Consiliul
Uniunii Europene

Bruxelles, 16 septembrie 2022
(OR. en)

12429/22
ADD 1

Dosar interinstituțional:
2022/0272 (COD)

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

NOTĂ DE ÎNSOȚIRE

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

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

Anexă: COM(2022) 454 final - Annexes

COMISIA
EUROPEANĂ

Bruxelles, 15.9.2022
COM(2022) 454 final

ANNEXES 1 to 6

ANEXE

la

PROPUNEREA DE REGULAMENT AL PARLAMENTULUI EUROPEAN ȘI AL CONSILIULUI

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

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

ANEXA I

CERINȚE ESENȚIALE DE SECURITATE CIBERNETICĂ

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

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

(2) Produsele cu elemente digitale sunt livrate fără vulnerabilități exploatabile cunoscute;

(3) Pe baza evaluării riscurilor menționate la articolul 10 alineatul (2) și după caz, produsele cu elemente digitale trebuie:

(a) să fie livrate cu o configurație securizată implicită, inclusiv cu posibilitatea de a reseta produsul la starea sa inițială;

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

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

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

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

(f) să protejeze disponibilitatea funcțiilor esențiale, inclusiv reziliența împotriva atacurilor vizând blocarea accesului la servicii și atenuarea acestora;

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

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

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

(j) să furnizeze informații legate de securitate prin înregistrarea și/sau monitorizarea activității interne relevante, inclusiv accesul la date, servicii sau funcții sau modificarea acestora;

(k) să asigure faptul că vulnerabilitățile pot fi abordate prin actualizări de securitate, inclusiv, după caz, prin actualizări automate și prin notificarea utilizatorilor cu privire la actualizările disponibile.

2. CERINȚE PRIVIND GESTIONAREA VULNERABILITĂȚILOR

Producătorii de produse cu elemente digitale trebuie:

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

(2) în ceea ce privește riscurile pe care le prezintă produsele cu elemente digitale, să abordeze și să remedieze fără întârziere vulnerabilitățile, inclusiv prin furnizarea de actualizări de securitate;

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

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

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

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

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

(8) să se asigure că, în cazul în care sunt disponibile corecții de securitate sau actualizări pentru abordarea problemelor de securitate identificate, acestea sunt difuzate fără întârziere și gratuit, însoțite de mesaje de consiliere care să ofere utilizatorilor informațiile relevante, inclusiv cu privire la eventualele acțiuni care trebuie întreprinse.

ANEXA II

INFORMAȚII ȘI INSTRUCȚIUNI PENTRU UTILIZATOR

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

1. numele, denumirea comercială înregistrată sau marca înregistrată a producătorului, precum și adresa poștală și adresa de e-mail la care poate fi contactat producătorul, pe produs sau, dacă acest lucru nu este posibil, pe ambalaj sau într-un document care însoțește produsul;
2. punctul de contact unde pot fi raportate și primite informații cu privire la vulnerabilitățile în materie de securitate cibernetică ale produsului;
3. identificarea corectă a tipului, lotului, versiunii sau numărului de serie sau a altui element care permite identificarea produsului, precum și instrucțiunile și informațiile de utilizare corespunzătoare;
4. utilizarea preconizată, inclusiv mediul de securitate furnizat de producător, precum și funcționalitățile esențiale ale produsului și informații cu privire la proprietățile de securitate;
5. orice circumstanță cunoscută sau previzibilă legată de utilizarea produsului cu elemente digitale în conformitate cu scopul preconizat sau în condiții de utilizare necorespunzătoare previzibile în mod rezonabil care poate conduce la riscuri semnificative de securitate cibernetică;
6. dacă și, după caz, unde poate fi accesată lista materialelor software;
7. dacă este cazul, adresa de internet la care poate fi accesată declarația de conformitate UE;
8. tipul de asistență tehnică de securitate oferită de producător și data până la care aceasta va fi furnizată, cel puțin data până la care utilizatorii se pot aștepta să primească actualizări de securitate;
9. instrucțiuni detaliate sau o adresă de internet la care să se găsească astfel de instrucțiuni detaliate și informații privind:
   (a) măsurile necesare în timpul punerii în funcțiune inițiale și pe toată durata de viață a produsului pentru a se asigura o utilizare securizată a acestuia;
   (b) modul în care modificările aduse produsului pot afecta securitatea datelor;
   (c) modul în care pot fi instalate actualizările relevante pentru securitate;
   (d) dezafectarea securizată a produsului, inclusiv informații privind modul în care datele utilizatorilor pot fi eliminate în mod securizat.

ANEXA III

PRODUSELE CRITICE CU ELEMENTE DIGITALE

Clasa I

1. Software pentru sisteme de gestionare a identității și software de gestionare a accesului privilegiat;
2. Browsere autonome și încorporate;
3. Manageri de parole;
4. Software care caută, elimină sau plasează în carantină programe informatice malware;
5. Produse cu elemente digitale cu funcție de rețea privată virtuală (VPN);
6. Sisteme de administrare a rețelei;
7. Instrumente de gestionare a configurației rețelei;
8. Sisteme de monitorizare a traficului în rețea;
9. Gestionarea resurselor rețelei;
10. Sisteme de gestionare a informațiilor de securitate și a evenimentelor de securitate (SIEM);
11. Gestionarea actualizărilor/corecțiilor, inclusiv managerii de boot;
12. Sisteme de gestionare a configurațiilor aplicațiilor;
13. Software de accesare/partajare de la distanță;
14. Software de gestionare a dispozitivelor mobile;
15. Interfețe fizice de rețea;
16. Sisteme de operare neincluse în clasa II;
17. Firewall-uri, sisteme de detectare și/sau prevenire a intruziunilor care nu sunt incluse în clasa II;
18. Routere, modemuri destinate conectării la internet și comutatoare care nu sunt incluse în clasa II;
19. Microprocesoare neincluse în clasa II;
20. Microcontrolere;
21. Circuite integrate specifice aplicațiilor (ASIC) și rețele de porți programabile de utilizator (FPGA) destinate utilizării de către entități esențiale de tipul celor menționate în [anexa I la Directiva XXX/XXXX (NIS2)];
22. Sisteme de control pentru automatizări industriale (IACS) neincluse în clasa II, cum ar fi controlerele logice programabile (PLC), sistemele de control distribuit (SCD), controlerele numerice computerizate pentru mașini-unelte (CNC) și sistemele de control de supraveghere și de achiziție de date (SCADA);
23. Internetul industrial al obiectelor neinclus în clasa II.

Clasa II

1. Sisteme de operare pentru servere, calculatoare de tip desktop și dispozitive mobile;
2. Hipervizoare și sisteme de runtime a containerelor care sprijină executarea virtualizată a sistemelor de operare și a mediilor similare;
3. Infrastructuri de chei publice și emitenți de certificate digitale;
4. Firewall-uri, sisteme de detectare și/sau prevenire a intruziunilor destinate utilizării industriale;
5. Microprocesoare de uz general;
6. Microprocesoare destinate integrării în controlere logice programabile și în elemente securizate;
7. Routere, modemuri destinate conectării la internet și comutatoare, de uz industrial;
8. Elemente securizate;
9. Module de securitate hardware (HSM);
10. Criptoprocesoare securizate;
11. Carduri inteligente, cititoare și tokenuri pentru carduri inteligente;
12. Sisteme de control pentru automatizări industriale (IACS) destinate utilizării de către entități esențiale de tipul celor menționate în [anexa I la Directiva XXX/XXXX (NIS2)], cum ar fi controlerele logice programabile (PLC), sistemele de control distribuit (SCD), controlerele numerice computerizate pentru mașini-unelte (CNC) și sistemele de control de supraveghere și de achiziție de date (SCADA);
13. Dispozitive pentru internetul industrial al obiectelor destinate utilizării de către entități esențiale de tipul celor menționate în [anexa I la Directiva XXX/XXXX (NIS2)];
14. Componente de detecție și de acționare a roboților și unități de control al roboților;
15. Contoare inteligente.

ANEXA IV

DECLARAȚIA DE CONFORMITATE UE

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

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

Semnat pentru și în numele: ……

(locul și data emiterii):

(numele, funcția) (semnătura):

ANEXA V

CONȚINUTUL DOCUMENTAȚIEI TEHNICE

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

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

6. o copie a declarației de conformitate UE;

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

ANEXA VI

PROCEDURI DE EVALUARE A CONFORMITĂȚII

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

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

2. Producătorul întocmește documentația tehnică descrisă în anexa V.

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

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

4. Marcajul de conformitate și declarația de conformitate

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

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

5. Reprezentanți autorizați

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

Examinarea UE de tip (pe baza modulului B)

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

– Examinarea UE de tip se efectuează prin evaluarea caracterului adecvat al proiectării și dezvoltării tehnice a produsului prin examinarea documentației tehnice și a

documentelor justificative menționate la punctul 3, la care se adaugă examinarea unor exemplare ale uneia sau mai multor părți critice ale produsului (combinație de tip de producție și tip de proiectare).

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

Cererea trebuie să cuprindă:

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

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

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

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

3. Organismul de certificare notificat:

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

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

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

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

anexa I, dacă soluțiile adoptate de către producător îndeplinesc cerințele esențiale corespunzătoare;

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

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

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

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

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

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

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

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

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

Comisia, statele membre și celelalte organisme notificate pot obține, la cerere, o copie a certificatelor de examinare UE de tip și/sau a suplimentelor la acestea. Pe baza unei cereri, Comisia și statele membre pot obține o copie a documentației tehnice și a rezultatelor examinărilor efectuate de organismul notificat. Organismul notificat păstrează un exemplar al certificatului de examinare UE de tip, al anexelor și suplimentelor acestuia, precum și dosarul tehnic incluzând documentația depusă de producător, până la expirarea valabilității certificatului.

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

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

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

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

2. Producția

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

3. Marcajul de conformitate și declarația de conformitate

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

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

4. Reprezentantul autorizat

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

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

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

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

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

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

3. Sistemul de calitate

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

Cererea trebuie să cuprindă:

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

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

– documentația referitoare la sistemul de calitate; și

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

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

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

Documentația trebuie să cuprindă în special o descriere adecvată:

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

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

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

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

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

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

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

– a înregistrărilor referitoare la calitate, cum ar fi rapoarte de inspecție și informații referitoare la teste, precum și date privind etalonarea, rapoarte referitoare la calificarea personalului implicat etc.;

– a mijloacelor de monitorizare privind atingerea calității cerute a proiectului și a produsului și funcționarea eficace a sistemului de calitate.

3.3. Organismul notificat evaluează sistemul de calitate pentru a stabili dacă acesta îndeplinește cerințele menționate la punctul 3.2.

Acesta prezumă conformitatea cu cerințele respective pentru elementele sistemului de calitate care sunt conforme cu specificațiile corespunzătoare ale standardului național care pune în aplicare standardul armonizat și/sau specificațiile tehnice relevante.

Pe lângă experiența în sisteme de management al calității, echipa de audit trebuie să aibă cel puțin un membru cu experiență de evaluator în domeniul produsului relevant și al tehnologiei produsului în cauză și să cunoască cerințele aplicabile prevăzute în prezentul regulament. Auditul trebuie să includă o vizită de evaluare la sediul producătorului, în cazul în care există un astfel de sediu. Echipa de audit analizează documentația tehnică menționată la punctul 3.1 a doua liniuță în vederea verificării capacității producătorului de a identifica cerințele aplicabile prevăzute în prezentul regulament și a efectuării examinărilor necesare cu scopul de a asigura conformitatea produsului cu aceste cerințe.

Decizia este notificată producătorului sau reprezentantului autorizat al acestuia.

Notificarea trebuie să cuprindă concluziile procesului de audit și decizia motivată referitoare la evaluare.

3.4. Producătorul se angajează să îndeplinească obligațiile care decurg din sistemul de calitate astfel cum a fost aprobat și să îl mențină astfel încât acesta să rămână adecvat și eficace.

3.5. Producătorul informează în permanență organismul notificat care a aprobat sistemul de calitate în legătură cu orice intenție de modificare a sistemului de calitate.

Organismul notificat evaluează modificările propuse și decide dacă sistemul de calitate modificat va continua să îndeplinească cerințele menționate la punctul 3.2 sau dacă este necesară o reevaluare.

Organismul notificat notifică decizia sa producătorului. Notificarea trebuie să cuprindă concluziile examinării și decizia motivată referitoare la evaluare.

4. Supravegherea care intră în sfera de responsabilitate a organismului notificat

4.1. Scopul supravegherii este acela de a asigura îndeplinirea corespunzătoare de către producător a obligațiilor ce decurg din sistemul de calitate aprobat.

4.2. Producătorul autorizează accesul organismului notificat, în scopul evaluării, la spațiile de proiectare, dezvoltare, producție, inspecție, testare și depozitare și îi furnizează orice informație necesară, în special:

– documentația privind sistemul de calitate;

– înregistrările referitoare la calitate, astfel cum sunt prevăzute în partea sistemului de calitate destinată proiectării, de exemplu rezultatele analizelor, calculelor, testelor etc.;

– înregistrările referitoare la calitate, astfel cum sunt prevăzute în partea sistemului de calitate destinată fabricării, de exemplu rapoarte de inspecție și date privind testele, date privind etalonarea, rapoarte privind calificarea personalului în cauză etc.

4.3. Organismul notificat efectuează misiuni de audit periodice pentru a se asigura că producătorul menține și aplică sistemul de calitate și prezintă producătorului un raport de audit.

5. Marcajul de conformitate și declarația de conformitate

5.1. Producătorul aplică marcajul CE și, sub responsabilitatea organismului notificat menționat la punctul 3.1, numărul de identificare al acestuia pe fiecare produs în parte care îndeplinește cerințele prevăzute în secțiunea 1 din anexa I la prezentul regulament.

5.2. Producătorul întocmește o declarație de conformitate scrisă pentru fiecare model de produs și o păstrează la dispoziția autorităților naționale timp de zece ani de la introducerea pe piață a produsului. Declarația de conformitate trebuie să identifice modelul produsului pentru care a fost întocmită.

O copie a declarației de conformitate trebuie să fie pusă la dispoziția autorităților relevante, la cerere.

6. Pe o perioadă de cel puțin zece ani de la introducerea pe piață a produsului, producătorul menține la dispoziția autorităților naționale:

– documentația tehnică menționată la punctul 3.1;

– documentația privind sistemul de calitate prevăzută la punctul 3.1;

– modificarea menționată la punctul 3.5, astfel cum a fost aprobată;

– deciziile și rapoartele organismului notificat menționate la punctele 3.5, 4.3 și 4.4.

7. Fiecare organism notificat își informează autoritățile de notificare în legătură cu aprobările sistemului de calitate care au fost emise sau retrase și, în mod periodic sau la cerere, pune la dispoziția autorităților sale de notificare lista aprobărilor sistemelor de calitate care au fost refuzate, suspendate sau restricționate în alt mod.

Fiecare organism notificat informează celelalte organisme notificate în legătură cu aprobările sistemelor de calitate pe care le-a refuzat, suspendat sau retras și, la cerere, în legătură cu aprobările sistemelor de calitate pe care le-a emis.

8. Reprezentantul autorizat

Obligațiile producătorului menționate la punctele 3.1, 3.5, 5 și 6 pot fi îndeplinite de către reprezentantul său autorizat, în numele său și pe răspunderea sa, cu condiția ca acestea să fie menționate în mandat.