce articolul 22 se referă la orice persoană fizică sau juridică, alta decât producătorul, importatorul sau distribuitorul.

115. În cazul în care modificarea substanțială este efectuată de producătorul de origine al produsului cu elemente digitale, consecințele decurg din conceptul general stabilit de modificare substanțială menționat la considerentul 41 din CRA și sunt detaliate în secțiunea 2.1 din Ghidul albastru. Această secțiune prevede că un produs care a făcut obiectul unor modificări importante sau al unor reparații generale după ce a fost introdus pe piață trebuie considerat produs nou dacă se modifică performanța, destinația sau tipul original al acestuia, natura pericolului s-a schimbat sau nivelul de risc a crescut, iar produsul cu elemente digitale este pus la dispoziție pe piață.

116. Prin urmare, consecința general stabilită este că, în cazul în care o modificare a unui produs cu elemente digitale se califică drept modificare substanțială, iar produsul modificat cu elemente digitale este pus la dispoziție pe piață, acesta trebuie tratat ca un produs nou cu elemente digitale în sensul CRA. Prin urmare, punerea la dispoziție pe piață a produsului modificat substanțial constituie o nouă introducere pe piață. Acest lucru este valabil indiferent dacă modificarea substanțială este efectuată de producătorul de origine sau de o altă persoană. Pentru a asigura aplicarea CRA în mod uniform și proporțional la nivelul diverselor categorii de actori care pot efectua o modificare substanțială, următoarele subsecțiuni abordează obligațiile rezultate ale persoanei care efectuează modificarea substanțială atunci când produsul cu elemente digitale modificat substanțial este introdus pe piață. Consecințele pentru perioada de asistență a produsului cu elemente digitale sunt abordate în secțiunea *5 Perioada de asistență*.

4.4.1. *Modificări substanțiale efectuate de o altă persoană decât producătorul de origine*

117. În conformitate cu articolele 21 și 22, în cazul în care o modificare substanțială a unui produs cu elemente digitale deja introdus pe piață este efectuată de o altă persoană fizică sau juridică decât producătorul produsului cu elemente digitale, persoana care efectuează modificarea substanțială și pune la dispoziție pe piață produsul modificat cu elemente digitale trebuie considerată producătorul produsului modificat cu elemente digitale, indiferent dacă persoana respectivă a fost implicată în proiectarea inițială sau în introducerea pe piață a produsului respectiv.

118. Articolul 22 clarifică, de asemenea, faptul că persoana care efectuează modificarea este supusă obligațiilor prevăzute la articolele 13 și 14 numai în ceea ce privește partea produsului cu elemente digitale care este afectată de modificarea substanțială, în cazul în care modificarea respectivă nu are un impact asupra securității cibernetice a produsului cu elemente digitale în ansamblul său.

119. În cazul în care o modificare substanțială afectează conformitatea cu cerințele esențiale, dar nu afectează în mod negativ securitatea cibernetică a produsului cu elemente digitale în ansamblul său, persoanei care efectuează modificarea i se aplică articolul 13 (inclusiv obligația de a asigura conformitatea cu cerințele esențiale și de a efectua o procedură de evaluare a conformității) și articolul 14 (obligații de raportare) numai în ceea ce privește partea produsului cu elemente digitale care a fost modificată substanțial ([16]). În plus, obligațiile producătorului de origine în temeiul CRA continuă să se aplice produsului original cu elemente digitale introdus pe piață, asigurând continuitatea gestionării vulnerabilităților și conformitatea pentru piesele neschimbate.

120. Un caz de modificare substanțială nu ar trebui confundat cu cazurile de integrare, în care o persoană asamblează componente (inclusiv, după caz, prin modificarea acestora) într-un produs nou cu elemente digitale pe care îl introduce ea însăși pe piață. În astfel de cazuri, integratorul nu modifică un produs cu elemente digitale deja introdus pe piață de un alt producător; mai degrabă, acesta introduce pe piață un nou produs cu elemente digitale proprii. Integratorul este producătorul respectivului produs nou cu elemente digitale în scopul CRA și trebuie să respecte regulamentul în totalitate în ceea ce privește produsul cu elemente digitale în ansamblul său. În cazul în care producătorul integrează componente care fac obiectul CRA, acesta se poate baza pe activitățile de asigurare a conformității ale producătorilor de componente pentru a facilita conformitatea sa cu CRA.

Exemplul 51: O societate achiziționează module de microcontroler și componente de conectivitate gata de utilizare de la furnizori terți, dezvoltă firmware brevetat și un pachet de senzori și le asamblează într-un produs conectat de monitorizare a utilajelor agricole cu elemente digitale pe care îl introduce pe piață în nume propriu. Deși societatea a modificat modulele de microcontroler subiacente și le-a combinat cu alte componente, aceasta nu modifică în mod substanțial un produs cu elemente digitale deja introdus pe piață; mai degrabă, aceasta introduce pe piață un nou produs cu elemente digitale. Societatea este producătorul monitorului de utilaj agricol în sensul CRA și trebuie să respecte regulamentul în ceea ce privește monitorul de utilaj agricol în ansamblu.

([16]) În conformitate cu secțiunea 2.1 din Ghidul albastru, „nu este necesar să se repete teste sau să se întocmească noi documente pentru aspectele asupra cărora modificarea nu are efecte. Persoanei fizice sau juridice care modifică sau solicită modificarea produsului îi revine sarcina de a demonstra că nu toate elementele din documentația tehnică trebuie să facă obiectul unei actualizări. Persoanei fizice sau juridice care modifică sau solicită modificarea produsului este responsabilă pentru conformitatea produsului modificat și întocmește o declarație de conformitate, chiar dacă utilizează testele și documentația tehnică existente”.

121. În cazul în care o modificare substanțială efectuată de o altă persoană decât producătorul de origine afectează în mod negativ securitatea cibernetică a produsului cu elemente digitale în ansamblu, de exemplu deoarece modificarea nu mai vizează sau nu mai este limitată la o componentă specifică sau la un subsistem specific, produsul modificat cu elemente digitale pus la dispoziție pe piață ar trebui tratat ca un produs nou cu elemente digitale care face integral obiectul CRA. În astfel de cazuri, profilul general de risc în materie de securitate cibernetică al produsului respectiv se schimbă, iar modificarea nu poate fi evaluată fără a avea în vedere produsul cu elemente digitale în ansamblu. Persoana care efectuează modificarea este supusă obligațiilor unui producător prevăzute la articolele 13 și 14 în ceea ce privește produsul modificat cu elemente digitale în ansamblu.

4.4.2. *Modificări substanțiale efectuate de producătorul de origine*

122. În cazul în care modificarea substanțială este efectuată de producătorul de origine, inclusiv în contextul dezvoltării iterative de produse software cu elemente digitale, producătorul respectiv rămâne producător în sensul CRA. Cu toate acestea, produsul cu elemente digitale modificat substanțial trebuie considerat ca fiind nou introdus pe piață.

123. În conformitate cu secțiunea 2.1 din Ghidul albastru, producătorul de origine care introduce pe piață produsul cu elemente digitale modificat substanțial poate reutiliza documentele și testele existente pentru aspecte ale produsului cu elemente digitale asupra cărora modificarea substanțială nu are efecte. În special în cazul în care producătorul introduce pe piață versiuni modificate substanțial ale aceluiași produs cu elemente digitale, procedura de evaluare a conformității ar trebui să se concentreze asupra părților modificate substanțial ale produsului cu elemente digitale. În mod similar, în cazul în care se efectuează o evaluare a conformității de către o parte terță, organismul de evaluare a conformității ar trebui să își concentreze evaluarea asupra părților modificate substanțial. Pentru piesele neschimbate ale produsului cu elemente digitale, acesta poate reutiliza documentele existente și rezultatele testelor.

124. Considerentele privind proporționalitatea prevăzute în subsecțiunea anterioară se aplică în egală măsură modificărilor substanțiale efectuate de producătorul de origine al unui produs cu elemente digitale introdus pe piață înainte de 11 decembrie 2027. O astfel de modificare substanțială efectuată de producătorul de origine nu impune, în sine, producătorului să aducă întregul produs cu elemente digitale introdus pe piață înainte de data respectivă în deplină conformitate cu CRA, cu excepția cazului în care modificarea afectează în mod negativ securitatea cibernetică a produsului cu elemente digitale în ansamblu. În cazul în care modificarea nu afectează securitatea cibernetică a produsului cu elemente digitale în ansamblu, obligațiile producătorului de origine în ceea ce privește modificarea ar trebui să se limiteze la piesele modificate substanțial.

5. **PERIOADA DE ASISTENȚĂ**

125. Articolul 13 alineatul (8) din CRA prevede obligația producătorilor de a stabili perioada de asistență în care vulnerabilitățile produsului cu elemente digitale, inclusiv ale componentelor sale, sunt gestionate în mod eficace și în conformitate cu cerințele esențiale prevăzute în anexa I partea II. Perioada de asistență reflectă perioada de timp în care se preconizează că produsul cu elemente digitale va fi în uz (durata de utilizare preconizată) și ar trebui să fie stabilit ținând seama de criteriile prevăzute la articolul 13 alineatul (8), în special de așteptările rezonabile ale utilizatorilor, de natura produsului cu elemente digitale, inclusiv de scopul său preconizat, precum și de dreptul relevant al Uniunii care stabilește durata de viață a produselor cu elemente digitale ([17]). În general, astfel de criterii trebuie avute în vedere într-un mod care să asigure proporționalitatea în contextul stabilirii perioadei de asistență.

([17]) Criteriile suplimentare care pot fi luate în considerare, în conformitate cu articolul 13 alineatul (8), includ perioadele de asistență aferente produselor cu elemente digitale care oferă o funcționalitate similară introduse pe piață de alți producători, disponibilitatea mediului de operare, perioadele de asistență aferente componentelor integrate care oferă funcții de bază și care sunt furnizate de părți terțe, precum și orientările relevante furnizate de grupul de cooperare administrativă (ADCO) instituit în temeiul CRA și de către Comisie.

126. Articolul 13 alineatul (8) prevede, de asemenea, ca perioada de asistență să fie de cel puțin cinci ani, cu excepția cazului în care se preconizează că produsul cu elemente digitale va fi utilizat mai puțin de cinci ani, caz în care perioada de asistență corespunde duratei de utilizare preconizate. Prin urmare, perioada minimă de asistență funcționează numai ca o garanție, asigurându-se că vulnerabilitățile sunt gestionate pentru o perioadă suficient de lungă, permițând în același timp producătorilor să ia în considerare produsele cu elemente digitale în cazul cărora duratele de utilizare preconizate sunt cu adevărat mai scurte. Considerentul 60 oferă mai multe orientări în acest sens, clarificând faptul că produsele cu elemente digitale despre care se preconizează în mod rezonabil că vor fi utilizate mai mult de cinci ani ar trebui, în consecință, să beneficieze de perioade de asistență mai lungi. Prin urmare, o perioadă de asistență de cinci ani nu trebuie considerată implicită pentru toate produsele cu elemente digitale. În schimb, producătorul ar trebui să stabilească perioada de asistență adecvată în lumina criteriilor menționate la articolul 13 alineatul (8).

127. Articolul 13 alineatul (19) prevede obligația producătorilor de a indica, la momentul achiziției, în mod clar și inteligibil, data de încheiere a perioadei de asistență (cel puțin luna și anul). De asemenea, impune producătorilor să afișeze o notificare adresată utilizatorilor după expirarea perioadei de asistență, în cazul în care acest lucru este fezabil din punct de vedere tehnic, având în vedere natura produsului cu elemente digitale. Această obligație este menită să ofere transparență utilizatorilor în ceea ce privește durata preconizată pentru asistență în materie de securitate.

128. În cazul produselor software cu elemente digitale, care sunt adesea dezvoltate și lansate iterativ și în cazul cărora versiuni modificate substanțial pot fi introduse pe piață în mod frecvent de-a lungul timpului, perioada de asistență trebuie înțeleasă în lumina acestui model de dezvoltare. Fiecare versiune modificată substanțial a unui produs software cu elemente digitale introdus pe piață trebuie să beneficieze de o perioadă de asistență declarată care să fie în conformitate cu articolul 13 alineatul (8). Aceasta include perioada minimă de asistență de cel puțin cinci ani, cu excepția cazului în care se poate demonstra că durata de utilizare preconizată a versiunii respective este mai scurtă, astfel cum se clarifică și la considerentul 60. Secțiunea *5.1 Modificări substanțiale și perioada de asistență* clarifică, de asemenea, faptul că, în cazul în care modificarea substanțială nu conduce la modificări ale factorilor care au determinat inițial durata de utilizare preconizată a produsului cu elemente digitale, perioada de asistență inițială nu este afectată (și anume inclusiv în cazurile în care perioada de asistență rămasă este mai mică de cinci ani).

129. Articolul 13 alineatul (10) oferă flexibilitate pentru produsele software cu elemente digitale, permițând producătorilor, în anumite condiții, să asigure conformitatea cu cerința de gestionare a vulnerabilităților prevăzută în partea II punctul 2 din anexa I (abordarea și remedierea vulnerabilităților) numai pentru versiunea produsului software cu elemente digitale introdusă ultima dată pe piață. Acest fapt este permis în cazul în care utilizatorii versiunilor introduse anterior au acces gratuit la ultima versiune introdusă pe piață și nu suportă costuri suplimentare pentru a ajusta echipamentele hardware și programele software în care utilizează versiunea originală a produsului respectiv.

130. În sensul articolului 13 alineatul (10), conceptul de „costuri suplimentare” ar trebui interpretat în mod practic și proporțional, ținând seama de practicile normale și preconizate în ceea ce privește întreținerea și exploatarea software-ului. Acesta nu include efortul operațional rezonabil care este inerent aplicării actualizărilor de software sau menținerii unui mediu de operare securizat, cum ar fi timpul de lucru al personalului, testarea de rutină, ajustările configurației sau actualizările dependențelor de software subiacente care sunt necesare pentru a aborda componentele scoase din uz sau vulnerabilitățile de securitate cunoscute. În schimb, „costurile suplimentare” se referă la sarcini care depășesc așteptările normale în contextul actualizărilor de software, cum ar fi achizițiile obligatorii de echipamente hardware noi, înlocuirea infrastructurii sau modificări fundamentale ale mediului de operare.

131. În cazul produselor software cu elemente digitale care evoluează permanent, producătorii pot introduce pe piață versiuni succesive modificate substanțial la intervale relativ scurte și pot solicita utilizatorilor să efectueze periodic actualizări. În astfel de cazuri, perioada de asistență declarată pentru fiecare versiune modificată substanțial trebuie să respecte articolul 13 alineatul (8) în momentul introducerii pe piață. Cu alte cuvinte, producătorul trebuie să declare o nouă perioadă de asistență pentru respectiva versiune modificată substanțial. Cu toate acestea, producătorii se pot întemeia pe articolul 13 alineatul (10) pentru a înceta abordarea și remedierea vulnerabilităților în ceea ce privește versiunile anterioare odată ce utilizatorii sunt în măsură să treacă gratuit la o versiune ulterioară

și fără a li se imputa costuri suplimentare, astfel cum se menționează mai sus, chiar dacă aceasta determină o perioadă de asistență efectivă mai scurtă pentru versiunile anterioare respective ([18]). Producătorul se supune în continuare celorlalte cerințe de gestionare a vulnerabilităților prevăzute în anexa I partea II, precum și obligațiilor de raportare prevăzute la articolul 14. Astfel cum se explică și la considerentul 40, aceste cerințe includ, printre altele, pentru toate versiunile ulterioare modificate substanțial ale produsului software cu elemente digitale introdus pe piață: (i) menținerea unei politici privind divulgarea coordonată a vulnerabilităților și (ii) măsuri de facilitare a schimbului de informații cu privire la potențialele vulnerabilități ([19]).

Exemplul 52: Un producător introduce un model de telefon inteligent pe piața UE și declară o perioadă de asistență de X ani de la data introducerii pe piață, în cursul căreia va furniza actualizări de securitate care să abordeze vulnerabilitățile. În perioada respectivă, producătorul pune la dispoziție actualizări periodice ale software-ului și versiuni modificate substanțial ale sistemului de operare, pe care utilizatorii le pot instala gratuit fără a avea nevoie de echipament hardware nou.

În conformitate cu articolul 13 alineatul (10), producătorul poate aborda și remedia vulnerabilitățile pentru cea mai recentă versiune a sistemului de operare pusă la dispoziție pentru modelul de telefon inteligent respectiv, cu condiția ca versiunile anterioare să poată fi actualizate gratuit și fără costuri suplimentare. Pe durata perioadei de asistență, producătorul se supune în continuare celorlalte cerințe de gestionare a vulnerabilităților, cum ar fi măsurile de divulgare coordonată a vulnerabilităților și de schimb de informații.

Exemplul 53: Un producător introduce pe piață un produs software cu elemente digitale utilizat în întreprinderi și lansează versiuni modificate substanțial o dată la câteva luni, reflectând îmbunătățirile în materie de securitate, noile caracteristici și compatibilitatea cu platformele și sistemele de operare actualizate. Fiecare versiune este introdusă pe piață cu o perioadă de asistență declarată în conformitate cu articolul 13 alineatul (8). Producătorul solicită utilizatorilor să efectueze actualizări în mod regulat în contextul funcționării normale și oferă acces gratuit la cea mai recentă versiune. Implementarea actualizărilor poate necesita un efort operațional rezonabil, cum ar fi testări și ajustări ale configurației, însă nu presupune costuri suplimentare, cum ar fi achiziționarea de echipament hardware nou sau modificări fundamentale la nivel de infrastructură. În acest context, producătorul se poate întemeia pe articolul 13 alineatul (10) pentru a înceta abordarea și remedierea vulnerabilităților aferente versiunilor anterioare odată ce utilizatorii pot trece la cea mai recentă versiune, respectând totodată în continuare celelalte cerințe de gestionare a vulnerabilităților pentru toate versiunile ulterioare modificate substanțial.

5.1. **Modificări substanțiale și perioada de asistență**

132. Astfel cum se prevede în secțiunea 4.4 *Consecințele unei modificări substanțiale*, în cazul în care o modificare a unui produs cu elemente digitale se califică drept modificare substanțială, iar produsul modificat cu elemente digitale este pus la dispoziție pe piață, acesta trebuie tratat ca un produs nou în sensul CRA, iar acțiunea de a pune la dispoziție pe piață produsul cu elemente digitale modificat substanțial constituie o nouă introducere pe piață. Prin urmare, este util să se clarifice efectul pe care această nouă introducere pe piață îl are asupra perioadei de asistență aferentă produsului cu elemente digitale modificat substanțial.

133. Perioada de asistență aferentă unui produs cu elemente digitale modificat substanțial ar trebui stabilită în funcție de durata de utilizare preconizată a produsului respectiv, având în vedere criteriile prevăzute la articolul 13 alineatul (8) din CRA. Prin urmare, o modificare substanțială ar trebui să presupună o reevaluare în raport cu criteriile respective, dar nu conduce în mod automat la resetarea sau chiar la prelungirea perioadei de asistență. Întrebarea relevantă este dacă modificarea substanțială afectează factorii care au determinat inițial durata de utilizare preconizată a produsului respectiv și, prin urmare, perioada de asistență inițială.

([18]) Ar trebui reamintit faptul că articolul 13 alineatul (19) prevede, în cazul în care acest lucru este fezabil din punct de vedere tehnic, având în vedere natura produsului cu elemente digitale, obligația producătorilor de a afișa o notificare adresată utilizatorilor prin care îi informează că produsul lor cu elemente digitale a ajuns la sfârșitul perioadei sale de asistență. Prin urmare, în cazul în care abordarea și remedierea vulnerabilităților pentru versiunile anterioare încetează, se preconizează că utilizatorii care nu au trecut la cea mai nouă versiune sunt informați, dacă acest lucru este fezabil din punct de vedere tehnic.

([19]) Ar trebui remarcat faptul că, în cazul în care utilizatorii pot trece la cea mai recentă versiune a software-ului fără costuri suplimentare, producătorii pot alege totuși să abordeze și să remedieze în continuare vulnerabilitățile aferente versiunilor anterioare ale software-ului respectiv, inclusiv în schimbul unei plăți sau în temeiul altor acorduri comerciale. CRA nu prevede obligația producătorilor de a furniza gratuit actualizări de securitate pentru astfel de versiuni anterioare.

134. În cazul în care modificarea substanțială nu afectează factorii respectivi, criteriile prevăzute la articolul 13 alineatul (8) indică în continuare aceeași durată de utilizare preconizată ca cea stabilită inițial, iar perioada de asistență a produsului cu elemente digitale modificat ar trebui să se alinieze la durata rămasă de utilizare preconizată a produsului, astfel cum a fost introdus inițial pe piață. Această situație va surveni, de regulă, în cazul în care durata de utilizare preconizată este determinată în principal de factori pe care modificarea nu îi afectează, cum ar fi durabilitatea fizică a componentelor hardware, în cazul în care modificarea substanțială vizează exclusiv funcționalitatea software sau serviciile *back-end*.

Exemplul 54: Un producător introduce pe piață un aspirator robot având o durată de utilizare preconizată de X ani, stabilită în funcție de natura produsului cu elemente digitale, inclusiv durabilitatea fizică și caracteristicile de uzură ale componentelor hardware, precum și ținând seama de așteptările rezonabile ale utilizatorilor cu privire la durata de viață a produsului respectiv. Producătorul stabilește o perioadă de asistență de X ani. După Y ani, producătorul lansează o actualizare de software care se califică drept modificare substanțială, adăugând noi moduri de curățare și caracteristici de orientare. Actualizarea de software nu afectează durabilitatea fizică a hardware-ului și nu modifică așteptările rezonabile ale utilizatorilor cu privire la durata de viață a produsului respectiv. Prin urmare, criteriile prevăzute la articolul 13 alineatul (8) indică în continuare aceeași durată de utilizare preconizată. Perioada de asistență a produsului cu elemente digitale modificat se aliniază la durata rămasă de utilizare preconizată, astfel cum s-a stabilit inițial.

Exemplul 55: Un producător introduce pe piață un produs complex asimilat utilajelor industriale, cu elemente digitale, având un sistem back-end de tip cloud care constituie o soluție de prelucrare a datelor la distanță. Durata de utilizare preconizată este de X ani, stabilită având în vedere așteptările rezonabile ale utilizatorilor și natura produsului cu elemente digitale, cum ar fi durabilitatea fizică a hardware-ului utilajului și uzura preconizată. Perioada de asistență este stabilită pentru a se alinia la durata de utilizare preconizată de X ani. După Y ani, producătorul restructurează sistemul back-end de tip cloud (soluția de prelucrare a datelor la distanță), introducând noi API și fluxuri de date, într-un mod care se califică drept o modificare substanțială a produsului cu elemente digitale, dar care nu modifică natura produsului respectiv și nu afectează așteptările utilizatorilor. Prin urmare, criteriile prevăzute la articolul 13 alineatul (8) indică în continuare aceeași durată de utilizare preconizată. Perioada de asistență a produsului cu elemente digitale modificat se aliniază la durata rămasă de utilizare preconizată, astfel cum s-a stabilit inițial.

135. În cazul în care modificarea substanțială afectează factorii care au determinat inițial durata de utilizare preconizată a produsului cu elemente digitale, producătorul ar trebui să recalculeze perioada de asistență pentru a reflecta noua durată de utilizare preconizată, aplicând în consecință criteriile prevăzute la articolul 13 alineatul (8). Acesta poate fi cazul, de exemplu, al revitalizării modificărilor hardware-ului care prelungesc durata de viață operațională a produsului respectiv sau al unei reprogramări sau rescrieri substanțiale a software-ului de bază al produsului respectiv care modifică în mod semnificativ durata de utilizare preconizată a acestuia ([20]).

Exemplul 56: Un producător introduce pe piață un controler logic programabil (PLC) având o durată de utilizare preconizată de X ani, stabilită în principal în funcție de natura produsului cu elemente digitale și de durabilitatea echipamentului hardware subiacent. Perioada de asistență este stabilită în consecință. La câțiva ani de la introducerea inițială pe piață, producătorul efectuează o modificare substanțială constând în înlocuirea platformei informatice integrate a PLC, inclusiv a procesorului, a memoriei și a mediului de funcționare, cu o nouă generație de componente concepute pentru o durată de viață operațională semnificativ mai lungă. Ca urmare a modificării, așteptările rezonabile ale utilizatorilor și natura produsului cu elemente digitale se modifică: utilizatorul PLC se poate aștepta acum în mod rezonabil ca PLC să rămână în circuitul utilizării productive dincolo de durata sa de utilizare preconizată declarată inițial, având ca suport noua platformă de calcul. Prin urmare, criteriile prevăzute la articolul 13 alineatul (8) indică o durată de utilizare preconizată mai lungă, iar producătorul recalculează în consecință perioada de asistență pentru PLC specific în cauză.

6. **PRODUSE IMPORTANTE ȘI CRITICE CU ELEMENTE DIGITALE**

136. Articolul 7 alineatul (1) din CRA stabilește că produsele cu elemente digitale care au funcționalitatea de bază a unei categorii de produse prevăzute în anexa III la regulament sunt considerate „produse importante cu elemente digitale”. Anexa III împarte în continuare produsele importante cu elemente digitale în clasele I și II. În mod similar, articolul 8 alineatul (1) stabilește că produsele cu elemente digitale care au funcționalitatea de bază a unei categorii de produse prevăzute în anexa IV la CRA sunt considerate „produse critice cu elemente digitale” ([21]).

([20]) Ar trebui reamintit faptul că, astfel cum se indică în secțiunea *4.1 Reparații fizice*, operațiunile de recondiționare, întreținere sau reparare nu sunt considerate, în general, modificări substanțiale.

([21]) Regulamentul de punere în aplicare (UE) 2025/2392 al Comisiei stabilește descrierea tehnică a categoriilor de produse importante și critice.

137. Clasificarea unui produs cu elemente digitale ca fiind important sau critic sau, dimpotrivă, ca aparținând categoriei „implicite” ([22]) este relevantă pentru stabilirea procedurii de evaluare a conformității pe care producătorul trebuie să o urmeze, în conformitate cu articolul 32, înainte de a putea introduce pe piață respectivul produs cu elemente digitale. În special, produsele cu elemente digitale din categoria implicită se pot întemeia întotdeauna pe procedura de control intern bazată pe modulul A („autoevaluare”) ([23]). Produsele importante cu elemente digitale din clasa I sau II și produsele critice cu elemente digitale fac obiectul unor proceduri mai stricte de evaluare a conformității. Aceasta nu include produsele importante cu elemente digitale din clasa I sau II care se califică drept software liber și cu sursă deschisă care sunt introduse pe piață, pentru care, în conformitate cu articolul 32 alineatul (5), producătorilor li se permite să urmeze procedurile aferente categoriei implicite.

138. Conceptul de funcționalitate de bază este, prin urmare, esențial pentru ca producătorul să stabilească regimul aplicabil de evaluare a conformității. Totuși, acest concept nu este definit în mod explicit în CRA. Produsele cu elemente digitale pot îndeplini o serie de funcții, dintre care unele pot fi auxiliare funcționalității de bază a produsului respectiv, și nu ar trebui să afecteze clasificarea produsului ca implicit/important din clasa I/important din clasa II/critic. Prin urmare, este util să se ofere mai multe orientări pentru a ajuta producătorii să efectueze în mod corect procedurile relevante de evaluare a conformității și pentru a ajuta autoritățile de supraveghere a pieței să asigure aplicarea armonizată a CRA în întreaga UE.

6.1. **Funcționalitatea de bază**

139. Funcționalitatea de bază a unui produs cu elemente digitale se referă la principalele caracteristici și capacități tehnice ale produsului respectiv, fără de care acesta nu ar fi în măsură să își îndeplinească scopul preconizat. Aceasta poate fi evaluată având în vedere contextul și condițiile de utilizare specifice ale produsului respectiv, ținând seama, printre altele, de informațiile pe care producătorul le furnizează în instrucțiunile de utilizare, în materialele promoționale sau de vânzare și în declarații, precum și în documentația tehnică.

Exemplul 57: Un produs software cu elemente digitale oferă un strat de abstractizare peste echipamentul hardware subiacent și gestionează execuția componentelor software. Principalele sale caracteristici includ inițializarea componentelor hardware și periferice, gestionarea proceselor și a memoriilor, controlul intrărilor și al ieșirilor, programarea, alocarea resurselor și expunerea serviciilor sistemului și a interfețelor de programare a aplicațiilor (API) prin care aplicațiile interacționează cu resursele hardware și software ale dispozitivului. Documentația tehnică indică faptul că produsul cu elemente digitale orchestrează resursele informatice, pune în aplicare configurațiile sistemului și oferă interfețe standardizate pentru modulele software și echipamentele periferice conectate. Producătorul subliniază că aceste capacități permit platformei să servească drept mediu software centralizat pe care aplicațiile pot funcționa în mod fiabil. Produsul cu elemente digitale are funcționalitatea de bază a unui sistem de operare, astfel cum se descrie la punctul 11 din anexa I la Regulamentul de punere în aplicare (UE) 2025/2392.

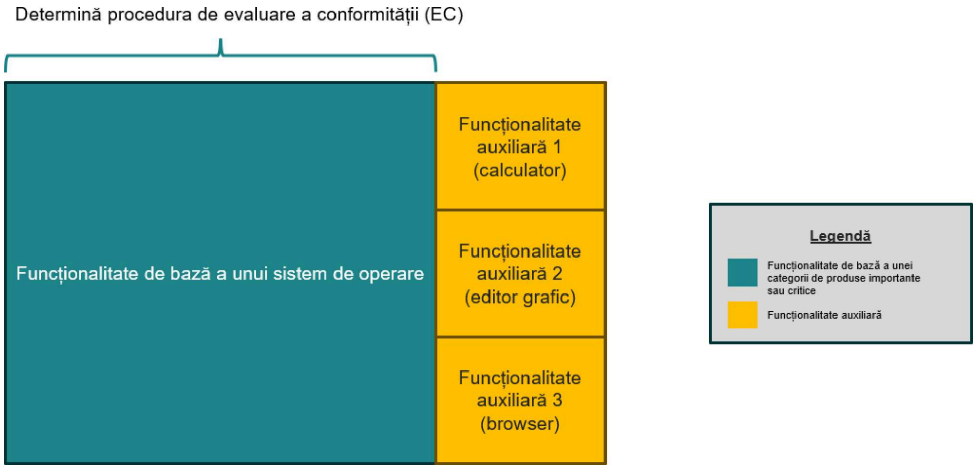
140. Funcționalitatea unui produs cu elemente digitale este rareori limitată exclusiv la funcționalitatea sa de bază, deoarece produsele cu elemente digitale îndeplinesc adesea – dacă nu întotdeauna – funcții suplimentare care nu contribuie la funcționalitatea de bază a produsului. Aceasta poate include, de asemenea, încorporarea unor componente care au ele însele funcționalitatea unui alt produs important sau critic cu elemente digitale. Cu toate acestea, faptul că un produs cu elemente digitale îndeplinește alte funcții decât cele detaliate în descrierile tehnice ale produselor importante sau critice cu elemente digitale sau funcții suplimentare față de acestea nu împiedică, în sine, produsul să aibă o astfel de funcționalitate de bază.

([22]) Termenul categorie „implicită” nu este un termen definit în CRA. Utilizarea termenului în prezentul document se referă la produsele cu elemente digitale care nu au funcționalitatea de bază a unei categorii de produse prevăzute în anexele III sau IV la CRA și care, în consecință, fac obiectul regimului de evaluare a conformității prevăzut la articolul 32 alineatul (1).

([23]) Cu toate acestea, producătorul poate alege întotdeauna să aplice o procedură mai strictă de evaluare a conformității, astfel cum se prevede la articolul 32 alineatul (1).

Figura 2

Ilustrarea modului în care funcționalitatea de bază, și nu funcționalitățile auxiliare, determină procedura aplicabilă de evaluare a conformității



141. Un produs cu elemente digitale poate avea capacitatea de a îndeplini funcțiile unei categorii de produse importante sau critice, dar are totuși o funcționalitate de bază diferită de cea a unei astfel de categorii de produse. În aceste cazuri, produsul cu elemente digitale nu s-ar califica drept un produs important sau critic cu elemente digitale. Astfel cum se menționează în mod explicit la articolul 7 alineatul (1) din CRA în ceea ce privește produsele importante cu elemente digitale (și aplicând aceeași logică pentru produsele critice cu elemente digitale), simpla integrare a unui produs important sau critic cu elemente digitale nu implică, în sine, faptul că produsul cu elemente digitale este un produs important sau critic cu elemente digitale.

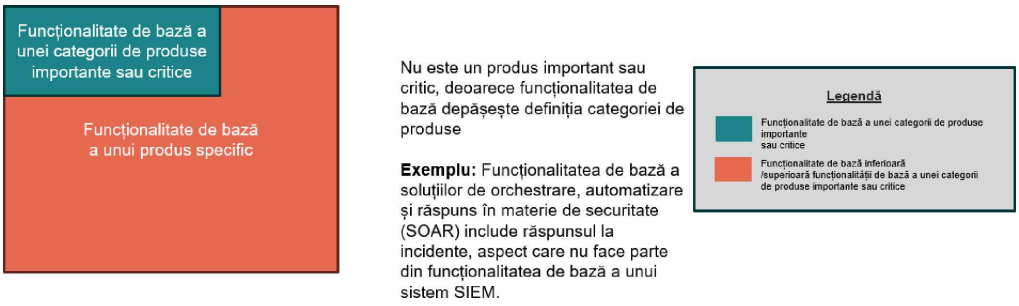
Exemplul 58: Un telefon inteligent integrează un sistem de operare care oferă funcționalitățile descrise la punctul 11 din anexa I la Regulamentul de punere în aplicare (UE) 2025/2392. În timp ce sistemul de operare permite gestionarea resurselor hardware și executarea aplicațiilor software, telefonul inteligent în ansamblu are o funcționalitate de bază diferită (de exemplu, aceea de a permite utilizatorilor să comunice și să acceseze informații și servicii). Simpla integrare a unui sistem de operare nu înseamnă că telefonul inteligent are funcționalitatea de bază a unui sistem de operare.

142. Unele produse cu elemente digitale pot fi asimilate unei categorii de produse importante sau critice sau pot aparține aceleiași familii de produse generale, însă funcționalitatea lor de bază poate depăși substanțial sau poate fi în mod considerabil inferioară funcționalității de bază a categoriei respective. Acest lucru nu este valabil în cazul în care un produs cu elemente digitale include funcționalități suplimentare care doar completează sau îmbunătățesc funcționalitatea de bază, care, la rândul său, corespunde celei a unei categorii de produse importante sau critice; în astfel de cazuri, produsul cu elemente digitale păstrează funcționalitatea de bază a categoriei respective și este clasificat în consecință. Această evaluare ar trebui să se bazeze pe principalele caracteristici și capacități tehnice ale produsului respectiv, avute în vedere în mod obiectiv din perspectiva scopului său preconizat, și nu pe modul în care este descris sau comercializat produsul cu elemente digitale, în cazul în care descrierea respectivă nu reflectă caracteristicile tehnice reale ale produsului.

Exemplul 59: Un software de orchestrare, automatizare și răspuns în materie de securitate (security orchestration, automation and response – SOAR) are adesea capacitatea de a îndeplini funcțiile produselor cu elemente digitale din categoria „sisteme de gestionare a informațiilor de securitate și a evenimentelor de securitate (SIEM)”, și anume de a colecta date din surse multiple, de a analiza și corela datele respective și de a le prezenta ca informații care pot fi puse în aplicare în scopuri legate de securitate. Cu toate acestea, funcționalitatea de bază a software-ului o depășește în mod substanțial pe cea a unui SIEM, incluzând servicii precum intervenția în caz de incidente ca elemente esențiale ale capacităților sale tehnice. Prin urmare, se consideră, în general, că software-ul SOAR nu are funcționalitatea de bază a sistemelor SIEM.

Figura 3

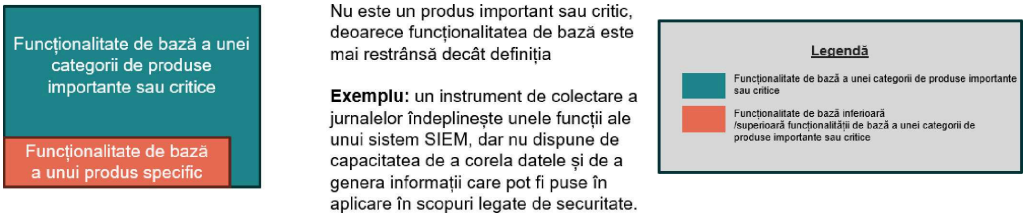
Ilustrarea funcționalității de bază a unui produs cu elemente digitale care depășește în mod substanțial definiția unei categorii de produse importante sau critice



Exemplul 60: Anumite instrumente de colectare și vizualizare a jurnalelor au capacitatea de a asimila date din jurnale și de a prezenta tablouri de bord de bază care prezintă evenimentele din sistem. Deși aceste instrumente pot sprijini activitățile de monitorizare a securității, funcționalitatea lor de bază este inferioară celei a sistemelor SIEM, deoarece nu efectuează corelarea datelor și nici nu oferă informații care pot fi puse în aplicare în materie de securitate. Prin urmare, astfel de instrumente nu trebuie considerate, în general, ca având funcționalitatea de bază a sistemelor SIEM.

Figura 4

Ilustrarea funcționalității de bază a unui produs cu elemente digitale care nu se încadrează în mod substanțial în definiția unei categorii de produse importante sau critice

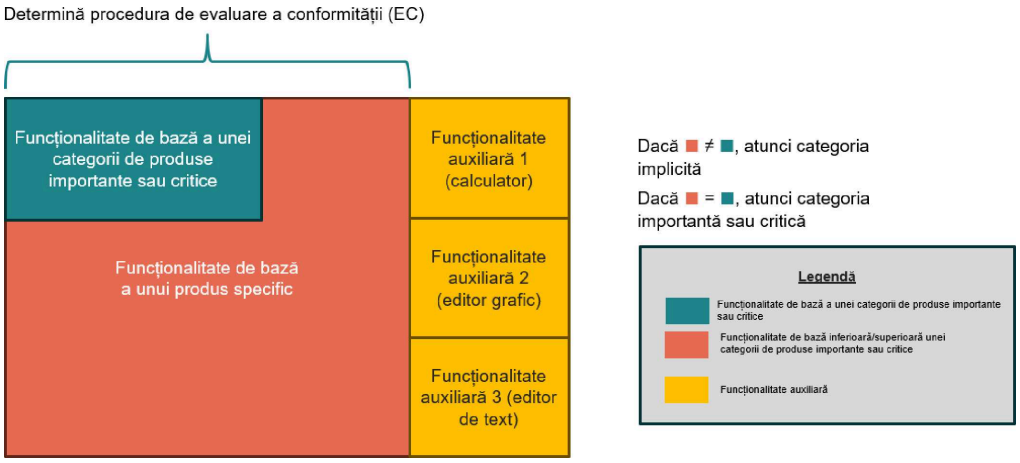


143. Un producător nu poate prezenta în mod eronat funcționalitatea de bază a produsului său cu elemente digitale astfel încât să se sustragă regimului de evaluare a conformității aplicabil produselor importante sau critice cu elemente digitale, de exemplu prin evidențierea sau minimizarea excesivă a rolului anumitor funcționalități, astfel încât produsul să depășească o anumită funcționalitate de bază sau să fie lipsit în mod substanțial de aceasta. Acest lucru ar fi valabil, de exemplu, în cazul în care există neconcordanțe clare între materialele promoționale, instrucțiunile de utilizare și documentația tehnică.

144. Un produs cu elemente digitale nu poate avea mai mult de o funcționalitate de bază în scopul stabilirii regimului aplicabil de evaluare a conformității. În conformitate cu anexa VII la CRA, ca parte a documentației tehnice a unui produs, producătorii trebuie să descrie scopul preconizat al produsului lor cu elemente digitale și procedura de evaluare a conformității pe care au urmat-o. Funcționalitatea de bază a produsului ar trebui, prin urmare, să fie identificată în mod clar. Acest aspect permite identificarea corectă a regimului aplicabil de evaluare a conformității și permite autorităților de supraveghere a pieței să supravegheze și să verifice aplicarea corectă a regulamentului.

Figura 5

Ilustrarea modului în care funcționalitatea de bază a unui anumit produs cu elemente digitale determină clasa produsului și, prin urmare, procedura aplicabilă de evaluare a conformității



145. Unele produse cu elemente digitale sunt introduse pe piață ca produse unice cu elemente digitale, dar sunt compuse din module distincte cu funcționalități separate. În cazul în care un producător pune la dispoziție pe piață modulele respective și separat, cum ar fi în cazul în care acestea sunt oferite spre cumpărare, acordare de licențe sau abonament separat, modulele respective constituie produse de sine stătătoare cu elemente digitale în sine. Ca atare, acestea trebuie clasificate pe baza funcționalităților lor de bază respective (și, prin urmare, fac obiectul regimului adecvat de evaluare a conformității pe baza funcționalității de bază a fiecărui modul). Acest aspect nu aduce atingere modulelor furnizate exclusiv sub formă de componente ale unui produs integrat cu elemente digitale și care nu sunt puse la dispoziție separat; în astfel de cazuri, funcționalitatea de bază este stabilită la nivelul produsului integrat cu elemente digitale.

Exemplul 61: un producător introduce pe piață un pachet de securitate unificat care combină mai multe module, inclusiv un SIEM, un sistem de detectare a intruziunilor și un modul analitic. Producătorul oferă, de asemenea, aceste module pentru abonamente separate. În acest scenariu, fiecare modul este un produs distinct cu elemente digitale și este clasificat pe baza propriei funcționalități de bază. Modulul SIEM face obiectul regimului de evaluare a conformității pentru produsele importante cu elemente digitale din clasa I, deoarece funcționalitatea sa de bază este cea a „sistemelor de gestionare a informațiilor de securitate și a evenimentelor de securitate (SIEM)”. Sistemul de detectare a intruziunilor face obiectul regimului de evaluare a conformității pentru produsele importante cu elemente digitale din clasa II, deoarece funcționalitatea sa de bază este cea de „Firewall-uri, sisteme de detectare și prevenire a intruziunilor”. Modulul analitic face obiectul regimului de evaluare a conformității pentru produsele „implicite” cu elemente digitale, deoarece funcționalitatea sa de bază nu este cea a unei categorii de produse importante sau critice.

146. Nerespectarea obligațiilor prevăzute la articolul 32 din CRA poate angaja amenzi administrative în conformitate cu articolul 64 alineatul (3).

6.2. Evaluarea conformității pentru produsele importante și critice cu elemente digitale

147. Odată ce producătorul a stabilit funcționalitatea de bază a produsului său cu elemente digitale, acesta trebuie să efectueze una dintre procedurile aplicabile de evaluare a conformității. Producătorul trebuie să se asigure că produsul cu elemente digitale în ansamblu îndeplinește cerințele esențiale, ținând seama, după caz, de securitatea componentelor sau a funcționalităților integrate în acesta.

148. O procedură mai strictă de evaluare a conformității, cu implicarea unui terț (pe baza modulului B+C, a modulului H sau a sistemelor de certificare a securității cibernetice), este obligatorie pentru produsele importante cu elemente digitale din clasa II [cu excepția celor care se califică drept software liber și cu sursă deschisă, în conformitate cu articolul 32 alineatul (5)] și pentru produsele critice cu elemente digitale ([24]). În schimb, produsele importante cu elemente digitale din clasa I [cu excepția celor care se califică drept software liber și cu sursă deschisă, în conformitate cu articolul 32 alineatul (5)] trebuie să facă obiectul unei proceduri de evaluare a conformității de către o parte terță numai în cazul în care producătorul nu a aplicat sau a aplicat doar parțial standardele armonizate relevante ale căror referințe au fost publicate în *Jurnalul Oficial al Uniunii Europene* (denumite în continuare „standarde armonizate”), specificațiile comune sau sistemele europene de certificare de securitate cibernetică cu un nivel de asigurare cel puțin „substanțial” ([25]).

149. Prin urmare, pentru ca un produs important cu elemente digitale din clasa I să fie eligibil pentru procedura de control intern, (i) trebuie aplicate toate cerințele aplicabile ale unui standard armonizat relevant și (ii) domeniul de aplicare al standardului trebuie să acopere cel puțin toate riscurile de securitate cibernetică asociate funcționalității de bază a produsului respectiv.

150. Domeniul de aplicare al produsului cu elemente digitale poate fi mai larg decât domeniul de aplicare prevăzut de standardul armonizat relevant, iar astfel de funcții suplimentare pot prezenta riscuri diferite sau suplimentare în materie de securitate cibernetică. Producătorul are întotdeauna obligația de a efectua o evaluare a riscurilor în temeiul articolului 13 alineatul (2) și, în consecință, ar trebui să verifice dacă punerea în aplicare a unui standard armonizat acoperă toate riscurile asociate produsului cu elemente digitale. În cazul în care punerea în aplicare a standardului nu acoperă toate riscurile, producătorul ar trebui să se asigure, prin alte mijloace, că produsul său cu elemente digitale este în conformitate cu cerințele esențiale.

151. Prin urmare, în cazul în care producătorul unui produs important cu elemente digitale din clasa I aplică un standard armonizat relevant care acoperă riscurile asociate funcționalității de bază a produsului respectiv, acesta poate decide să utilizeze procedura de control intern pentru a demonstra conformitatea produsului său. În cadrul activităților sale de evaluare a conformității, producătorul va trebui în continuare să demonstreze că sunt abordate toate riscurile aplicabile produsului său cu elemente digitale. Prin urmare, în cazul în care există un decalaj între acoperirea standardului armonizat și domeniul de aplicare al produsului cu elemente digitale în ansamblu, producătorul trebuie în continuare să documenteze măsurile suplimentare pe care le-a instituit pentru a aborda riscurile respective.

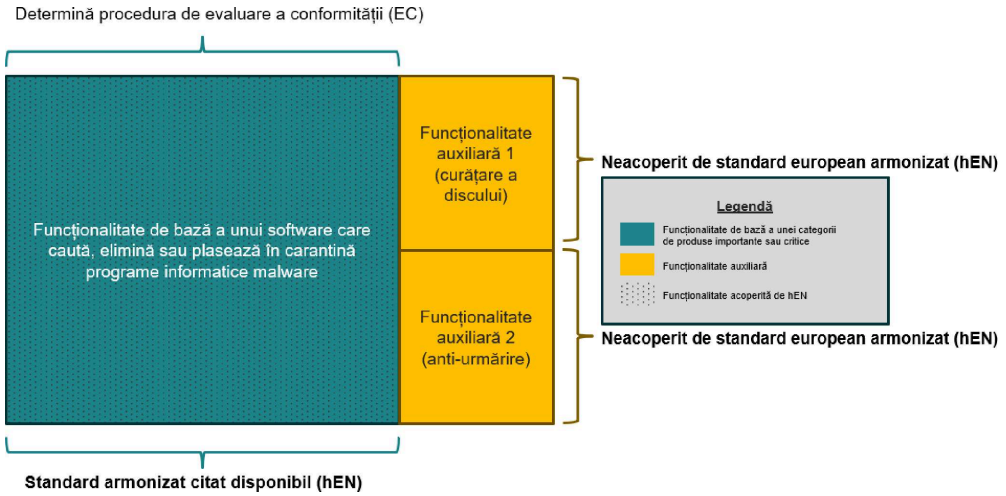
Exemplul 62: Un software antivirus are funcționalitatea de bază a unui software care caută, elimină sau plasează în carantină programe informatice malware, astfel cum se descrie la punctul 4 din anexa I la Regulamentul de punere în aplicare (UE) 2025/2392. Acest produs cu elemente digitale include și caracteristici suplimentare, și anume o funcție de curățare a discului și o funcție anti-urmărire care protejează utilizatorul atunci când navighează pe internet. Producătorul efectuează o evaluare a riscurilor care acoperă produsul cu elemente digitale în ansamblul său, inclusiv funcționalitatea de bază a antivirusului, funcțiile de curățare a discurilor și funcțiile anti-urmărire. Acesta aplică un standard armonizat care acoperă riscurile asociate funcționalității de bază a antivirusului și măsuri suplimentare pentru a face față riscurilor care decurg din funcții suplimentare. Producătorul este autorizat să utilizeze procedura de control intern pentru evaluarea conformității, care acoperă produsul cu elemente digitale în ansamblu, inclusiv funcțiile de curățare a discurilor și funcțiile anti-urmărire.

([24]) Acest lucru este valabil și atunci când se utilizează un sistem european de certificare de securitate cibernetică cu un nivel de asigurare cel puțin „substanțial”, deoarece este necesară implicarea unui organism de certificare terț.

([25]) Din motive de concizie, restul acestei secțiuni se referă numai la standardele armonizate ale căror referințe au fost publicate în *Jurnalul Oficial al Uniunii Europene*. Cu toate acestea, aceleași orientări se aplică, de asemenea, specificațiilor comune adoptate în conformitate cu articolul 27 alineatul (2) și sistemelor europene de certificare de securitate cibernetică, în cazurile specificate de Comisie prin acte delegate în conformitate cu articolul 27 alineatul (9).

Figura 6

Ilustrarea modului în care utilizarea unui standard armonizat citat care acoperă numai funcționalitatea de bază determină procedura aplicabilă de evaluare a conformității



152. Acest aspect este valabil și în cazul în care produsul cu elemente digitale integrează o funcție suplimentară care este în sine cea a unui alt produs important sau critic cu elemente digitale. În fapt, funcționalitatea de bază a produsului cu elemente digitale în ansamblu și nu funcționalitatea componentelor integrate luate separat este cea care determină dacă produsul cu elemente digitale aparține categoriei de produse importante sau critice (și, prin urmare, regimului aplicabil de evaluare a conformității). De exemplu, dacă un produs cu elemente digitale are funcționalitatea de bază a unui produs important cu elemente digitale din clasa I, produsul respectiv în ansamblu face obiectul regimului de evaluare a conformității aplicabil produselor importante cu elemente digitale din clasa I, chiar dacă integrează o componentă care este în sine un produs critic cu elemente digitale. În aceste cazuri, atunci când producătorul aplică un standard armonizat care acoperă riscurile asociate funcționalității de bază a produsului respectiv, acestuia i se permite să utilizeze procedura de control intern.

Exemplul 63: Un produs hardware cu elemente digitale are funcționalitatea de bază a unui router, astfel cum se descrie la punctul 12 din anexa I la Regulamentul de punere în aplicare (UE) 2025/2392. Acest produs cu elemente digitale include, de asemenea, funcționalități suplimentare, inclusiv capacități firewall, deoarece integrează o componentă firewall. Producătorul efectuează o evaluare a riscurilor care acoperă produsul cu elemente digitale în ansamblul său, inclusiv funcționalitatea de bază a routerului și funcționalitatea de firewall. Acesta aplică un standard armonizat care acoperă riscurile asociate funcționalității de bază a routerului și măsuri suplimentare pentru a face față riscurilor care decurg din funcții suplimentare. De exemplu, producătorul poate aplica standardul armonizat pentru firewall-uri pentru a acoperi riscurile asociate funcționalității de firewall. Producătorul este autorizat să utilizeze procedura de control intern pentru evaluarea conformității, care acoperă produsul cu elemente digitale în ansamblu, inclusiv funcționalitatea de firewall.

6.3. Implicații pentru prezumția de conformitate

153. Articolul 27 alineatul (1) din CRA prevede că 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* (JOUE) sunt considerate a fi conforme cu cerințele esențiale prevăzute în CRA,

vizate de respectivele standarde sau părți ale acestora ([26]). Articolul 27 alineatul (5) extinde aceeași prezumție de conformitate la produsele cu elemente digitale și la procesele instituite de producător care sunt conforme cu specificațiile comune adoptate de Comisie prin acte de punere în aplicare, iar articolul 27 alineatul (8) stabilește prezumția de conformitate pentru 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, dacă acest lucru a fost specificat prin acte delegate în conformitate cu articolul 27 alineatul (9) ([27]).

154. Prin urmare, în cazul în care producătorul aplică un standard armonizat ale cărui referințe au fost publicate în JOUE, acesta beneficiază de o prezumție de conformitate pentru riscurile acoperite de standardul respectiv. Acest lucru ar putea fi valabil, de exemplu, în cazul în care standardul armonizat menționat abordează toate riscurile asociate funcționalității de bază a unui produs cu elemente digitale și nu există funcționalități suplimentare care să prezinte riscuri în materie de securitate cibernetică. De exemplu, se preconizează că standardul armonizat pentru routere va aborda cel puțin riscurile asociate funcționalității de bază a acestor produse cu elemente digitale. Dacă un astfel de produs nu conține funcționalități suplimentare sau dacă aceste funcționalități suplimentare nu prezintă riscuri neabordate de standard, produsul cu elemente digitale poate beneficia de prezumția de conformitate.

155. În cazurile discutate la punctele 151 și 152, producătorului i se permite să utilizeze procedura de control intern, deoarece standardul armonizat acoperă riscurile asociate funcționalității de bază a produsului cu elemente digitale. Cu toate acestea, produsele cu elemente digitale descrise în exemplele respective pot fi mai ample decât domeniul de aplicare al standardelor armonizate, iar funcționalitățile suplimentare pot prezenta riscuri în materie de securitate cibernetică care nu sunt abordate de un astfel de standard armonizat. Prin urmare, este posibil ca aceste produse cu elemente digitale să nu beneficieze de prezumția de conformitate pentru funcționalitățile suplimentare respective.

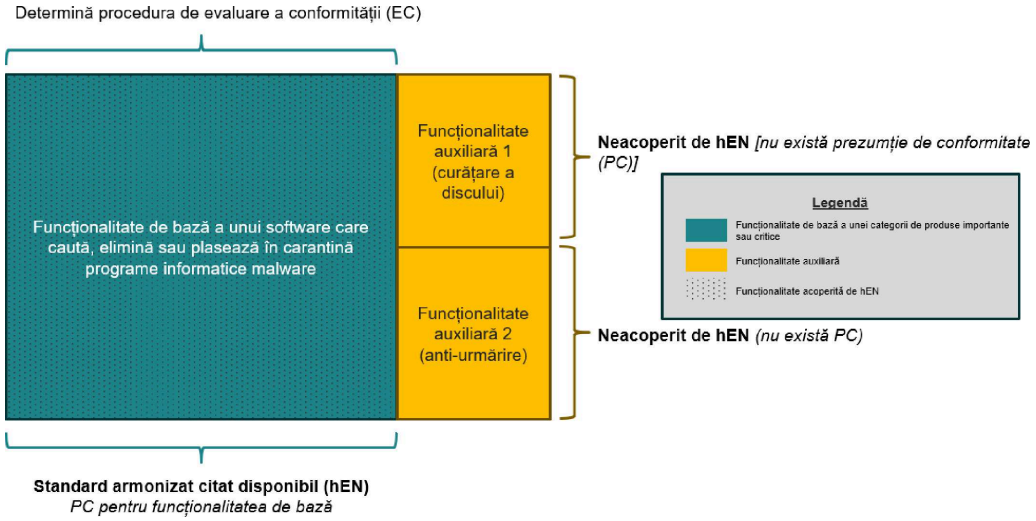
Exemplul 64: Un software antivirus are funcționalitatea de bază a unui software care caută, elimină sau plasează în carantină programe informatice malware, iar riscurile asociate funcționalității de bază respective sunt acoperite de standardul armonizat. Acest produs cu elemente digitale include și funcționalități suplimentare, și anume o funcție de curățare a discului și o funcționalitate anti-urmărire care protejează utilizatorul atunci când navighează pe internet, ale căror riscuri nu sunt acoperite de standardul armonizat. În cazul în care se aplică standardul armonizat, producătorul este autorizat să utilizeze procedura de control intern pentru evaluarea conformității. Acesta va beneficia de prezumția de conformitate pentru riscurile asociate funcționalității de bază a produsului respectiv, dar nu și pentru riscurile asociate funcționalităților suplimentare.

([26]) Astfel cum se menționează în mod clar în secțiunea 4.1.2.2 din Ghidul albastru, „în legislația de armonizare în materie de riscuri [...] producătorilor, chiar și în cazul în care aplică standarde armonizate ale căror trimiteri sunt publicate în *Jurnalul Oficial al Uniunii Europene*, le revine întotdeauna deplina responsabilitate de a evalua toate riscurile produsului lor pentru a stabili care sunt cerințele esențiale (sau alte cerințe) relevante. După o astfel de evaluare, un producător poate alege să aplice specificațiile tehnice cuprinse în standardele armonizate ale căror trimiteri sunt publicate în *Jurnalul Oficial al Uniunii Europene* pentru a pune în aplicare «măsurile de reducere a riscurilor» stabilite de standardele armonizate”.

([27]) După cum se prevede mai sus, din motive de concizie, restul acestei secțiuni se referă numai la standardele armonizate ale căror referințe au fost publicate în *Jurnalul Oficial al Uniunii Europene*. Cu toate acestea, aceleași orientări se aplică, de asemenea, specificațiilor comune și sistemelor europene de certificare de securitate cibernetică.

Figura 7

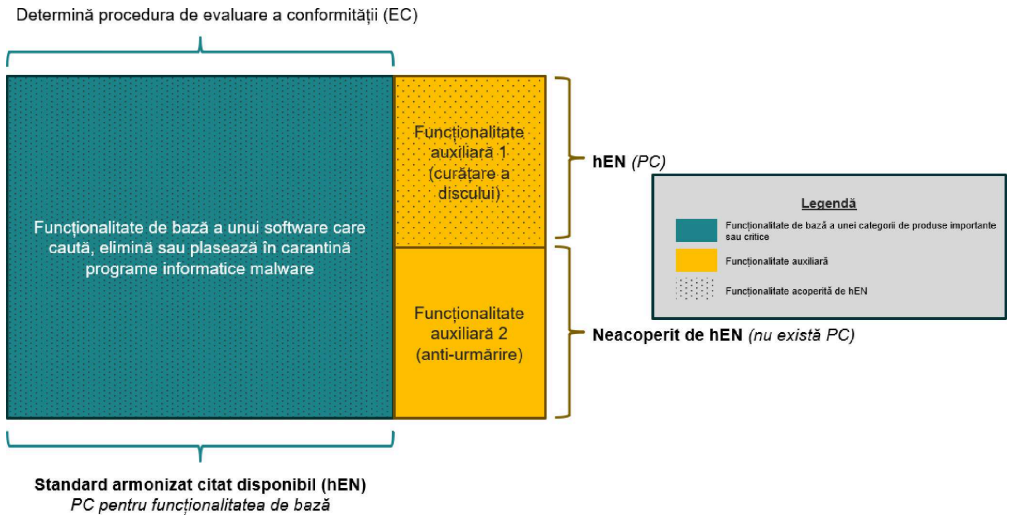
Standardul armonizat acordă prezumția de conformitate (PC) pentru funcționalitatea de bază, deoarece abordează toate riscurile asociate funcționalității de bază respective, dar nu și pentru funcționalitățile auxiliare



Exemplul 65: În același scenariu ca și exemplul anterior, standardul armonizat a fost actualizat pentru a acoperi și riscurile asociate uneia dintre funcționalitățile suplimentare, și anume funcția de curățare a discului, dar nu și celeilalte (și anume funcția anti-urmărire). În cazul în care se aplică standardul armonizat, producătorul este autorizat să utilizeze procedura de control intern pentru evaluarea conformității. Acesta va beneficia de o prezumție de conformitate pentru riscurile asociate funcționalității de bază a produsului respectiv și funcționalității de curățare a discului, dar nu și pentru riscurile legate de funcționalitatea anti-urmărire.

Figura 8

Standardul armonizat acordă PC pentru funcționalitatea de bază și funcționalitatea auxiliară 1, deoarece abordează toate riscurile asociate acestor două funcționalități, dar nu și pentru funcționalitatea auxiliară 2



7. EVALUAREA RISCURILOR ÎN MATERIE DE SECURITATE CIBERNETICĂ ȘI INTEGRAREA PRODUSELOR CU ELEMENTE DIGITALE ȘI COMPONENTE

7.1. În ceea ce privește evaluarea și abordarea riscurilor în materie de securitate cibernetică

156. Evaluarea riscurilor în materie de securitate cibernetică prevăzută la articolul 13 alineatul (2) din CRA prevede obligația producătorilor de a identifica riscurile relevante și de a evalua impactul potențial al acestora asupra produsului cu elemente digitale. Producătorii trebuie, de asemenea, să pună în aplicare măsuri adecvate pentru a aborda aceste riscuri, în conformitate cu cerințele esențiale prevăzute în anexa I.

157. În gestionarea riscurilor organizaționale, riscurile sunt evaluate în mod obișnuit pe baza criteriilor de acceptare derivate din obiectivele interne ale organizației sau din apetitul pentru risc. În schimb, în temeiul CRA, riscul rezidual de securitate cibernetică ar trebui evaluat având în vedere cerința ca produsul cu elemente digitale introdus pe piață să asigure un nivel adecvat de securitate cibernetică bazat pe riscuri, ținând seama de scopul său preconizat și de utilizarea sa previzibilă în mod rezonabil.

158. În consecință, toleranța internă la risc a producătorului, strategia comercială sau simple considerații legate de costuri nu sunt relevante pentru a stabili dacă riscurile au fost abordate. În sensul articolului 13 alineatele (2) și (3), producătorii trebuie să fie în măsură să stabilească dacă riscurile de securitate cibernetică identificate au fost abordate în mod satisfăcător prin punerea în aplicare a cerințelor esențiale prevăzute în anexa I partea I, având în vedere scopul preconizat, utilizarea previzibilă în mod rezonabil și condițiile de utilizare, inclusiv, după caz, mediul operațional (de exemplu, utilizatorii preconizați ai produsului cu elemente digitale) și activele care urmează să fie protejate, ținând seama de perioada de timp în care se preconizează că produsul cu elemente digitale va fi în uz.

159. Riscul rezidual în materie de securitate cibernetică este un rezultat inerent al evaluării riscurilor și al abordării riscurilor. Este recunoscut faptul că riscurile în materie de securitate cibernetică nu pot fi eliminate în totalitate în practică. Cu toate acestea, existența unui risc rezidual nu implică faptul că orice risc poate fi acceptat la latitudinea producătorului. Un produs cu elemente digitale poate fi introdus pe piață numai în cazul în care riscurile reziduale, odată ce au fost luate măsurile adecvate, au fost abordate în mod satisfăcător prin punerea în aplicare a cerințelor esențiale, ținând seama de scopul preconizat și de utilizarea previzibilă în mod rezonabil a produsului cu elemente digitale.

160. În conformitate cu articolul 13 alineatul (3), în cazul în care sunt identificate riscuri în materie de securitate cibernetică, producătorii au obligația de a le aborda prin măsuri adecvate, inclusiv la nivel de produs. În funcție de circumstanțe, acest lucru poate implica, de exemplu, reducerea suprafeței de atac, punerea în aplicare a unor garanții tehnice, limitarea sau adaptarea funcționalității sau definirea mai precisă a scopului preconizat al produsului cu elemente digitale. Producătorii pot lua, de asemenea, măsuri pentru a modela utilizarea previzibilă în mod rezonabil a produsului cu elemente digitale, de exemplu prin comunicarea riscurilor, îndrumarea utilizatorilor sau proiectarea interfeței cu utilizatorul, pentru a orienta comportamentul utilizatorilor către modele de utilizare sigure.

161. CRA nu prevede transferul riscului în materie de securitate cibernetică sau al responsabilității utilizatorilor sau părților terțe pentru a compensa deficiențele în proiectarea produselor sau pentru a justifica neabordarea riscurilor în materie de securitate cibernetică. Obligația de a introduce pe piață un produs securizat cu elemente digitale și de a demonstra conformitatea cu cerințele esențiale revine producătorului.

162. Informațiile și instrucțiunile furnizate utilizatorilor pot fi utilizate pentru a sprijini implementarea și exploatarea în condiții de siguranță a produsului cu elemente digitale, inclusiv în cazul în care producătorul a ales să restricționeze scopul preconizat al produsului respectiv la medii fiabile, precum și pentru a informa utilizatorii cu privire la riscurile reziduale, într-un mod adecvat naturii produsului cu elemente digitale și utilizatorilor preconizați ai acestuia.

Exemplul 66: Un producător dezvoltă un senzor industrial pentru a fi utilizat în medii de încredere. Pentru ca senzorul să funcționeze corect, producătorul nu pune în aplicare măsuri de protecție împotriva atacurilor fizice asupra senzorului în sine. Pentru a atenua riscurile asociate identificate în evaluarea riscurilor, producătorul limitează scopul preconizat al senzorului la utilizarea exclusiv în medii de încredere în care este prevenit accesul fizic neautorizat la produsul cu elemente digitale. Informațiile și instrucțiunile pentru utilizatori oferă informații clare cu privire la aceste limitări ale utilizării senzorului, într-un mod adecvat naturii produsului cu elemente digitale și utilizatorilor preconizați ai acestuia.

Exemplul 67: Un producător dezvoltă o aplicație software pentru uz profesional pe dispozitive de tip desktop și mobile gestionate. Aplicația prelucrează date sensibile stocate la nivel local și conținut generat de utilizatori. În cursul evaluării riscurilor, producătorul identifică riscul de acces neautorizat la astfel de date, dacă acestea sunt stocate în format necriptat pe dispozitiv. În loc să proiecteze și să pună în aplicare un mecanism de criptare brevetat în cadrul aplicației în sine, producătorul alege să se bazeze pe funcțiile de criptare și de gestionare a cheilor furnizate în mod intrinsec de sistemul de operare proiectat pentru funcționarea aplicației, întrucât serviciile criptografice încorporate ale sistemului de operare sunt consolidate și întreținute în permanență.

163. În cazul în care evaluarea riscurilor în materie de securitate cibernetică identifică riscuri care nu pot fi abordate în mod adecvat prin măsuri corespunzătoare, respectarea CRA poate necesita modificări ale proiectării, funcționalității sau scopului preconizat al produsului cu elemente digitale. Considerațiile legate exclusiv de costuri sau de fezabilitatea comercială nu constituie motive suficiente pentru neabordarea acestor riscuri în cazul în care acest aspect ar împiedica îndeplinirea cerințelor esențiale de către produsul cu elemente digitale.

7.2. În ceea ce privește proiectarea, dezvoltarea și fabricarea de produse cu elemente digitale astfel încât să asigure un nivel adecvat de securitate cibernetică bazat pe riscuri

164. Cerința esențială de securitate cibernetică menționată la punctul 1 din partea I a anexei I la CRA prevede că produsele cu elemente digitale sunt proiectate, dezvoltate și fabricate astfel încât să asigure un nivel adecvat de securitate cibernetică bazat pe riscuri.

165. Această cerință esențială vizează abordarea tuturor riscurilor în materie de securitate cibernetică care au fost identificate în cadrul evaluării riscurilor în materie de securitate cibernetică. În special, aceasta include riscurile în materie de securitate cibernetică neabordate în mod adecvat în alt mod ca parte a punerii în aplicare a cerințelor esențiale din partea I a anexei I, altele decât cele menționate la punctul 1. Această cerință esențială este diferită de obligația legală de a efectua o evaluare a riscurilor în materie de securitate cibernetică, care trebuie efectuată în temeiul articolului 13 alineatul (2).

166. În cazul în care toate riscurile de securitate cibernetică relevante legate de un produs cu elemente digitale sunt tratate prin punerea în aplicare a unor măsuri adecvate pentru a aborda alte cerințe esențiale aplicabile decât cele menționate la punctul 1, cerința esențială menționată în anexa I partea I punctul 1 este considerată îndeplinită. În schimb, în cazul în care evaluarea riscurilor în materie de securitate cibernetică identifică riscuri suplimentare care nu sunt abordate pe deplin de astfel de măsuri, producătorii au obligația de a pune în aplicare măsuri adecvate privind produsul cu elemente digitale pentru a aborda riscurile respective, astfel încât să respecte cerința esențială menționată în anexa I partea I punctul 1. În practică, în majoritatea cazurilor, se preconizează că respectarea celorlalte cerințe esențiale va determina respectarea acestei cerințe.

7.3. Evaluarea riscurilor și diligența necesară în ceea ce privește dependențele externe și componentele integrate

167. CRA stabilește două obligații distincte, dar complementare, pentru producători în ceea ce privește gestionarea riscurilor în materie de securitate cibernetică. În primul rând, articolul 13 alineatul (2) impune producătorilor să efectueze o evaluare a riscurilor în materie de securitate cibernetică pentru produsul cu elemente digitale în sine. În al doilea rând, articolul 13 alineatul (5) impune obligația de diligență în ceea ce privește componentele integrate. Împreună, aceste două obligații sunt concepute pentru a se asigura că produsul cu elemente digitale rămâne securizat, inclusiv în cazul în care se bazează pe soluții de prelucrare a datelor la distanță, pe servicii la distanță sau pe componente software sau hardware ale terților.

168. Evaluarea riscurilor în materie de securitate cibernetică se referă la identificarea și gestionarea riscurilor relevante care pot afecta produsul cu elemente digitale, inclusiv a riscurilor care provin din afara produsului în sine, cum ar fi rețelele externe, factorii de mediu sau alte aspecte externe care ar putea afecta produsul cu elemente digitale sau pe care se bazează produsul. În cazul unor astfel de riscuri externe, CRA nu impune producătorilor să controleze sau să reglementeze mediul extern. Mai degrabă, producătorii sunt obligați să identifice astfel de riscuri și să le atenueze prin proiectarea și dezvoltarea produsului cu elemente digitale în sine. Acest aspect va implica punerea în aplicare a cerințelor esențiale adecvate prevăzute în anexa I partea I și, dacă este necesar, furnizarea de informații și instrucțiuni utilizatorilor cu privire la riscurile de integrare sau de implementare.

169. De exemplu, un producător poate identifica riscul ca persoane neautorizate să obțină acces la sistemele back-end care nu fac parte din produsul cu elemente digitale în sine în timp ce produsul este în funcțiune și poate încerca să trimită comenzi dăunătoare produsului cu elemente digitale. Astfel de sisteme back-end, în cazul în care nu sunt proiectate și dezvoltate de producător sau sub responsabilitatea acestuia sau în cazul în care nu suportă una dintre funcțiile produsului cu elemente digitale, nu constituie soluții de prelucrare a datelor la distanță și, prin urmare, nu intră în domeniul de aplicare al produsului cu elemente digitale în sensul CRA. Cu toate acestea, CRA impune producătorului să abordeze riscul pe care îl poate prezenta prin măsuri la nivel de produs, cum ar fi impunerea autentificării criptografice a comenzilor la distanță, verificarea integrității modificărilor de configurație sau generarea de jurnale sau alerte relevante pentru securitate atunci când se detectează un comportament anormal. În mod similar, în cazul în care un producător identifică un risc care rezultă din faptul că un astfel de serviciu extern devine indisponibil, de exemplu din cauza penelor de curent sau a disfuncționalităților la nivel de infrastructură, CRA poate solicita măsuri de atenuare la nivel de produs împotriva unor astfel de riscuri în materie de securitate cibernetică, de exemplu asigurarea faptului că pana de curent nu determină condiții nesigure pentru produs. În astfel de cazuri, CRA reglementează modul în care produsul cu elemente digitale răspunde acestor riscuri externe; acesta nu impune obligații cu privire la modul în care infrastructura *back-end* este organizată, dotată cu personal sau exploatată și nici nu tratează infrastructura respectivă ca parte a produsului cu elemente digitale.

170. Diligența necesară se referă la elemente care fac parte din produsul cu elemente digitale în sine, în special la componentele software sau hardware integrate furnizate de un terț. Producătorii au obligația de a lua măsuri adecvate pentru a se asigura că astfel de componente nu subminează conformitatea produsului cu elemente digitale cu cerințele esențiale. Acest lucru poate fi realizat numai stabilind de ce are nevoie produsul cu elemente digitale de la propriile componente pentru a-și îndeplini obiectivele de securitate cibernetică și verificând, într-un mod bazat pe riscuri, că respectivele componente sunt în conformitate cu nevoile produsului, astfel cum se indică și la considerentul 34.

171. În conformitate cu evaluarea riscurilor în materie de securitate cibernetică, producătorul trebuie să identifice cerințele pe care componenta integrată ar trebui să le îndeplinească. De exemplu, în cazul în care produsul cu elemente digitale se bazează pe funcții criptografice, pe mecanisme de actualizare sau pe comunicații securizate furnizate de o componentă, producătorul trebuie, ca parte a obligației sale de diligență, să identifice nevoile respective și să verifice îndeplinirea lor de către componentă. Dovezile în acest sens pot consta în documentația obținută de la producătorul componentei, cum ar fi specificațiile tehnice, documentația de securitate sau documentația relevantă în materie de conformitate sau nivel de asigurare. După caz, producătorul poate efectua, de asemenea, teste pentru a verifica dacă respectivele componente îndeplinesc în mod adecvat funcțiile relevante. Deși diligența necesară este o obligație juridică separată, aceasta sprijină și stă la baza capacității producătorului de a demonstra conformitatea cu cerințele esențiale pentru produsul cu elemente digitale în ansamblu.

172. Atunci când se evaluează riscurile pentru produsul cu elemente digitale în ansamblu, elementele din afara produsului, cum ar fi elementele de mediu, infrastructura externă, alte sisteme sau rețele, trebuie luate în considerare în evaluarea riscurilor în materie de securitate cibernetică și, după caz, abordate prin măsuri la nivel de produs pentru a asigura conformitatea produsului cu elemente digitale cu cerințele esențiale. Componentele care sunt integrate fizic sau logic în produsul cu elemente digitale, dar care provin de la o parte terță, trebuie, de asemenea, să fie considerate ca făcând parte din evaluarea riscurilor. Cu toate acestea, în scopul asigurării conformității, producătorul ar trebui să le trateze drept componente furnizate extern ale căror proprietăți sunt verificate cu diligența necesară în momentul integrării, deoarece este posibil ca producătorul să nu le fi reproiectat sau îmbunătățit.

173. Aceeași logică se aplică în contextul dezvoltării și integrării componentelor. În cazul în care producătorul dezvoltă el însuși funcționalități, acesta trebuie să pună în aplicare în mod direct cerințele esențiale. În cazul în care producătorul integrează componente dezvoltate de alții, acesta trebuie să se asigure, prin diligența necesară, că respectivele componente pot fi utilizate într-un mod care să permită conformitatea produsului cu elemente digitale în ansamblu. În ambele cazuri, obiectivul rămâne același: faptul că produsul cu elemente digitale, astfel cum este introdus pe piață, atinge un nivel adecvat de securitate cibernetică, astfel cum prevede CRA, ținând seama de riscurile identificate în evaluarea riscurilor în materie de securitate cibernetică.

7.4. **Reutilizarea evaluărilor riscurilor și a documentației de conformitate pentru familiile de produse cu elemente digitale**

174. Producătorii pot introduce pe piață produse cu elemente digitale similare, de exemplu variante, modele sau configurații diferite ale aceleiași familii de produse. În cazul în care astfel de produse cu elemente digitale au aceeași arhitectură, același design relevant pentru securitate și același scop preconizat și sunt expuse acelorași riscuri de securitate cibernetică, CRA nu impune producătorilor să trateze fiecare variantă ca un produs cu elemente digitale complet separat în scopul evaluării riscurilor și al evaluării conformității.

175. În astfel de cazuri, cu condiția ca toate variantele în cauză să fie acoperite în mod adecvat în ceea ce privește riscurile relevante și cerințele esențiale, producătorii se pot baza pe: (i) o singură evaluare a riscurilor în materie de securitate cibernetică efectuată în conformitate cu articolul 13 alineatul (2) din CRA; (ii) un set unic de documentație tehnică și (iii) o procedură unică de evaluare a conformității. Acest fapt permite, de asemenea, emiterea unei declarații de conformitate UE unice pentru grupul de produse cu elemente digitale, atât timp cât identifică în mod clar variantele de produse cărora li se aplică.

176. Factorul decisiv este dacă diferențele dintre variante sunt relevante pentru securitatea cibernetică. Variantele care nu afectează proprietățile de securitate cibernetică ale produsului cu elemente digitale, cum ar fi diferențele în ceea ce privește culoarea, factorul de formă, dimensiunea memoriei sau alte caracteristici care nu sunt relevante pentru securitate, nu necesită evaluări separate ale riscurilor sau ale conformității. În schimb, în unele cazuri, variantele pot diferi în moduri care afectează punerea în aplicare a cerințelor esențiale, de exemplu prin diferite interfețe de comunicare, pachete de software, mecanisme de actualizare sau conectivitate la distanță. În astfel de cazuri, diferențele respective trebuie să se reflecte în evaluarea riscurilor și, dacă este necesar, în evaluarea conformității și în documentația tehnică.

177. Producătorii rămân responsabili de asigurarea faptului că evaluarea riscurilor și documentația aferentă reflectă cu acuratețe produsele cu elemente digitale introduse pe piață. În cazul în care o nouă variantă introduce noi riscuri în materie de securitate cibernetică sau modifică modul în care sunt puse în aplicare cerințele esențiale, evaluarea riscurilor și documentația de conformitate existente trebuie actualizate în consecință. Recurgerea la o singură evaluare a conformității este posibilă numai în măsura în care produsele cu elemente digitale nu prezintă diferențe în ceea ce privește proprietățile lor în materie de securitate cibernetică.

8. **PRELUCRAREA DATELOR LA DISTANȚĂ**

178. Articolul 3 punctul 1 din CRA definește un produs cu elemente digitale ca fiind „un produs software sau hardware și soluțiile sale de prelucrare de date la distanță, inclusiv componentele software sau hardware introduse pe piață separat”. În acest context, producătorul trebuie să ia în considerare produsul cu elemente digitale în ansamblu, inclusiv soluțiile sale de prelucrare a datelor la distanță (RDPS). De exemplu, atunci când se demonstrează că produsul cu elemente digitale respectă cerințele esențiale prevăzute în anexa I, trebuie să se țină seama de RDPS, începând cu evaluarea riscurilor [articolul 13 alineatul (2)]. Același lucru este valabil și atunci când se iau în considerare obligațiile privind ciclul de viață, cum ar fi raportarea vulnerabilităților exploatate activ și a incidentelor grave (articolul 14).

179. Scopul prezentelor orientări este de a oferi asistență suplimentară producătorilor pentru a stabili dacă produsul lor cu elemente digitale are RDPS, astfel cum sunt definite în CRA, precum și modul de îndeplinire a obligațiilor lor de conformitate în această privință. După o analiză inițială a definițiilor și a considerentelor prevăzute în CRA, prezentele orientări vor oferi întrebări pentru a ajuta producătorii să clarifice dacă produsul lor cu elemente digitale include RDPS (a se vedea secțiunea *8.1 Ce se consideră a fi o soluție de prelucrare a datelor la distanță pentru un produs cu elemente digitale?*). Ulterior, vor detalia implicațiile tehnice ale RDPS și modul de evaluare a conformității cu CRA (a se vedea secțiunea *8.2 Implicațiile practice și tehnice ale soluțiilor de prelucrare a datelor la distanță și dependența de soluțiile oferite de terți*).

180. În fapt, articolul 3 punctul 2 definește conceptul de „prelucrare de date la distanță” ca fiind „prelucrarea de date la distanță pentru care software-ul este proiectat și dezvoltat de producător sau sub responsabilitatea producătorului și a cărei absență ar împiedica produsul cu elemente digitale să își îndeplinească vreuna dintre funcții”. Prin urmare, RDPS sunt definite ca fiind elementele software („acea parte a unui sistem informatic electronic care constă într-un cod informatic”, astfel cum este definit la articolul 3 punctul 4) ale prelucrării datelor la distanță. Acestea nu sunt menite să includă, ca parte a domeniului de aplicare al produsului cu elemente digitale, hardware-ul pe care se poate baza prelucrarea datelor la distanță.

181. Considerentele 11 și 12 oferă explicații suplimentare cu privire la modul în care ar trebui interpretat acest concept. Considerentul 11 clarifică faptul că obiectivul de a acoperi soluția de prelucrare a datelor la distanță este că „astfel de produse sunt securizate în mod adecvat și integral de către producătorii lor, indiferent dacă datele sunt prelucrate sau stocate local pe dispozitivul utilizatorului sau la distanță de către producător”. De asemenea, prevede că „cerințele privind soluțiile de prelucrare a datelor la distanță care intră în domeniul de aplicare al prezentului regulament nu implică măsuri tehnice, operaționale sau organizatorice menite să gestioneze riscurile la adresa securității rețelelor și a sistemelor informatice ale unui producător în ansamblu”.

182. Prin urmare, din considerentul 11 rezultă că scopul nu este ca cerințele CRA să acopere întreaga infrastructură informatică a unei organizații, ci numai componentele software care permit executarea soluției de prelucrare a datelor. De exemplu, sistemele interne referitoare la resursele umane proprii ale producătorului, remunerațiile, gestionarea relației cu clienții, fluxurile de integrare/livrare continuă (CI/CD), distribuirea actualizărilor de securitate către locațiile periferice nu ar trebui considerate RDPS. De asemenea, sistemele legate de activitățile de audit și testare, cum ar fi testele de penetrare, depistarea amenințărilor și formarea de echipe roșii, nu intră în domeniul de aplicare al unui produs cu elemente digitale, potrivit celor reglementate de CRA. Este important de remarcat faptul că, deși aplicarea unor teste și reexaminări eficace și periodice ale securității produsului cu elemente digitale este o cerință esențială prevăzută la punctul 3 din partea II a anexei I la CRA, acest lucru nu înseamnă că astfel de activități trebuie considerate RDPS pentru produsul cu elemente digitale.

183. Considerentul 12 se axează pe serviciile de cloud și detaliază circumstanțele în care serviciile de cloud ar putea fi considerate RDPS. Considerentul se încheie prin a reaminti că serviciile de cloud computing și modelele de servicii de cloud intră în domeniul de aplicare al Directivei (UE) 2022/2555 (NIS 2) ([28]), care stabilește cerințe de gestionare a riscurilor în materie de securitate cibernetică pentru furnizorii de servicii de cloud computing. Cerințele respective sunt specificate în detaliu în Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei ([29]).

8.1. **Ce se consideră a fi o soluție de prelucrare a datelor la distanță pentru un produs cu elemente digitale?**

184. Astfel, definiția prelucrării de date la distanță prevăzută la articolul 3 punctul 2 se bazează pe trei elemente: (i) dacă prelucrarea datelor are loc „la distanță”; (ii) dacă absența unei astfel de prelucrări a datelor ar împiedica produsul cu elemente digitale să își îndeplinească vreuna dintre funcții și (iii) dacă software-ul este proiectat și dezvoltat de producător sau sub responsabilitatea acestuia. Următoarele trei subsecțiuni abordează fiecare dintre aceste elemente mai detaliat.

([28]) Directiva (UE) 2022/2555 a Parlamentului European și a Consiliului din 14 decembrie 2022 privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune, de modificare a Regulamentului (UE) nr. 910/2014 și a Directivei (UE) 2018/1972 și de abrogare a Directivei (UE) 2016/1148 (Directiva NIS 2) (JO L 333, 27.12.2022, p. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/2022-12-27).

([29]) Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei din 17 octombrie 2024 de stabilire a normelor de aplicare a Directivei (UE) 2022/2555 în ceea ce privește cerințele tehnice și metodologice ale măsurilor de gestionare a riscurilor în materie de securitate cibernetică și specificarea suplimentară a cazurilor în care un incident este considerat semnificativ referitor la furnizorii de servicii DNS, registrele de nume TLD, furnizorii de servicii de cloud computing, furnizorii de servicii de centre de date, furnizorii de rețele de furnizare de conținut, furnizorii de servicii gestionate, furnizorii de servicii de securitate gestionate, furnizorii de piețe online, de motoare de căutare online și de platforme de servicii de socializare în rețea, precum și prestatorii de servicii de încredere (JO L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

8.1.1. *Noțiunea „la distanță”*

185. Noțiunea „la distanță” menționată la articolul 3 punctul 2 este relevantă, dar nu suficientă pentru a stabili dacă un produs cu elemente digitale include RDPS. În plus, având în vedere varietatea soluțiilor care ar putea intra sub incidența acestui concept, nu este posibilă oferirea unei definiții exhaustive a termenului „la distanță”. Este necesară o evaluare de la caz la caz de către producător.

186. Considerentul 11 din CRA menționează datele prelucrate sau stocate „la distanță de către producător”, spre deosebire de datele prelucrate sau stocate „local pe dispozitivul utilizatorului”. Prelucrarea datelor la distanță are loc, de regulă, în afara mediului de utilizare a unui produs cu elemente digitale sau a mediului operațional al unei organizații (pentru un utilizator profesionist). Acest aspect nu împiedică însă ca prelucrarea să aibă loc și în apropierea dispozitivului („la margine”). Transmiterea datelor poate fi realizată prin cablu (de exemplu, cablu ethernet) sau fără fir (de exemplu, Wi-Fi, Bluetooth). Tehnica de calcul în cloud (*cloud computing*), inclusiv tehnica de calcul la margine (*edge computing*), este un exemplu tipic de prelucrare a datelor care are loc „la distanță”. De exemplu, în cazul unei funcții bazate pe cloud accesate de utilizator dintr-o aplicație mobilă, o parte din prelucrarea datelor are loc în cloud, în afara mediului utilizatorului.

187. Este important de remarcat faptul că RDPS nu funcționează neapărat pe infrastructura de cloud a terților. Prelucrarea datelor la distanță care funcționează pe servere locale la sediul producătorului poate constitui, de asemenea, RDPS. Cu alte cuvinte, o soluție care funcționează la sediu și pe un cloud privat este la fel de probabil să se califice drept RDPS ca o soluție care funcționează pe un cloud public și în afara sediului.

188. Cele două întrebări decisive și cumulative care stabilesc dacă prelucrarea datelor intră sub incidența CRA ca soluție de prelucrare a datelor la distanță sunt prezentate mai jos, în secțiunile *8.1.2* și *8.2*. În cazul unui răspuns afirmativ la ambele întrebări, prelucrarea datelor la distanță se califică drept RDPS.

8.1.2. *Absența unei astfel de prelucrări a datelor ar împiedica produsul cu elemente digitale să își îndeplinească vreuna dintre funcții?*

189. Astfel cum se prevede în definiția pentru „prelucrarea de date la distanță” inclusă la articolul 3 punctul 2, pentru ca prelucrarea datelor la distanță să se califice drept RDPS, absența acesteia ar trebui să împiedice produsul cu elemente digitale să își îndeplinească una dintre funcții. Noțiunea de „funcții” inclusă în această definiție nu se limitează la „funcționalitatea de bază” sau la „scopul preconizat” al produsului cu elemente digitale, întrucât CRA nu impune o astfel de limitare. Funcțiile care intră în domeniul de aplicare al CRA sunt atât funcții care îndeplinesc în mod direct scopul preconizat al produsului cu elemente digitale, astfel cum este experimentat de utilizatori, cât și funcții care sprijină performanța generală a produsului.

190. Printre exemplele de funcții în care poate avea loc prelucrarea datelor la distanță și care ar împiedica un produs cu elemente digitale să își îndeplinească vreuna dintre funcții se numără: (i) trimiterea de comenzi către un dispozitiv; (ii) sincronizarea fișierelor; (iii) integrarea utilizatorului; (iv) configurarea (personalizarea produsului cu elemente digitale); (v) distribuirea automată a actualizărilor, inclusiv actualizarea caracteristicilor și efectuarea corecțiilor de securitate; (vi) gestionarea identității și a accesului.

191. În unele cazuri, utilizatorul poate utiliza o funcție atât de la distanță, cât și manual (de exemplu, aprinderea unui bec cu ajutorul unei aplicații sau manual). Existența acestei opțiuni nu exclude calificarea ca RDPS a prelucrării datelor asociate cu îndeplinirea la distanță a funcției. Îndeplinirea acestei funcții de la distanță este, de asemenea, considerată ca făcând parte din funcțiile pe care le oferă produsul cu elemente digitale.

192. În schimb, în cazul în care absența unei anumite prelucrări a datelor nu împiedică produsul cu elemente digitale să își îndeplinească vreuna dintre funcții, o astfel de prelucrare nu este considerată RDPS în sensul CRA. Aceasta include, de exemplu, analiza la distanță a datelor telemetrice colectate exclusiv în scopuri statistice sau pentru dezvoltarea viitoare a produselor.

193. Cu toate acestea, chiar și atunci când prelucrarea datelor nu sprijină o funcție a unui produs cu elemente digitale, producătorii ar putea fi nevoiți să ia în considerare dacă respectivele componente la distanță generează riscuri pentru produsul cu elemente digitale ca parte a evaluării riscurilor în materie de securitate cibernetică (de exemplu, având în vedere mediul operațional al produsului) și să atenueze astfel de riscuri în consecință (de exemplu, prin măsuri de atenuare la nivel de produs).

194. Site-urile web reprezintă un caz specific care merită clarificări suplimentare, astfel cum se explică și în *secțiunea 2.1 Introducerea pe piață*. Site-urile web nu intră în domeniul de aplicare al RDPS dacă nu sprijină o funcție a unui produs cu elemente digitale, astfel cum se explică la considerentul 11 din CRA. Nu este suficient ca un site web să conțină informații cu privire la un produs cu elemente digitale pentru a se considera că intră în domeniul de aplicare al RDPS, chiar dacă produsul redirecționează către un astfel de site web. De exemplu, redirecționarea utilizatorilor către o pagină web externă care oferă informații și instrucțiuni utilizatorilor nu constituie RDPS. În schimb, un site web poate intra în domeniul de aplicare al RDPS dacă permite sau sprijină o funcție a unui produs cu elemente digitale. De exemplu, un portal de autentificare care emite acreditări sau tokenuri necesare pentru ca produsul cu elemente digitale să funcționeze ar fi considerat RDPS (cu condiția ca și celelalte criterii ale definiției să fie îndeplinite).

8.1.3. *Software-ul a fost proiectat și dezvoltat de producător sau sub responsabilitatea acestuia?*

195. Definiția care privește „prelucrarea de date la distanță” de la articolul 3 punctul 2 din CRA precizează, de asemenea, că software-ul unei astfel de prelucrări a datelor la distanță trebuie să fie proiectat și dezvoltat de producător sau sub responsabilitatea acestuia. Prelucrarea de date la distanță dezvoltată și proiectată integral de producător (intern) s-ar califica în mod firesc drept RDPS. Acest lucru ar fi valabil și în cazul în care producătorii se bazează pe un prestator extern de servicii pentru dezvoltarea și proiectarea unei soluții (și anume „sub responsabilitatea acestuia”). Expresia „sub responsabilitatea producătorului” se referă la soluțiile de prelucrare la distanță care sunt adaptate pentru producător. Acestea sunt cazuri în care producătorul nu acordă doar licențe pentru un produs cu elemente digitale sau un serviciu existent pe care un furnizor de servicii îl oferă clienților săi sau pentru versiuni ușor modificate ale acestuia. „[S]ub responsabilitatea producătorului” înseamnă că software-ul este construit exclusiv de către producător sau în numele acestuia, pe baza proiectelor și a specificațiilor furnizate de acesta.

196. Pentru a înțelege RDPS, noțiunea de „cine aplică soluția” nu este un factor decisiv, întrucât definiția CRA se referă numai la proiectarea și dezvoltarea RDPS. Acest aspect este în concordanță cu abordarea CRA, potrivit căreia cerințele și obligațiile îi vizează pe producători, și nu funcționarea produsului cu elemente digitale. În cazul în care producătorii proiectează și dezvoltă soluții, care sunt apoi exploatate de o parte terță, aceștia rămân responsabili pentru conformitatea cu cerințele esențiale prevăzute în CRA în ceea ce privește produsul cu elemente digitale pe care îl introduc pe piață.

197. Este necesar să se facă distincție între cazurile în care proiectarea și dezvoltarea sunt realizate de producători (sau sub responsabilitatea acestora) și cazurile în care se recurge la soluții furnizate de terți care nu sunt proiectate și dezvoltate de producători (sau sub responsabilitatea acestora). De exemplu, este util să se ia în considerare cele mai frecvente modele de servicii de cloud care oferă grade diferite de control al utilizatorilor și care sunt, de asemenea, menționate la considerentul 12 din CRA, și anume software ca serviciu (SaaS), platforma ca serviciu (PaaS) și infrastructura ca serviciu (IaaS).

198. În cazul unei soluții IaaS a unei părți terțe, producătorul nu gestionează sau controlează resursele fizice și virtuale subiacente (cum ar fi hardware-ul subiacent și hipervizorul furnizorului de servicii de cloud), ci este în măsură să implementeze și să ruleze software arbitrar utilizând astfel de resurse, cum ar fi aplicațiile și sistemele de operare. Un astfel de software este proiectat și dezvoltat de producător sau sub responsabilitatea acestuia și, prin urmare, se poate califica drept RDPS (dacă îndeplinește celelalte elemente ale definiției).

199. În cazul unei soluții PaaS oferite de o parte terță, producătorul își implementează propria aplicație (creată sau dobândită) utilizând limbaje de programare și medii de execuție puse la dispoziție de furnizorul de servicii de cloud și integrează aplicația în produsul său cu elemente digitale. Producătorul deține controlul asupra aplicației și, eventual, asupra setărilor de configurare pentru mediul de execuție. Astfel, aplicația este proiectată și dezvoltată de producător sau sub responsabilitatea acestuia și, prin urmare, se poate califica drept RDPS (dacă îndeplinește celelalte elemente ale definiției).

200. În cazul unei soluții SaaS oferite de o parte terță, furnizorul SaaS oferă producătorului o aplicație complet dezvoltată pentru a fi integrată în produsul cu elemente digitale al producătorului. Producătorul are o capacitate limitată de a gestiona setările de configurare ale aplicației specifice utilizatorului. Prin urmare, aplicația nu este proiectată și dezvoltată de producător sau sub responsabilitatea acestuia.

201. Cu toate acestea, în cazul în care anumite elemente nu se califică drept RDPS (de exemplu, hipervizorul în cazul unei infrastructuri IaaS terțe, sistemul de operare în cazul unei soluții PaaS terțe sau aplicația SaaS terță), dar sunt integrate în produsul cu elemente digitale într-un mod care afectează securitatea acestuia, astfel de soluții ar trebui considerate similare componentelor terțe. Producătorul trebuie să identifice și să evalueze riscurile legate de integrarea acestor elemente și să le abordeze prin punerea în aplicare a cerințelor esențiale privind produsul cu elemente digitale în sine. Acest aspect poate fi sprijinit, după caz, de funcțiile de securitate puse la dispoziție de furnizorul de servicii cloud prin modelul său de responsabilitate comună, în cazul în care producătorul utilizează sau configurează funcțiile respective pentru a aborda riscurile identificate. În plus, se preconizează că producătorul va exercita o obligație similară cu obligația de diligență necesară menționată la articolul 13 alineatul (5) în ceea ce privește securitatea acestor componente, într-un mod proporțional cu riscul pe care soluția la distanță îl prezintă pentru securitatea produsului cu elemente digitale.

202. Prin urmare, se poate rezuma că:

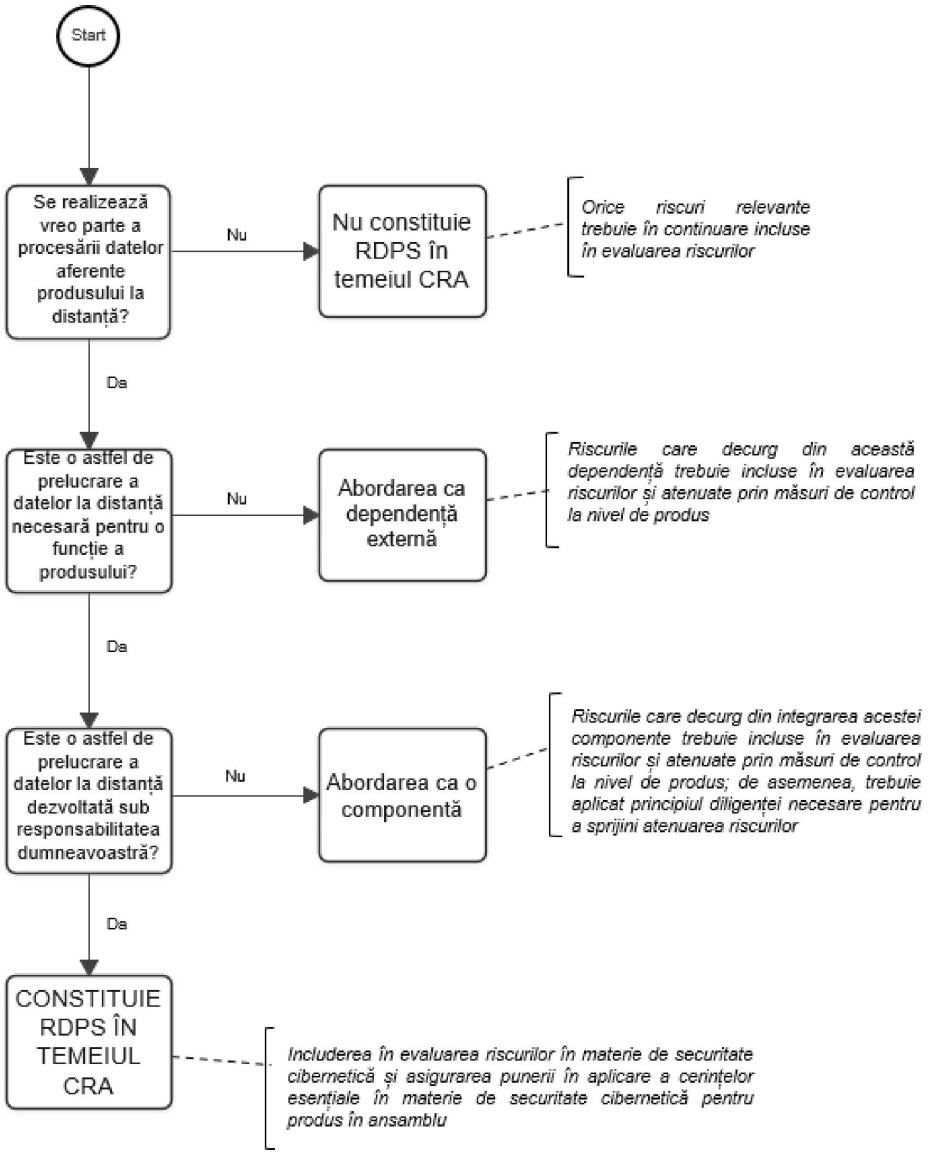
(a) Pentru ca prelucrarea datelor să se califice drept RDPS, răspunsul la ambele întrebări adresate în secțiunile *8.1.2 Absența unei astfel de prelucrări a datelor ar împiedica produsul cu elemente digitale să își îndeplinească vreuna dintre* funcții? și *8.1.3 Software-ul a fost proiectat și dezvoltat de producător sau sub responsabilitatea acestuia?* trebuie să fie afirmativ.

(b) În cazul în care răspunsul la întrebarea din secțiunea *8.1.2 Absența unei astfel de prelucrări a datelor ar împiedica produsul cu elemente digitale să își îndeplinească vreuna dintre funcții*? este negativ, producătorii ar trebui să evalueze riscurile care decurg din existența unei astfel de prelucrări a datelor în cadrul evaluării riscurilor.

(c) În cazul în care răspunsul la întrebarea din secțiunea *8.1.2 Absența unei astfel de prelucrări a datelor ar împiedica produsul cu elemente digitale să își îndeplinească vreuna dintre funcții*? este afirmativ, dar răspunsul la întrebarea din *8.1.3 Software-ul a fost proiectat și dezvoltat de producător sau sub responsabilitatea acestuia?* este negativ, producătorii ar trebui să trateze soluția oferită de terț drept componentă. În cadrul evaluării riscurilor, producătorii ar trebui să evalueze riscurile care decurg din integrarea unei astfel de soluții și să le atenueze în consecință. În plus, producătorii ar trebui să exercite diligența necesară.

Figura 9

Diagramă stilizată pentru a stabili dacă un produs cu elemente digitale conține RDPS



8.2. **Implicațiile practice și tehnice ale soluțiilor de prelucrare a datelor la distanță și dependența de soluțiile oferite de terți**

203. CRA urmează o abordare bazată pe riscuri, care este consacrată la articolul 13 alineatele (2) și (3), precum și în prima cerință esențială prevăzută în anexa I partea I, potrivit căreia „produsele cu elemente digitale sunt proiectate, dezvoltate și fabricate astfel încât să asigure un nivel adecvat de securitate cibernetică bazat pe riscuri”. În consecință, ar trebui luată în considerare o abordare bazată pe riscuri atunci când se aplică cerințele CRA în cazul RDPS și abordarea riscurilor care decurg din serviciile furnizate de terți integrate în produsul cu elemente digitale.

204. În primul rând, producătorii ar trebui (i) să indice în documentația tehnică dacă produsul lor cu elemente digitale are RDPS ori se bazează pe soluții la distanță furnizate de terți și (ii) să descrie astfel de soluții. Dacă aceeași RDPS susține mai multe produse cu elemente digitale, RDPS trebuie declarată în documentația tehnică a fiecărui produs. Documentația privind RDPS care deservește mai multe produse cu elemente digitale poate fi reutilizată de la o evaluare a conformității produsului la alta.

205. Astfel cum se indică la considerentul 11, RDPS care fac parte din produsul cu elemente digitale și, prin urmare, fac obiectul evaluării conformității produsului ar trebui să se limiteze la modulele software care sunt responsabile pentru funcționalitatea produsului cu elemente digitale și la interfețele pe care modulele respective le utilizează cu servicii externe. Alte sisteme *back-end* care efectuează prelucrarea ulterioară și cu care produsul cu elemente digitale nu interacționează în mod direct nu sunt considerate RDPS.

206. Cu toate acestea, sistemele *back-end* respective rămân dependențe externe care trebuie evaluate în cadrul evaluării riscurilor în materie de securitate cibernetică și atenuate prin măsuri la nivel de produs. În fapt, evaluarea riscurilor efectuată de producător ar trebui să aibă în vedere: (i) riscurile legate de RDPS; (ii) riscurile legate de dependența de soluții la distanță oferite de terți (similare componentelor furnizate de terți) și (iii) riscurile legate de mediul produsului (de exemplu, hardware-ul subiacent). Producătorii ar trebui să pună în aplicare ei înșiși controale de securitate asupra produsului cu elemente digitale pentru a atenua aceste riscuri.

207. În plus, ca parte a evaluării conformității și/sau a îndeplinirii obligațiilor de diligență legate de serviciile furnizate de terți la distanță, următoarea listă neexhaustivă de artefacte de asigurare poate fi reutilizată în sprijinul evaluării producătorului:

(a) dovada îndeplinirii obligațiilor în temeiul Regulamentului de punere în aplicare (UE) 2024/2690 al Comisiei;

(b) dovada îndeplinirii obligațiilor în temeiul Regulamentului (UE) 2022/2554 (DORA);

(c) declarația de conformitate sau certificatul obținut în cadrul unui sistem european de certificare de securitate cibernetică [adoptat în temeiul Regulamentului (UE) 2019/881 – Regulamentul privind securitatea cibernetică];

(d) dovada conformității cu ISO/IEC 27017:2015 sau cu ISO/IEC 27001:2022.

208. În cele din urmă, în interacțiunile lor cu furnizorii terți de servicii la distanță, producătorii trebuie să pună în aplicare cele mai adecvate măsuri de securitate pe baza evaluării riscurilor (și, după caz, susținute de modelul de responsabilitate partajată al furnizorului). Aceste măsuri de atenuare ar trebui să includă controale de securitate pentru produsele lor cu elemente digitale și verificarea măsurilor de securitate furnizate chiar de furnizorii terți (diligența necesară). Un instrument de atenuare a acestor riscuri poate fi integrarea garanțiilor de securitate în acordurile lor privind nivelul serviciilor (SLA) cu furnizorii terți, inclusiv asigurările că furnizorii gestionează în mod adecvat vulnerabilitățile. O modificare majoră a soluțiilor oferite de furnizorii terți de servicii la distanță nu ar trebui să se califice drept modificare substanțială a produsului cu elemente digitale, deoarece aceste elemente nu se află în responsabilitatea producătorului. Cu toate acestea, ca parte a obligațiilor lor de diligență necesară și pentru a atenua în mod corect riscurile care decurg din utilizarea de către furnizorii terți, producătorii sunt încurajați să se asigure că furnizorii lor terți de servicii de cloud îi informează în mod adecvat cu privire la modificările pe care le pun în aplicare în ceea ce privește soluțiile lor. Pe baza acestor informații, producătorii ar putea fi nevoiți să își reexamineze evaluarea riscurilor. Evaluarea actualizată a riscurilor ar trebui să analizeze dacă furnizorii terți de servicii oferă în continuare garanții suficiente în ceea ce privește securitatea cibernetică și dacă controalele de securitate la nivel de produs sunt în continuare adecvate. În unele cazuri, producătorii ar putea fi nevoiți să modifice astfel de controale sau să schimbe furnizorii terți de servicii.

8.3. **Cazuri de utilizare pentru soluții de prelucrare a datelor la distanță**

Pentru a oferi orientări practice suplimentare producătorilor, prezenta secțiune introduce o serie de cazuri de utilizare fictivă, descriind produsele arhetipale cu elemente digitale care se bazează pe prelucrarea datelor la distanță și ilustrând dacă o astfel de prelucrare se califică drept soluții de prelucrare a datelor la distanță în sensul CRA.

8.3.1. *Aplicația pentru servicii bancare prin telefonul mobil*

O entitate financiară introduce pe piață o aplicație pentru servicii bancare prin telefonul mobil. Sistemele *back-end* ale aplicației sprijină, printre altele, autentificarea, autorizarea, gestionarea conturilor și plățile. Entitatea financiară utilizează o strategie hibridă care se bazează pe infrastructura internă, precum și pe soluții de la distanță ale terților pentru a sprijini funcționalitățile aplicației. Printre acestea se numără:

Infrastructura negăzduită dezvoltată de entitatea financiară:

— Clientul deschide aplicația pentru servicii bancare prin telefonul mobil și este autentificat prin intermediul interfeței bancare, o soluție negăzduită dezvoltată de entitatea financiară care primește cererile aplicației și returnează răspunsurile corespunzătoare. Interfața bancară verifică identitatea clientului prin interogarea sistemului de gestionare a conturilor și acordă acces la aplicație.

— Clientul inițiază un transfer prin intermediul aplicației. Aplicația transmite instrucțiunea către interfața bancară, care transmite o cerere corespunzătoare către sistemul de registre.

— Sistemul de gestionare a conturilor și sistemul de registre, atât cele negăzduite, cât și cele separate logic de interfața bancară, înregistrează tranzacția.

— Sistemul de registre raportează statutul tranzacției către interfața bancară, care prezintă rezultatul clientului.

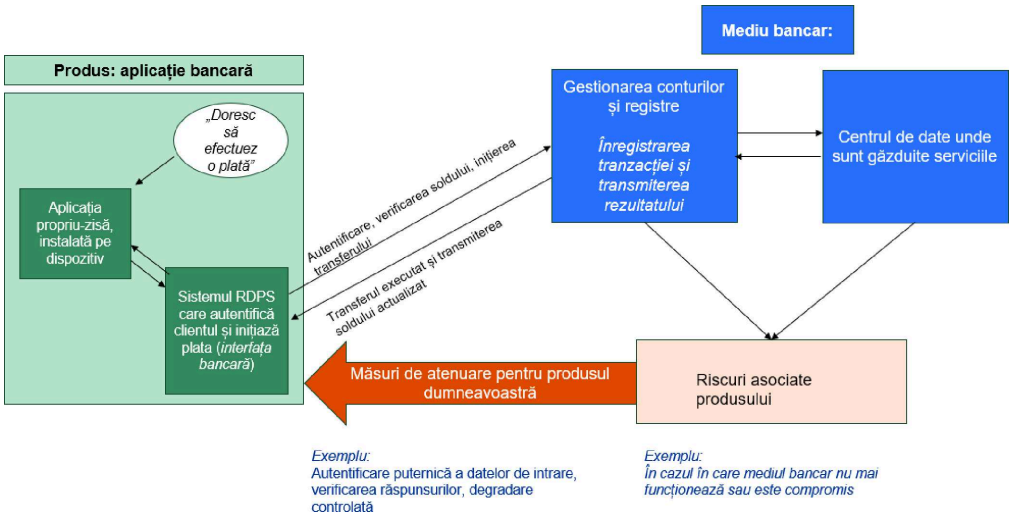
Implicații pentru RDPS:

— Interfața bancară este necesară pentru ca aplicația să își îndeplinească funcțiile, și anume autentificarea clientului, transmiterea instrucțiunilor clientului, inclusiv a instrucțiunilor de plată și de transfer, precum și raportarea statutului rezultat. Interfața bancară este proiectată și dezvoltată sub responsabilitatea producătorului. Întrucât răspunsul la ambele întrebări prezentate în secțiunile anterioare este afirmativ, interfața bancară trebuie considerată RDPS. Prin urmare, aceasta trebuie inclusă în evaluarea riscurilor în materie de securitate cibernetică și în punerea în aplicare a cerințelor esențiale pentru produsul cu elemente digitale în ansamblu. Prelucrarea ulterioară a unei instrucțiuni, odată transmisă, în special înregistrarea tranzacției în sistemele de gestionare a conturilor și de registre, de decontare și de compensare, este efectuată de sisteme cu care aplicația nu interacționează în mod direct și nu constituie, pe această bază, RDPS.

— Sistemul de gestionare a conturilor și sistemul de registre nu se califică drept RDPS pentru aplicația bancară. Aplicația nu interacționează direct cu acestea (ci interacționează cu interfața bancară, care, la rândul său, se bazează pe acestea). Deși disponibilitatea acestora poate fi necesară pentru finalizarea unei funcții, CRA acoperă numai acele părți ale sistemului care interacționează direct cu produsul cu elemente digitale. Prin urmare, acestea nu se încadrează în definiția RDPS în sensul CRA. Cu toate acestea, sistemele respective rămân dependențe externe care pot genera riscuri semnificative în materie de securitate cibernetică pentru produsul cu elemente digitale. De exemplu, compromiterea sistemului de registre ar putea permite unui atacator să influențeze rezultatele tranzacțiilor care sunt afișate ulterior în aplicație. Prin urmare, producătorul trebuie să identifice și să evalueze riscurile respective în cadrul evaluării riscurilor în materie de securitate cibernetică și să le atenueze prin măsuri la nivel de produs, cum ar fi autentificarea strictă a interfețelor *back-end*, protecția integrității datelor privind tranzacțiile, canalele de comunicare securizată și verificarea răspunsurilor primite de aplicație.

Figura 10

Reprezentare stilizată a unei aplicații bancare care se bazează pe RDPS



SaaS furnizat de terți pentru asistența oferită clienților:

— Entitatea financiară integrează în aplicația sa o soluție de chat de asistență pentru clienți dezvoltată și operată de un furnizor terț; furnizorul terț a scris codul serverului de chat, a construit interfața pentru utilizatori și operează infrastructura în care este implementat chatul (și anume modelul SaaS).

— Atunci când clientul inițiază o cerere de asistență, aplicația conectează clientul la serviciul furnizat de terți pentru a stabili o sesiune de chat și pentru a gestiona fluxul de mesagerie, fără a oferi terțului acces la sistemele bancare de bază.

Implicații pentru RDPS:

— Soluția de chat de asistență este necesară pentru ca produsul cu elemente digitale să își îndeplinească una dintre funcții, dar nu este proiectată și dezvoltată de entitatea financiară sau sub responsabilitatea acesteia; prin urmare, aceasta nu este RDPS. Cu toate acestea, ar trebui tratată ca o componentă terță. Recurgerea la acest serviciu furnizat de terți poate crea riscuri în materie de securitate cibernetică pentru aplicația bancară, de exemplu în cazul în care un atacator ar utiliza canalul de chat pentru a uzurpa identitatea băncii sau pentru a furniza conținut dăunător utilizatorilor. Entitatea financiară trebuie să țină seama de aceste riscuri în evaluarea riscurilor în materie de securitate cibernetică și să le atenueze prin măsuri la nivel de produs, cum ar fi izolarea funcției de chat de caracteristicile bancare de bază, controlul fluxurilor de date și validarea conținutului. De asemenea, ar trebui exercitată diligența necesară în ceea ce privește SaaS.

8.3.2. *Termostat inteligent*

Un termostat inteligent le permite utilizatorilor să controleze temperatura locuințelor lor prin intermediul unei aplicații mobile. Aplicația mobilă și termostatul inteligent se bazează pe prelucrarea datelor la distanță pentru a face schimb de date (de exemplu, cerere de creștere a temperaturii) și pentru a stoca date (de exemplu, preferințele utilizatorilor). Aceste funcții au fost dezvoltate și proiectate sub responsabilitatea producătorului, dar funcționează pe o infrastructură fizică și virtuală subiacentă furnizată de un terț (IaaS terță).

Întrucât termostatul inteligent nu ar fi în măsură să își îndeplinească funcționalitățile inteligente fără această prelucrare de date la distanță, absența sa ar împiedica produsul cu elemente digitale să își îndeplinească una sau mai multe dintre funcții. În plus, software-ul a fost dezvoltat și proiectat sub responsabilitatea producătorului de termostate inteligente. Prin urmare, prelucrarea datelor la distanță se califică drept RDPS, astfel cum definește CRA.

În scopul respectării CRA, producătorul termostatului inteligent trebuie să documenteze RDPS, precum și dependența de IaaS terță în documentația tehnică a produsului cu elemente digitale, inclusiv detaliile serviciului contractat. Producătorul trebuie să ia în considerare aceste elemente în evaluarea riscurilor, care include scopul preconizat și utilizarea previzibilă în mod rezonabil a produsului cu elemente digitale. Producătorul pune în aplicare cerințele esențiale prevăzute în CRA pe baza riscurilor asociate RDPS. Pentru IaaS terță, producătorul trebuie să se asigure că măsurile de securitate asigurate de furnizorul terț sunt adecvate și/sau să ia măsurile relevante în ceea ce privește infrastructura. În cazul celor dintâi, producătorul ar putea, de exemplu, să solicite dovezi că obligațiile NIS 2 au fost îndeplinite.

8.3.3. *e-Reader*

Producătorul unui program informatic e-Reader (cititor electronic) utilizează un serviciu de stocare SaaS terț pentru a stoca cărți electronice achiziționate de clienți și pentru a le permite acestora să aibă acces la cărțile lor. Absența acestui serviciu de stocare ar împiedica produsul cu elemente digitale să își îndeplinească una dintre funcții, dar serviciul de stocare SaaS terț nu este dezvoltat de producător sau sub responsabilitatea acestuia; furnizorul SaaS îl pune la dispoziția clienților pentru orice caz de utilizare.

Serviciul de stocare SaaS nu se încadrează în definiția RDPS. Cu toate acestea, producătorul de cititoare electronice se bazează pe acest serviciu extern pentru funcționarea produsului său cu elemente digitale și, prin urmare, trebuie să țină seama de riscurile asociate în evaluarea riscurilor în materie de securitate cibernetică. Producătorul cititorului electronic ar trebui să trateze SaaS ca pe o componentă. Producătorul trebuie să pună în aplicare măsuri de securitate adecvate la nivel de produs, cum ar fi autentificarea securizată, criptarea și protecția integrității comunicațiilor cu serviciul de stocare. Diligența necesară la selectarea și integrarea furnizorului SaaS va sprijini, de asemenea, obligațiile producătorului, astfel încât produsul cu elemente digitale în ansamblu să poată respecta cerințele esențiale.

8.3.4. *Robot industrial*

Un robot industrial are sarcina de a colecta piese. Robotul trimite informațiile colectate prin intermediul camerelor către un serviciu la distanță proiectat și dezvoltat de producător. Acest serviciu funcționează pe o infrastructură fizică și virtuală subiacentă asigurată de un furnizor terț de servicii (IaaS terț). Serviciul cloud calculează poziția unei piese pe baza fluxurilor camerei și trimite comenzile înapoi către robot pentru a colecta piesele.

Absența acestei prelucrări a datelor ar împiedica robotul industrial să colecteze piese și, prin urmare, să își îndeplinească una dintre funcții. În plus, software-ul care funcționează pe lângă infrastructură a fost proiectat și dezvoltat de producător. Software-ul proiectat și dezvoltat de producător se încadrează în definiția RDPS.

Producătorul robotului industrial trebuie să documenteze RDPS, precum și dependența de IaaS terț în documentația tehnică a produsului cu elemente digitale (inclusiv detalii privind serviciul contractat). Producătorul trebuie, de asemenea, să ia în considerare aceste elemente în evaluarea riscurilor, care include scopul preconizat și utilizarea previzibilă în mod rezonabil a produsului cu elemente digitale. Producătorul pune în aplicare cerințele esențiale prevăzute în CRA privind produsul cu elemente digitale, inclusiv RDPS, pe baza riscurilor. Diligența necesară la selectarea furnizorului IaaS va sprijini, de asemenea, obligațiile producătorului. De exemplu, producătorul ar putea solicita dovezi că obligațiile NIS 2 au fost îndeplinite.

8.3.5. *Rețeaua celulară*

Un telefon inteligent se bazează pe o rețea 5G pentru a oferi conexiune la internet, apeluri telefonice și mesaje utilizatorilor săi (conectivitate mobilă). Rețeaua celulară este dezvoltată și proiectată de operatorii de telecomunicații. Rețeaua cuprinde microcelule și turnuri celulare, precum și alte echipamente de rețea.

Produsul cu elemente digitale ar trebui să se poată conecta corect la o rețea; aceasta este una dintre funcțiile sale. Cu toate acestea, faptul că rețeaua respectivă este sau nu în funcțiune nu este relevant pentru a stabili dacă produsul cu elemente digitale funcționează corect. Rețeaua este doar un canal de comunicare și nu este necesară pentru ca produsul cu elemente digitale să își îndeplinească funcția de „conectare corectă la o rețea”. În mod similar, un cablu ethernet, un router sau un semnal Wi-Fi nu se consideră prelucrare de date a cărei absență ar împiedica produsul cu elemente digitale să își îndeplinească vreuna dintre funcții, ci mai degrabă un factor de facilitare a comunicării/conectivității.

În consecință, rețeaua celulară nu se încadrează în definiția RDPS. Rețeaua nu ar trebui considerată o componentă terță, deoarece nu există niciun software integrat în produsul cu elemente digitale, ci produsul se bazează doar pe această rețea. Ca atare, nu este necesar ca producătorul să exercite obligații de diligență față de furnizorul de rețea.

9. **ELEMENTE SUPLIMENTARE**

9.1. **Obligații de raportare**

209. În temeiul articolului 14 alineatele (1) și (3) din CRA, un producător are obligația de a notifica simultan către CSIRT desemnată drept coordonator, precum și către ENISA (i) orice vulnerabilitate exploatată activ conținută în produsul său cu elemente digitale de care ia cunoștință și (ii) orice incident grav care are un impact asupra securității produsului cu elemente digitale de care ia cunoștință.

210. În conformitate cu articolul 69 alineatul (3) și cu articolul 71 alineatul (2) a doua teză, obligația de a respecta articolul 14 se aplică de la 11 septembrie 2026 tuturor produselor cu elemente digitale care intră în domeniul de aplicare al CRA, inclusiv produselor cu elemente digitale introduse pe piață înainte de 11 decembrie 2027. În plus, spre deosebire de obligațiile de gestionare a vulnerabilităților, care continuă numai pe durata perioadei de asistență a unui produs, obligațiile de raportare continuă să se aplice după ce un produs cu elemente digitale nu mai beneficiază de asistență. În cazul în care un produs cu elemente digitale a fost introdus pe piață înainte de 11 decembrie 2027 sau în cazul în care perioada sa de asistență s-a încheiat, producătorul nu este obligat să respecte obligațiile de gestionare a vulnerabilităților prevăzute în anexa I partea II.

211. Ar trebui reamintit faptul că obligația de a notifica astfel de evenimente se aplică din momentul în care producătorul ia cunoștință de faptul că o vulnerabilitate este exploatată activ sau că a avut loc un incident grav care a condus la compromiterea securității produsului său cu elemente digitale. Prin urmare, orientările privind momentul în care se consideră că un producător a luat cunoștință de acest lucru ar trebui să îi ajute pe producători să stabilească momentul în care încep să curgă termenele de raportare aplicabile.

212. Producătorii pot fi supuși unor obligații de raportare comparabile în temeiul diferitelor acte ale UE. Pentru a se asigura că, în ceea ce privește conceptul de „luare la cunoștință”, acesta este interpretat în mod consecvent și pentru a facilita respectarea de către producători a acestor obligații, prezentele orientări sunt aliniate la considerentul 31 din Regulamentul de punere în aplicare (UE) 2024/2690 al Comisiei și la secțiunea II litera (A) din Orientările 9/2022 privind notificarea încălcării securității datelor cu caracter personal în temeiul RGPD.

213. În unele cazuri, un producător va detecta un eveniment suspect sau o parte terță, cum ar fi o persoană fizică, un client, o entitate, o autoritate, o organizație mass-media sau o altă sursă, îi va aduce la cunoștință un potențial incident sau o potențială vulnerabilitate. În astfel de cazuri, producătorul ar trebui să evalueze imediat evenimentul suspect pentru a stabili dacă acesta constituie o vulnerabilitate exploatată activ sau un incident grav care are un impact asupra securității produsului cu elemente digitale. Prin urmare, trebuie să se considere că producătorul a luat cunoștință de faptul că, după o astfel de evaluare inițială, are un grad rezonabil de certitudine că: (i) o vulnerabilitate conținută în produsul său cu elemente digitale este exploatată în mod activ; sau (ii) a avut loc un incident grav și a condus la compromiterea securității produsului său cu elemente digitale.

214. Prin urmare, momentul în care se poate considera că un producător are cunoștință va depinde de circumstanțele vulnerabilității specifice exploatate activ sau ale incidentului grav. În unele cazuri, va fi relativ clar de la bun început că o vulnerabilitate este exploatată în mod activ sau că un incident grav afectează securitatea unui produs cu elemente digitale. În altele, poate fi necesară o perioadă de timp pentru a stabili dacă un produs cu elemente digitale este afectat de o vulnerabilitate și dacă vulnerabilitatea respectivă este exploatată de un actor rău-intenționat sau dacă un incident afectează securitatea unui produs cu elemente digitale. Cu toate acestea, accentul ar trebui pus pe acțiuni prompte pentru a efectua evaluarea inițială cu scopul de a stabili dacă astfel de condiții sunt într-adevăr îndeplinite, în special în cazul în care vulnerabilitatea poate prezenta un risc semnificativ, și, în caz afirmativ, pentru a lua măsuri de remediere și a efectua notificări în conformitate cu dispozițiile CRA.

215. În plus, structura obligațiilor de raportare impune producătorilor să își actualizeze treptat notificările, pe măsură ce investigațiile lor interne avansează, iar cunoștințele lor cu privire la vulnerabilitatea exploatată activ sau la incident devin mai detaliate. În special, producătorii au obligația de a transmite o notificare de alertă timpurie care să conțină informații limitate, fără întârzieri nejustificate și, în orice caz, în termen de 24 de ore de la luarea la cunoștință. Ulterior, sunt necesare informații suplimentare ca parte a notificării care trebuie transmisă fără întârzieri nejustificate și, în orice caz, în termen de 72 de ore de la luarea la cunoștință („notificare în termen de 72 de ore”). Raportul complet trebuie prezentat în termen de 14 zile de la data la care este disponibilă o măsură corectivă sau de atenuare pentru vulnerabilitățile exploatate activ sau în termen de o lună de la notificarea în termen de 72 de ore pentru incidentele grave.

216. Astfel cum s-a reamintit și în secțiunea *3.3.1 Asistență susținută și asigurarea viabilității FOSS*, administratorii de software cu sursă deschisă au, de asemenea, obligația de a raporta vulnerabilitățile exploatate activ, în conformitate cu articolul 24 alineatul (3) ([30]). Această obligație se aplică din momentul în care se ia cunoștință de o vulnerabilitate exploatată activ și nu doar în cazul în care există o vulnerabilitate în baza de cod a unui FOSS pentru care entitatea respectivă este administrator. În practică, deoarece componentele FOSS sunt, de regulă, integrate în aval în alte produse cu elemente digitale, este probabil ca un administrator să aibă cunoștință de exploatarea activă prin intermediul rapoartelor terților, care identifică exploatarea în componentele FOSS ca fiind integrată în alte produse cu elemente digitale. Acest lucru se poate întâmpla, de exemplu, în cazul în care un producător al unui produs cu elemente digitale detectează exploatarea activă într-o componentă FOSS integrată în propriul produs și o raportează administratorului componentei respective; sau atunci când un utilizator sau un cercetător în domeniul securității găsește dovezi ale exploatării unei componente FOSS integrate într-un produs cu elemente digitale și raportează această exploatare activă administratorului componentei.

217. De asemenea, ar trebui să se clarifice faptul că, întrucât obligația de raportare a vulnerabilităților exploatate activ se aplică atunci când producătorul ia cunoștință de exploatarea activă, producătorul nu este obligat să raporteze vulnerabilitățile de a căror exploatare activă a luat deja cunoștință înainte de 11 septembrie 2026 (data la care începe să se aplice obligația de raportare). Prin urmare, CRA nu impune raportarea retroactivă a unor astfel de vulnerabilități. În schimb, obligația se aplică în cazul în care producătorul avea cunoștință de o vulnerabilitate înainte de 11 septembrie 2026, dar nu avea cunoștință, la momentul respectiv, de nicio exploatare activă a acesteia (fie pentru că nu avusese încă loc, fie pentru că producătorul nu o luase la cunoștință). În cazul în care, după 11 septembrie 2026, are loc ulterior o exploatare activă sau producătorul ia cunoștință de aceasta, vulnerabilitatea este considerată o vulnerabilitate exploatată activ care face obiectul obligației de raportare.

218. În mod similar, un producător are doar obligația de a raporta vulnerabilitățile exploatate activ conținute în produsul său cu elemente digitale. În cazul în care un produs cu elemente digitale conține o vulnerabilitate exploatată activ care provine de la o componentă terță, producătorul produsului cu elemente digitale are obligația de a notifica respectiva vulnerabilitate exploatată activ. Cu toate acestea, în cazul în care un producător are cunoștință de faptul că o componentă terță conține o vulnerabilitate, dar că vulnerabilitatea fie (i) nu poate fi exploatată în produsul său cu elemente digitale (de exemplu, deoarece codul vulnerabil nu este accesibil), fie (ii) nu a fost exploatată în produsul său cu elemente digitale, vulnerabilitatea respectivă nu se califică drept vulnerabilitate exploatată activ conținută în produsul său cu elemente digitale și, prin urmare, nu face obiectul raportării obligatorii pentru producătorul respectiv. Producătorul respectiv poate notifica în continuare vulnerabilitatea respectivă în mod voluntar, în conformitate cu articolul 15 din CRA. De asemenea, îi revine și obligația de a respecta cerințele de gestionare a vulnerabilităților prevăzute în partea II din anexa I la CRA, precum și de a raporta vulnerabilitatea respectivă persoanei sau entității care produce sau întreține componenta în cauză, în conformitate cu articolul 13 alineatul (6) și astfel cum se explică în detaliu în secțiunea *9.2.1 Raportarea în amonte și partajarea soluțiilor de securitate*.

([30]) În măsura în care administratorul este implicat în dezvoltarea unui produs cu elemente digitale.

219. După ce iau cunoștință de o vulnerabilitate exploatată activ sau de un incident grav, producătorilor le revine, de asemenea, obligația, în conformitate cu articolul 14 alineatul (8), de a informa utilizatorii afectați și, după caz, toți utilizatorii. În cazul în care informarea nu are lor în timp util, CSIRT care au primit notificarea pot furniza astfel de informații utilizatorilor atunci când ele sunt considerate a fi proporționale și necesare pentru prevenirea sau atenuarea impactului incidentului sau al vulnerabilității respective.

220. În conformitate cu abordarea bazată pe riscuri a CRA, obligația de a informa utilizatorii prevăzută la articolul 14 alineatul (8) trebuie aplicată în mod proporțional și bazat pe riscuri. În special, furnizarea de informații cu privire la o vulnerabilitate exploatată activ sau la un incident grav nu implică faptul că astfel de informații trebuie să fie făcute publice sau divulgate în mod nediscriminatoriu. După caz și având în vedere natura produsului cu elemente digitale, utilizatorii afectați și impactul potențial al vulnerabilității sau al incidentului, producătorii pot limita divulgarea de informații detaliate la utilizatorii sau clienții relevanți în cauză. Acest aspect este valabil în special pentru produsele cu elemente digitale utilizate în medii sensibile sau esențiale, în care divulgarea publică a detaliilor tehnice ar putea, la rândul său, să sporească riscurile în materie de securitate cibernetică sau să faciliteze exploatarea ulterioară.

221. Odată ce vulnerabilitatea a fost abordată sau atenuată în mod adecvat, se poate dovedi oportună o divulgare mai amplă. Acest aspect ar fi valabil, de exemplu, în cazul în care divulgarea contribuie la sensibilizarea opiniei publice sau permite utilizatorilor să verifice faptul că produsele lor cu elemente digitale nu mai sunt afectate. În astfel de cazuri, nivelul de detaliere și momentul oricărei divulgări mai ample ar trebui să își mențină caracterul proporțional și să țină seama de riscurile reziduale de exploatare, de natura produsului cu elemente digitale și de interesele utilizatorilor în cauză. În plus, punctul 4 din partea II a anexei I impune producătorilor să publice informații cu privire la vulnerabilitățile remediate, după punerea la dispoziție a unei actualizări de securitate.

9.2. **Gestionarea vulnerabilităților**

9.2.1. *Raportarea în amonte și partajarea soluțiilor de securitate*

222. Articolul 13 alineatul (6) din CRA prevede obligația producătorilor de a raporta vulnerabilitățile componentelor integrate persoanei sau entității care produce sau întreține componenta respectivă („raportarea în amonte”).

223. Producătorii au obligația de a raporta în amonte numai cu privire la versiunea componentei pe care o integrează. În cazul în care persoana sau entitatea care produce sau întreține componenta stabilește politici de securitate, procese de divulgare coordonată a vulnerabilităților sau canale desemnate pentru raportarea vulnerabilităților, producătorii ar trebui să raporteze în conformitate cu acestea, în special în cazul în care divulgarea prematură a vulnerabilităților neremediate ar putea crește riscurile în materie de securitate cibernetică. În plus, pentru a reduce sarcina asupra operatorilor de întreținere din amonte, în special în cazul proiectelor cu sursă deschisă, producătorii nu sunt obligați să raporteze în amonte în cazul în care pot confirma că persoana sau entitatea care produce sau întreține o componentă are cunoștință de existența unei vulnerabilități. Producătorii sunt încurajați să ia măsuri rezonabile pentru a evita transmiterea de rapoarte duble, de exemplu prin verificarea bazelor de date în materie de vulnerabilități accesibile publicului, a avertismentelor de securitate specifice proiectului sau a dispozitivelor consacrate de urmărire a problemelor înainte de raportarea în amonte.

224. Producătorii au obligația de a raporta în amonte numai vulnerabilitățile care există în componenta integrată în sine și nu vulnerabilitățile care există ca urmare a integrării între componentă și alt cod dezvoltat de producător sau prin integrarea altor componente. Cu toate acestea, pot exista situații în care integrarea unei componente într-un produs specific cu elemente digitale dezvăluie anumite comportamente, interacțiuni sau caracteristici relevante pentru securitate ale componentei respective care nu reieșeau în mod clar sau nu erau ușor de identificat în mod izolat. În astfel de cazuri, producătorii sunt încurajați să comunice aceste informații persoanei sau entității care produce sau întreține componenta, pentru a promova bune practici de gestionare a vulnerabilităților menite să faciliteze remedierea eficace și să îmbunătățească securitatea generală a ecosistemului componentelor.

225. În cele din urmă, producătorii nu sunt obligați nici să raporteze vulnerabilitatea în amonte în cazul în care componenta nu mai beneficiază de un operator de întreținere sau în cazul în care producătorul nu se mai bazează pe operatorul inițial de întreținere pentru noi versiuni sau soluții de securitate. În astfel de cazuri, producătorul este totuși încurajat să informeze utilizatorii cu privire la componenta respectivă prin măsuri alternative rezonabile, de exemplu prin intermediul mecanismelor comunitare existente (cum ar fi listele de adrese sau crearea de tichete) sau prin intermediul evidențelor publice privind vulnerabilitatea.

226. În plus, în temeiul articolului 13 alineatul (6), producătorii care au realizat o modificare a software-ului pentru a aborda o vulnerabilitate a unei componente integrate au obligația de a partaja respectiva modificare a software-ului („soluție de securitate”) cu persoana sau entitatea care produce sau întreține componenta („partajare în amonte”).

227. În cazul în care producătorilor li se solicită să partajeze o soluție de securitate în temeiul articolului 13 alineatul (6), soluția ar trebui, după caz, să fie furnizată într-un format care poate fi citit automat, într-un mod care să poată fi ușor verificat și, după caz, integrat de către persoana sau entitatea care produce sau întreține componenta în cauză. În cazul în care componenta este o componentă liberă și cu sursă deschisă, soluția de securitate ar trebui partajată într-un mod compatibil cu licența componentei respective, de exemplu prin partajarea sa în temeiul aceleiași licențe sau în temeiul unei licențe care îi permite operatorului de întreținere să distribuie soluția în temeiul propriei licențe. În cazul în care operatorul de întreținere a componentei respective dispune de orientări cu privire la modul în care ar trebui partajate soluțiile de securitate, producătorul ar trebui să respecte orientările respective.

228. Cu toate acestea, CRA nu impune producătorilor să se asigure că soluțiile lor de securitate sunt în mod necesar acceptate de persoana sau entitatea care produce sau întreține componenta. De asemenea, ei nu sunt obligați să se asigure că aceste soluții sunt în mod necesar integrate în registrul de coduri al componentei, de exemplu în cazul în care operatorul de întreținere poate prefera o opțiune diferită pentru a soluționa problema. În mod similar, producătorii nu sunt obligați să accepte o soluție propusă elaborată de operatorul de întreținere a componentei și ar putea prefera să atenueze problema în alte moduri adecvate.

229. În unele cazuri, este posibil ca persoana sau entitatea care produce sau întreține componenta să fi furnizat deja o soluție de securitate pentru a aborda vulnerabilitatea, dar un producător pune în aplicare o strategie de atenuare diferită (de exemplu, prin modificarea unei configurații diferite). În astfel de cazuri, CRA nu prevede obligația producătorului de a partaja modificarea unei alte părți a sistemului în amonte. Cu toate acestea, producătorul este încurajat să acționeze în acest sens în cazul în care acest lucru poate sprijini persoana sau entitatea care întreține componenta.

9.2.2. *Vulnerabilități exploatabile cunoscute*

230. Una dintre cerințele esențiale prevăzute în partea I a anexei I la CRA prevede că, pe baza evaluării riscurilor în materie de securitate cibernetică menționate la articolul 13 alineatul (2) și, după caz, produsele cu elemente digitale trebuie să fie puse la dispoziție pe piață fără vulnerabilități exploatabile cunoscute.

231. Articolul 3 punctul 41 definește „vulnerabilitatea exploatabilă” ca fiind „o vulnerabilitate care poate fi utilizată în mod eficace de un adversar în condiții operaționale practice”. Nu toate vulnerabilitățile sunt exploatabile în condiții operaționale practice, iar unele vulnerabilități pot fi exploatate numai în condiții teoretice (de exemplu, într-un laborator sau într-o simulare) și/sau nu în condiții care ar apărea în mediul operațional al unui produs cu elemente digitale.

232. CRA prevede obligația producătorilor de a dispune de politici și proceduri adecvate pentru a gestiona și a remedia vulnerabilitățile potențiale raportate din surse interne sau externe [articolul 13 alineatul (8)]. Cu toate acestea, nu specifică în mod explicit când ar trebui să se considere că o vulnerabilitate exploatabilă este cunoscută de producător, declanșând astfel obligația de a respecta această cerință esențială în momentul introducerii pe piață.

233. O vulnerabilitate ar trebui considerată cunoscută atunci când este inclusă în bazele de date relevante privind vulnerabilitățile accesibile publicului, cum ar fi baza de date europeană a vulnerabilităților instituită prin articolul 12 alineatul (2) din Directiva (UE) 2022/2555 sau alte baze de date importante privind vulnerabilitățile.

234. În plus, o vulnerabilitate poate fi cunoscută și atunci când producătorul a luat cunoștință cu privire la aceasta prin intermediul unor informații care nu sunt publice, de exemplu prin divulgarea coordonată de către un cercetător în domeniul securității sau prin propriile teste și analize interne ale producătorului, inclusiv, de exemplu, atunci când utilizează servicii bazate pe IA. De asemenea, o vulnerabilitate poate fi cunoscută atunci când este raportată public și în mod vizibil în canale mass-media fiabile, inclusiv în publicații specializate în materie de securitate cibernetică sau în mass-media generală.

235. Cu toate acestea, simplul fapt că o vulnerabilitate este raportată sau constatată nu înseamnă, în sine, că aceasta este exploatabilă în practică sau aplicabilă produsului specific cu elemente digitale în cauză. Producătorul va trebui să investigheze acest lucru și să confirme veridicitatea acestor informații și aplicabilitatea lor la propriul produs cu elemente digitale. În consecință, între primul raport privind vulnerabilitatea și confirmarea acesteia se poate scurge o perioadă limitată de timp. Astfel cum se indică în secțiunea *9.1 Obligații de raportare*, accentul ar trebui pus pe o acțiune promptă de investigare și de reacție.

236. În plus, obligația producătorilor de a respecta cerințele esențiale prevăzute în partea I din anexa I se aplică în momentul introducerii pe piață, în conformitate cu articolul 13 alineatul (1). În practică, este posibil ca noi vulnerabilități potențial exploatabile să fie descoperite în etapele finale ale ciclului de viață al dezvoltării produsului cu elemente digitale, inclusiv cu puțin timp înainte ca acesta să intre în lanțul de distribuție (și, prin urmare, să fie introdus pe piață).

237. Întrucât obligația de a introduce pe piață produse cu elemente digitale fără vulnerabilități exploatabile cunoscute este o obligație bazată pe riscuri, producătorului îi revine sarcina de a stabili dacă, pe baza evaluării riscurilor în materie de securitate cibernetică, produsul cu elemente digitale poate fi introdus pe piață în condiții de siguranță, în conformitate cu CRA. În mod alternativ, producătorul poate stabili că o nouă vulnerabilitate care este posibil să fi devenit cunoscută trebuie să fie remediată înainte ca produsul cu elemente digitale să poată fi introdus pe piață. Atunci când stabilesc acest lucru, producătorii ar trebui să țină seama de gravitatea, de posibilitatea de exploatare și de impactul potențial al vulnerabilității, precum și de riscurile care decurg pentru produsul cu elemente digitale în sine, odată ce este utilizat. Aceștia pot lua în considerare, de asemenea, riscurile de amânare a lansării produsului până la remedierea vulnerabilității, de exemplu deoarece noua versiune abordează și alte vulnerabilități exploatabile sau este necesară pentru funcționarea în continuare a sistemelor critice. În orice caz, odată ce un produs cu elemente digitale este introdus pe piață, producătorul rămâne supus obligației de a gestiona vulnerabilitățile în mod eficace și în conformitate cu cerințele de gestionare a vulnerabilităților prevăzute în anexa I partea II.

9.2.3. *Teste și reexaminări eficace și periodice*

238. Punctul 3 din partea II a anexei I impune producătorilor să aplice teste și reexaminări eficace și periodice ale produsului cu elemente digitale pe parcursul întregii perioade de asistență. Efectuarea de teste regulate nu necesită repetarea mecanică, la intervale fixe, a unei campanii de testare nemodificate. Aceasta înseamnă să se verifice periodic dacă noile date de intrare, cum ar fi amenințările nou identificate sau vulnerabilitățile nou descoperite, necesită actualizarea testelor existente și să se efectueze teste în consecință.

239. Frecvența, temeiul și conținutul reexaminării ar trebui să fie proporționale cu profilul de risc în materie de securitate cibernetică al produsului cu elemente digitale, cu evoluția sa în timp și cu starea ariei amenințărilor. În cazul în care reexaminarea identifică noi date de intrare relevante care afectează setul de teste, ar trebui proiectate și aplicate teste noi sau modificate pe produs, pentru a se asigura că nicio vulnerabilitate nu rămâne neabordată. Aceasta poate include reaplicarea testelor existente în cazul în care o modificare a produsului cu elemente digitale face ca astfel de tipuri de încercări să fie adecvate, cum ar fi testarea de regresie.

240. În cazul în care reexaminarea nu identifică astfel de date, nu este necesar să se conceapă teste suplimentare. Alte obligații de gestionare a vulnerabilităților, inclusiv cea în materie de abordare și remediere a vulnerabilităților în legătură cu riscurile prezentate, continuă să se aplice în paralel.

9.3. **Interacțiunea cu alte reglementări**

9.3.1. *Regulamentul (UE) 2019/2144 și Regulamentul (UE) nr. 168/2013*

241. Articolul 2 alineatul (2) litera (c) din CRA prevede că regulamentul nu se aplică produselor cu elemente digitale cărora li se aplică Regulamentul (UE) 2019/2144. Regulamentul (UE) 2019/2144 se aplică „vehiculelor din categoriile M, N și O, astfel cum sunt definite la articolul 4 din Regulamentul (UE) 2018/858, precum și sistemelor, componentelor și unităților tehnice separate concepute și construite pentru astfel de vehicule”.

242. În mod similar, produsele cu elemente digitale care intră în domeniul de aplicare al Regulamentului (UE) nr. 168/2013 au fost excluse din domeniul de aplicare al CRA prin Regulamentul delegat (UE) 2025/1535 al Comisiei. Regulamentul (UE) nr. 168/2013 se aplică vehiculelor din categoria L, precum și „sistemelor, componentelor și unităților tehnice separate, ca și pieselor și echipamentelor proiectate și fabricate pentru a funcționa pe aceste vehicule” [articolul 2 alineatul (1)].

243. Vehiculele cărora li se aplică regulamentele respective nu fac obiectul CRA. În plus, sunt necesare clarificări suplimentare în ceea ce privește domeniul de aplicare al derogării pentru sistemele, componentele, unitățile tehnice separate, piesele și echipamentele (în sensul prezentei secțiuni, „componentele”) proiectate și fabricate pentru a funcționa pe aceste vehicule care sunt considerate produse cu elemente digitale în sensul CRA.

244. Se consideră că astfel de componente nu fac obiectul CRA, cu condiția să fie proiectate și fabricate exclusiv pentru integrarea în vehicule care intră sub incidența Regulamentelor (UE) 2019/2144 și (UE) nr. 168/2013. Acest aspect este valabil indiferent dacă producătorul componentei respective o vinde direct producătorului vehiculului sau unui alt operator economic din lanțul de aprovizionare al autovehiculelor, atât timp cât componenta este în mod clar destinată și adecvată numai pentru integrarea finală în cadrul vehiculelor respective.

245. În schimb, un producător care vinde componente generice care sunt produse cu elemente digitale ce pot fi integrate în diferite tipuri de produse, și nu exclusiv în vehicule care intră sub incidența regulamentelor respective, face obiectul CRA.

246. Evaluarea introducerii pe piață a unei componente în sensul CRA trebuie să se bazeze pe condițiile obiective în care aceasta este pusă la dispoziție. În cazul în care un producător oferă o componentă care nu este adecvată exclusiv pentru integrarea finală în vehiculele respective prin canale de distribuție care sunt deschise clienților din afara lanțului de aprovizionare pentru autovehicule, cum ar fi punctele de vânzare cu amănuntul generale sau canalele de vânzare online care acceptă comenzi de la publicul larg, componenta respectivă intră în domeniul de aplicare al CRA, indiferent de orice declarații privind utilizarea preconizată a acesteia. În astfel de circumstanțe, componenta nu poate fi considerată ca fiind proiectată și fabricată exclusiv pentru integrarea în vehicule care intră sub incidența Regulamentelor (UE) 2019/2144 și (UE) nr. 168/2013, iar producătorul trebuie să respecte CRA. În schimb, utilizarea unor canale de distribuție restricționate între întreprinderi, limitate la lanțul de aprovizionare al autovehiculelor, poate indica faptul că aceasta este proiectată și fabricată exclusiv pentru o astfel de integrare.

9.3.2. *Valabilitatea certificatelor de examinare UE de tip [articolul 69 alineatul (1)]*

247. Articolul 69 alineatul (1) din CRA prevede că „certificatele de examinare UE de tip și deciziile de aprobare emise în ceea ce privește cerințele de securitate cibernetică pentru produsele cu elemente digitale care fac obiectul legislației de armonizare a Uniunii diferită de prezentul regulament, rămân valabile până la 11 iunie 2028, cu excepția cazului în care expiră înainte de data respectivă sau cu excepția cazului în care se prevede altfel în respectiva legislație de armonizare a Uniunii, caz în care rămân valabile, astfel cum se menționează în legislația respectivă”.

248. Menținerea valabilității unor astfel de certificate și decizii de aprobare ar trebui înțeleasă ca fiind limitată la riscurile în materie de securitate cibernetică și la cerințele corespunzătoare care sunt reglementate de respectivele acte legislative de armonizare ale Uniunii pe baza cărora au fost eliberate. În cazul acestor riscuri, producătorii nu sunt obligați să reevalueze sau să demonstreze din nou conformitatea exclusiv în sensul CRA în perioada de valabilitate menționată la articolul 69 alineatul (1) pentru produsele cu elemente digitale pe care intenționează să le introducă pe piață la 11 decembrie 2027 sau după această dată și până la 11 iunie 2028 ([31]). Această situație este valabilă pentru certificatele și deciziile de aprobare emise în cazul în care legislația de armonizare aplicabilă a Uniunii impune producătorului să efectueze procedura de evaluare a conformității prin intermediul unui organism notificat, precum și în cazul în care producătorul alege în mod voluntar să acționeze în acest sens.

249. În consecință, existența unui certificat valabil sau a unei decizii de aprobare valabile în temeiul altor acte legislative de armonizare ale Uniunii nu scutește producătorii de efectuarea unei evaluări cuprinzătoare a riscurilor în materie de securitate cibernetică în temeiul CRA (sau de alte obligații în temeiul acesteia). În schimb, aceasta le permite să se bazeze pe certificările existente ca dovadă a conformității în ceea ce privește procedura lor de evaluare a conformității, în măsura în care riscurile de securitate cibernetică corespunzătoare sunt deja acoperite. În cazul în care certificatul sau decizia de aprobare este valabil(ă) în temeiul altor acte legislative de armonizare ale Uniunii care se prelungesc după 11 iunie 2028, producătorul se poate baza totuși pe un astfel de certificat sau pe o astfel de decizie în scopurile CRA numai până la 11 iunie 2028.

250. În cazul în care evaluarea riscurilor în materie de securitate cibernetică efectuată în conformitate cu articolul 13 alineatul (2) identifică riscuri suplimentare care nu sunt acoperite de cerințele în materie de securitate cibernetică ce stau la baza certificatului existent sau a deciziei de aprobare existente, producătorii sunt în continuare responsabili de abordarea riscurilor respective în conformitate cu CRA. În astfel de cazuri, conformitatea impune ca lacunele identificate să fie evaluate și atenuate, indiferent de menținerea valabilității certificatului existent sau a deciziei de aprobare existente.

251. Acest aspect poate fi ilustrat prin luarea în considerare a cazului în care un produs cu elemente digitale face obiectul cerințelor în materie de securitate cibernetică prevăzute în Regulamentul delegat (UE) 2022/30 al Comisiei de completare a Directivei 2014/53/UE [Actul delegat referitor la Directiva privind echipamentele radio (RED)] și în care a fost emis un certificat de examinare UE de tip sau o decizie de aprobare pe baza cerințelor respective. În acest caz, certificatul sau decizia rămân valabile, în conformitate cu articolul 69 alineatul (1), pentru riscurile de securitate cibernetică vizate de certificatul respectiv și legate de cerințele esențiale de securitate cibernetică prevăzute în Directiva 2014/53/UE (Directiva privind echipamentele radio sau „RED”).

252. În astfel de cazuri, producătorii nu sunt obligați, în sensul CRA, să reevalueze sau să demonstreze din nou conformitatea în ceea ce privește riscurile deja abordate de certificatele respective, atât timp cât certificatul relevant sau decizia de aprobare relevantă rămân valabile și, în orice caz, nu mai târziu de 11 iunie 2028. Aceasta include, de exemplu, riscurile de securitate cibernetică legate de protecția rețelei, protecția datelor cu caracter personal și a vieții private sau prevenirea fraudei (în măsura în care riscurile respective sunt acoperite de certificatul în cauză) legate de cerințele de securitate cibernetică prevăzute în RED și reflectate în evaluarea conformității.

253. Cu toate acestea, în cazul în care evaluarea riscurilor în materie de securitate cibernetică efectuată în conformitate cu articolul 13 alineatul (2) din CRA identifică riscuri suplimentare în materie de securitate cibernetică care nu sunt acoperite de certificatele respective, producătorii sunt în continuare responsabili de abordarea riscurilor respective în conformitate cu CRA. Acestea pot include, de exemplu, riscuri legate de procesele de gestionare a vulnerabilităților, reducerea la minimum a datelor și reducerea suprafețelor de atac sau alte aspecte de securitate cibernetică specifice produsului care nu sunt abordate de certificatele respective sau, în orice caz, care nu intră sub incidența cerințelor esențiale de securitate cibernetică prevăzute în RED.

254. În consecință, existența unui certificat de examinare UE de tip valabil sau a unei decizii de aprobare valabile în temeiul RED pentru cerințele sale esențiale referitoare la securitatea cibernetică nu demonstrează, în sine, conformitatea deplină cu CRA. În schimb, aceasta permite producătorilor să se bazeze pe certificatul sau decizia în cauză ca dovadă a conformității pentru riscurile corespunzătoare, asigurându-se, în același timp, că orice riscuri rămase sau nou identificate sunt evaluate și atenuate în conformitate cu CRA.

([31]) Produsele cu elemente digitale introduse pe piață înainte de 11 decembrie 2027 fac obiectul legislației Uniunii aplicabile la momentul introducerii lor pe piață și, dacă au fost conforme, pot fi vândute și puse în funcțiune, cu excepția cazului în care, la 11 decembrie 2027 sau după această dată, fac obiectul unor modificări substanțiale. Pentru conceptele de „introducere pe piață” și „punere la dispoziție pe piață”, a se vedea, de asemenea, secțiunea *2.1 Introducerea pe piață* din prezentul document, precum și capitolul 2 din Ghidul albastru.

255. În mod similar, în cazul în care un produs cu elemente digitale face obiectul cerințelor esențiale privind sănătatea și securitatea legate de securitatea cibernetică prevăzute în Regulamentul (UE) 2023/1230 (Regulamentul privind mașinile), pe deplin aplicabil de la 20 ianuarie 2027, și în cazul în care a fost eliberat un certificat de examinare UE de tip sau a fost emisă o decizie de aprobare pe baza cerințelor respective, certificatul sau decizia de aprobare în cauză rămân valabile, în conformitate cu articolul 69 alineatul (1) din CRA, în ceea ce privește riscurile în materie de securitate cibernetică ce fac obiectul Regulamentului privind mașinile.

256. În special, este vorba despre aspecte de securitate cibernetică legate de protecția împotriva coruperii și de siguranța și fiabilitatea sistemelor de control, astfel cum se prevede în secțiunile 1.1.9 și 1.2.1 din anexa III la Regulamentul privind mașinile. În cazul acestor riscuri, producătorii nu sunt obligați, în sensul CRA, să reevalueze sau să demonstreze din nou conformitatea atât timp cât certificatul relevant sau decizia de aprobare relevantă rămân valabile și, în orice caz, nu mai târziu de 11 iunie 2028. Acest aspect este valabil în măsura în care riscurile respective sunt abordate în cadrul evaluării conformității în temeiul Regulamentului privind mașinile.

257. La fel ca în cazul cerințelor esențiale în materie de securitate cibernetică din RED menționate mai sus, în cazul în care evaluarea riscurilor în materie de securitate cibernetică efectuată în temeiul articolului 13 alineatul (2) din CRA identifică riscuri suplimentare în materie de securitate cibernetică care nu sunt acoperite de certificatul relevant eliberat în temeiul Regulamentului privind mașinile și care sunt legate de cerințele de securitate cibernetică prevăzute în regulamentul respectiv, producătorii rămân responsabili de abordarea riscurilor respective în conformitate cu CRA.