2024/3144

19.12.2024

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2024/3144 AL COMISIEI

din 18 decembrie 2024

de modificare a Regulamentului de punere în aplicare (UE) 2024/482 în ceea ce privește standardele internaționale aplicabile și de rectificare a regulamentului de punere în aplicare respectiv

(Text cu relevanță pentru SEE)

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului din 17 aprilie 2019 privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor și de abrogare a Regulamentului (UE) nr. 526/2013 (Regulamentul privind securitatea cibernetică) ([1]), în special articolul 49 alineatul (7),

întrucât:

(1) Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei ([2]) precizează rolurile, normele și obligațiile, precum și structura sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC) în conformitate cu cadrul european de certificare a securității cibernetice prevăzut în Regulamentul (UE) 2019/881.

(2) Regulamentul de punere în aplicare (UE) 2024/482 se bazează pe criteriile comune și metodologia comună de evaluare menținute de Organizația Internațională de Standardizare (ISO) și de Comisia Electrotehnică Internațională (IEC) care sunt standarde internaționale consacrate. Regulamentul de punere în aplicare (UE) 2024/482 face trimitere la standardele ISO/IEC, dar nu precizează versiunea aplicabilă a standardelor respective. Prin urmare, ar trebui să se precizeze ce versiune a standardelor se aplică certificatelor eliberate în cadrul EUCC.

(3) Organizațiile guvernamentale care au contribuit la elaborarea criteriilor comune și a metodologiei comune de evaluare prin Acordul privind recunoașterea certificatelor de criterii comune în domeniul securității informatice (CCRA) sunt titulari comuni ai drepturilor de autor asupra lor, împreună cu ISO/IEC. Aceste organizații guvernamentale își păstrează dreptul de a le utiliza. Având în vedere importanța documentelor care provin din CCRA, acestea ar trebui să constituie, de asemenea, o bază pentru certificarea în cadrul EUCC.

(4) Criteriile comune și standardele privind metodologia comună de evaluare fac obiectul unor interpretări efectuate prin CCRA care facilitează punerea lor în aplicare și care pot fi luate în considerare de unitățile de evaluare a securității tehnologiei informației (ITSEF) și de organismele de certificare.

(5) Standardele internaționale referitoare la criteriile comune ar putea face obiectul unor actualizări. Pentru a asigura o tranziție ordonată și în timp util, este oportun să se definească dispoziții tranzitorii pentru a acorda furnizorilor, ITSEF și organismelor de certificare, precum și altor entități relevante suficient timp pentru ajustările necesare. Aceste dispoziții tranzitorii ar trebui să se alinieze într-o măsură adecvată la practicile globale, precum cele stabilite de CCRA.

([1]) JO L 151, 7.6.2019, p. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj.

([2]) Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei din 31 ianuarie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) 2019/881 al Parlamentului European și al Consiliului în ceea ce privește adoptarea sistemului european de certificare a securității cibernetice bazat pe criterii comune (EUCC) (JO L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

(6) Regulamentul de punere în aplicare (UE) 2024/482 nu precizează momentul în care o certificare a produselor TIC s-ar putea baza pe versiunile anterioare ale standardelor privind criteriile comune și metodologia comună de evaluare. Domeniile tehnice și profilurile de protecție enumerate în anexele I, II și III la regulamentul de punere în aplicare respectiv se bazează pe versiunile anterioare ale standardelor ISO/IEC 15408 și 18045. Prin urmare, Regulamentul de punere în aplicare (UE) 2024/482 ar trebui să precizeze circumstanțele în care se aplică în continuare versiunea anterioară a criteriilor comune și a metodologiei comune de evaluare și modul în care va funcționa tranziția către cea mai recentă versiune a standardelor internaționale.

(7) În cursul perioadei de tranziție, actualizarea domeniilor tehnice și a profilurilor de protecție relevante ar trebui să constituie o prioritate pentru părțile interesate relevante. Regulamentul de punere în aplicare (UE) 2024/482 ar trebui să prevadă că obiectivele de securitate bazate pe o versiune anterioară a standardelor vor fi acceptate până la 31 decembrie 2027, în concordanță cu politica de tranziție adoptată de CCRA. Cu toate acestea, trebuie remarcat faptul că politica de tranziție a CCRA acoperă evaluările inițiale ale produselor și ale profilurilor de protecție care încep cel târziu la 30 iunie 2024, dată la care EUCC nu era încă aplicabil. În plus, în conformitate cu politica de tranziție a CCRA, Regulamentul de punere în aplicare (UE) 2024/482 ar trebui să prevadă că obiectivele de securitate conforme cu regulamentul de punere în aplicare respectiv și declarate conforme cu profilurile de protecție bazate pe o versiune anterioară a standardelor vor fi acceptate până la 31 decembrie 2027. În plus, în cazul în care se eliberează un nou certificat în temeiul Regulamentului de punere în aplicare (UE) 2024/482 în contextul unui proces de revizuire a unui certificat național care începe în termen de doi ani de la certificatul inițial, ar trebui să fie posibilă utilizarea unei versiuni anterioare a standardelor. Acest lucru nu ar fi relevant pentru un proces de revizuire care nu necesită eliberarea unui nou certificat în temeiul Regulamentului de punere în aplicare (UE) 2024/482 și în cazul în care certificatul rămâne valabil.

(8) În vederea asigurării unei tranziții ordonate către cea mai recentă versiune a standardelor, Regulamentul de punere în aplicare (UE) 2024/482 ar trebui să prevadă dispoziții tranzitorii specifice și să permită în continuare eliberarea de certificate în temeiul regulamentului de punere în aplicare respectiv declarate conforme cu profilurile de protecție bazate pe versiunile anterioare ale standardelor publicate de CCRA, în cazul în care utilizarea unor astfel de profiluri de protecție este necesară în temeiul legislației Uniunii. Acesta este cazul Regulamentului de punere în aplicare (UE) 2016/799 al Comisiei ([3]), al Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului ([4]) și al Deciziei de punere în aplicare (UE) 2016/650 a Comisiei ([5]).

(9) Anexa I la Regulamentul de punere în aplicare (UE) 2024/482 enumeră documentele aplicabile ce reflectă stadiul actual al tehnologiei pentru evaluarea produselor TIC și a profilurilor de protecție. Cu toate acestea, nu precizează versiunea documentelor. Prin urmare, ar trebui să se precizeze ce versiune a documentelor se aplică certificatelor eliberate în cadrul EUCC. Versiunile respective se bazează pe documente aprobate de Grupul european pentru certificarea securității cibernetice (ECCG), fiind supuse în același timp unei revizuiri suplimentare pentru a fi incluse în EUCC. În plus, anexa I ar trebui modificată pentru a include documente actualizate și noi care să reflecte stadiul actual al tehnologiei în urma aprobării acestora de către ECCG, asigurând astfel o acreditare uniformă a organismelor de evaluare a conformității în cadrul EUCC. Cerințele de acreditare legate de acreditarea ITSEF ar trebui actualizate pentru a clarifica aplicarea criteriilor de independență și imparțialitate și ar trebui elaborat un nou document care să reflecte stadiul actual al tehnologiei pentru acreditarea organismelor de certificare.

(10) Documentele ce reflectă stadiul actual al tehnologiei ar putea fi adăugate la EUCC sau ar putea face obiectul unor actualizări în contextul activităților sale de întreținere. Pentru documentele noi sau actualizate ce reflectă stadiul actual al tehnologiei, ar putea fi necesar să se stabilească dispoziții tranzitorii adecvate pentru a permite furnizorilor, ITSEF, organismelor de certificare și altor părți interesate să facă ajustările necesare. Pentru actualizarea documentului ce reflectă stadiul actual al tehnologiei referitor la acreditarea ITSEF, documentul actualizat ar trebui să se aplice acreditărilor emise înainte de 8 iulie 2025 numai atunci când sunt revizuite, de exemplu în contextul unei proceduri de evaluare sau de reevaluare. În plus, documentul actualizat ar trebui să se aplice tuturor acreditărilor pentru ITSEF emise după 8 iulie 2025.

([3]) Regulamentul de punere în aplicare (UE) 2016/799 al Comisiei din 18 martie 2016 de punere în aplicare a Regulamentului (UE) nr. 165/2014 al Parlamentului European și al Consiliului de stabilire a cerințelor pentru construirea, testarea, instalarea, operarea și repararea tahografelor și a componentelor acestora (JO L 139, 26.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

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

([5]) Decizia de punere în aplicare (UE) 2016/650 a Comisiei din 25 aprilie 2016 de stabilire a standardelor pentru evaluarea securității dispozitivelor de creare a semnăturilor și a sigiliilor calificate în temeiul articolului 30 alineatul (3) și al articolului 39 alineatul (2) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă (JO L 109, 26.4.2016, p. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).

(11) Rectificările suplimentare aduse articolelor 5, 8, 16, 29 și 44 și anexei IV la Regulamentul de punere în aplicare (UE) 2024/482 contribuie la asigurarea unei formulări uniforme și a unei interpretări juridice clare.

(12) Dispozițiile privind notificările organismelor de evaluare a conformității ar trebui stabilite orizontal pentru toate sistemele din cadrul european de certificare a securității cibernetice. Regulamentul de punere de aplicare (UE) 2024/3143 al Comisiei ([6]) cuprinde astfel de dispoziții de notificare. Prin urmare, articolele 23 și 24 din Regulamentul de punere de aplicare (UE) 2024/482 ar trebui eliminate de la data la care devine aplicabil Regulamentul de punere de aplicare (UE) 2024/3143.

(13) Prin urmare, Regulamentul de punere în aplicare (UE) 2024/482 ar trebui modificat și rectificat în consecință.

(14) Măsurile prevăzute în prezentul regulament sunt conforme cu avizul comitetului instituit în temeiul articolului 66 din Regulamentul (UE) 2019/881,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Regulamentul de punere în aplicare (UE) 2024/482 se modifică după cum urmează:

1. La articolul 2, punctele 1 și 2 se înlocuiesc cu următorul text:

„1. «criterii comune» înseamnă criteriile comune de evaluare a securității informatice, astfel cum sunt stabilite în standardele ISO/IEC 15408-1:2022, ISO/IEC 15408-2:2022, ISO/IEC 15408-3:2022, ISO/IEC 15408-4:2022 sau ISO/IEC 15408-5:2022 ori în criteriile comune de evaluare a securității informatice, versiunea CC:2022, părțile 1-5, publicate de participanții la Acordul privind recunoașterea certificatelor de criterii comune în domeniul securității informatice;

2. «metodologie comună de evaluare» înseamnă metodologia comună de evaluare a securității informatice, astfel cum este stabilită în standardul ISO/IEC 18045:2022, sau metodologia comună de evaluare a securității informatice, versiunea CEM:2022, publicată de participanții la Acordul privind recunoașterea certificatelor de criterii comune în domeniul securității informatice;".

2. Articolul 3 se înlocuiește cu următorul text:

„*Articolul 3*

Standarde de evaluare

(1) Următoarele standarde se aplică evaluărilor efectuate în cadrul sistemului EUCC:

(a) criteriile comune;

(b) metodologia comună de evaluare.

(2) Până la 31 decembrie 2027, se poate elibera un certificat în cadrul sistemului EUCC, aplicând oricare dintre următoarele standarde:

(a) ISO/IEC 15408-1:2009, ISO/IEC 15408-2:2008 sau ISO/IEC 15408-3:2008;

(b) Criteriile comune de evaluare a securității informatice, versiunea 3.1, revizia 5, publicate de participanții la Acordul privind recunoașterea certificatelor de criterii comune în domeniul securității informatice;

([6]) Regulamentul de punere în aplicare (UE) 2024/3143 al Comisiei din 18 decembrie 2024 de stabilire a circumstanțelor, a formatelor și a procedurilor pentru notificările efectuate în temeiul articolului 61 alineatul (5) din Regulamentul (UE) 2019/881 al Parlamentului European și al Consiliului privind ENISA (Agenția Uniunii Europene pentru Securitate Cibernetică) și privind certificarea securității cibernetice pentru tehnologia informației și comunicațiilor (JO L, 2024/3143, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3143/oj).

(c) ISO/IEC 18045:2008;

(d) Metodologia comună de evaluare a securității informatice, revizuirea 5, versiunea 3.1, publicată de participanții la Acordul privind recunoașterea certificatelor de criterii comune în domeniul securității informatice.

(3) Până la 31 decembrie 2027, se poate elibera un certificat care aplică standardele menționate la alineatul (1) în cadrul sistemului EUCC și care a fost declarat conform cu un profil de protecție care a aplicat standardele enumerate la alineatul (2).

(4) De asemenea, se poate elibera un certificat care aplică standardele menționate la alineatul (1) în cadrul sistemului EUCC și care a fost declarat conform cu un profil de protecție ce a aplicat oricare dintre următoarele standarde, cu condiția ca utilizarea unui astfel de profil de protecție să fie necesară în temeiul Regulamentului de punere în aplicare (UE) 2016/799 al Comisiei (*), al Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului (**) sau al Deciziei de punere în aplicare (UE) 2016/650 a Comisiei (***):

(a) Criteriile comune de evaluare a securității informatice, versiunea 3.1, revizuirile 1-4, publicate de participanții la Acordul privind recunoașterea certificatelor de criterii comune în domeniul securității informatice;

(b) Metodologia comună de evaluare a securității informatice, versiunea 3.1, revizuirile 1-4, publicată de participanții la Acordul privind recunoașterea certificatelor de criterii comune în domeniul securității informatice.

_____

(*) Regulamentul de punere în aplicare (UE) 2016/799 al Comisiei din 18 martie 2016 de punere în aplicare a Regulamentului (UE) nr. 165/2014 al Parlamentului European și al Consiliului de stabilire a cerințelor pentru construirea, testarea, instalarea, operarea și repararea tahografelor și a componentelor acestora (JO L 139, 26.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg_impl/2016/799/oj).

(**) Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului din 23 iulie 2014 privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă și de abrogare a Directivei 1999/93/CE (JO L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj).

(***) Decizia de punere în aplicare (UE) 2016/650 a Comisiei din 25 aprilie 2016 de stabilire a standardelor pentru evaluarea securității dispozitivelor de creare a semnăturilor și a sigiliilor calificate în temeiul articolului 30 alineatul (3) și al articolului 39 alineatul (2) din Regulamentul (UE) nr. 910/2014 al Parlamentului European și al Consiliului privind identificarea electronică și serviciile de încredere pentru tranzacțiile electronice pe piața internă (JO L 109, 26.4.2016, p. 40, ELI: http://data.europa.eu/eli/dec_impl/2016/650/oj).”

3. În capitolul IV se introduce următorul articol 20a:

„*Articolul 20a*

Specificarea cerințelor de acreditare a organismelor de evaluare a conformității

Acreditarea organismelor de evaluare a conformității ține seama de specificarea cerințelor de acreditare a organismelor de certificare și a unităților ITSEF, astfel cum se prevede în documentele care reflectă stadiul actual al tehnologiei și care sunt aplicabile și enumerate la punctul 2 din anexa I.”

4. Articolele 23 și 24 se elimină.

5. La articolul 48, se adaugă următorul alineat (4):

„(4) Cu excepția cazului în care se prevede altfel în anexa I sau II, documentele ce reflectă stadiul actual al tehnologiei se aplică de la data aplicării actului de modificare prin care au fost încorporate în anexa I sau II.”

6. La articolul 49, se adaugă următorul alineat (4):

„(4) Atunci când se efectuează revizuirea menționată la alineatul (3) în termen de doi ani de la eliberarea certificatului inițial și în cazul în care o astfel de revizuire conduce la eliberarea unui nou certificat în conformitate cu prezentul regulament, se pot aplica standardele enumerate la articolul 3 alineatul (2). Prin data eliberării certificatului inițial se înțelege data eliberării ultimului certificat pentru un produs TIC sau un profil de protecție pe care se bazează certificarea actuală.”

7. Anexa I se înlocuiește cu textul din anexa I la prezentul regulament.

8. Anexa IV se modifică în conformitate cu anexa II la prezentul regulament.

Articolul 2

Regulamentul de punere în aplicare (UE) 2024/482 se rectifică după cum urmează:

1. La articolul 5 alineatul (1), litera (b) se înlocuiește cu următorul text:

„(b) declarat conform cu un profil de protecție certificat ca parte a procesului TIC, în cazul în care produsul TIC se încadrează în categoria de produse TIC aflată sub incidența respectivului profil de protecție."

2. Articolul 8 se rectifică după cum urmează:

(a) titlul se înlocuiește cu următorul text:

„Informații necesare pentru certificare și evaluare";

(b) alineatul (1) se înlocuiește cu următorul text:

„(1) Un solicitant al unui certificat EUCC transmite sau pune în alt mod la dispoziția organismului de certificare și a unității ITSEF toate informațiile necesare pentru activitățile de certificare și evaluare."

3. Articolul 16 se înlocuiește cu următorul text:

„*Articolul 16*

Informații necesare pentru certificarea și evaluarea profilurilor de protecție

Un solicitant al unui certificat pentru un profil de protecție transmite sau pune în alt mod la dispoziția organismului de certificare și a ITSEF toate informațiile necesare pentru activitățile de certificare și evaluare într-o formă completă și corectă. Articolul 8 alineatele (2), (3), (4) și (7) se aplică *mutatis mutandis*."

4. La articolul 17, alineatul (1) se elimină.

5. La articolul 29, alineatul (2) se înlocuiește cu următorul text:

„(2) În cazul în care titularul certificatului EUCC nu propune măsuri de remediere adecvate în perioada menționată la alineatul (1), certificatul se suspendă în conformitate cu articolul 30 sau se retrage în conformitate cu articolul 14 sau 20."

Articolul 3

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

Articolul 1 alineatul (4) se aplică de la 8 ianuarie 2025.

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

Adoptat la Bruxelles, 18 decembrie 2024.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

ANEXA I

„„ANEXA I

Documente ce reflectă stadiul actual al tehnologiei și sprijină domeniile tehnice și alte documente ce reflectă stadiul actual al tehnologiei

1. Documente ce reflectă stadiul actual al tehnologiei și sprijină domeniile tehnice la nivelul 4 sau 5 al AVA_VAN:

   (a) următoarele documente referitoare la evaluarea armonizată a domeniului tehnic «carduri inteligente și dispozitive similare»:

      1. «Cerințe minime ale ITSEF privind evaluările de securitate ale cardurilor inteligente și dispozitivelor similare», versiunea 1.1;

      2. «Cerințe minime de securitate a site-ului», versiunea 1.1;

      3. «Aplicarea criteriilor comune în cazul circuitelor integrate», versiunea 1.1;

      4. «Cerințe privind arhitectura de securitate (ADV_ARC) pentru carduri inteligente și dispozitive similare», versiunea 1.1;

      5. «Certificarea produselor pentru carduri inteligente „deschise”», versiunea 1.1;

      6. «Cerințe privind arhitectura de securitate pentru carduri inteligente și dispozitive similare», versiunea 1.1;

      7. «Aplicarea potențialului de atac asupra cardurilor inteligente și a dispozitivelor similare», versiunea 1.2;

   (b) următoarele documente referitoare la evaluarea armonizată a domeniului tehnic «dispozitive hardware cu casete de securitate»:

      1. «Cerințe minime ale ITSEF privind evaluările de securitate ale dispozitivelor hardware cu casete de securitate», versiunea 1.1;

      2. «Cerințe minime de securitate a site-ului», versiunea 1.1;

      3. «Aplicarea potențialului de atac asupra dispozitivelor hardware cu casete de securitate», versiunea 1.2.

2. Documente ce reflectă stadiul actual al tehnologiei referitoare la acreditarea armonizată a organismelor de evaluare a conformității:

   (a) «Acreditarea ITSEF pentru EUCC», versiunea 1.1, pentru acreditările emise înainte de 8 iulie 2025;

   (b) «Acreditarea ITSEF pentru EUCC», versiunea 1.6c, pentru acreditările nou emise sau revizuite după 8 iulie 2025;

   (c) «Acreditarea organismelor de control pentru EUCC», versiunea 1.6b.””

ANEXA II

În anexa IV secțiunea IV.3 la Regulamentul de punere în aplicare (UE) 2024/482, punctele 5 și 6 se înlocuiesc cu următorul text:

„5. În cazul în care modificările au fost confirmate de organismul de certificare ca fiind minore, nu se eliberează niciun nou certificat pentru produsul TIC modificat și se întocmește un raport de menținere a raportului de certificare inițial.

Raportul de menținere este inclus ca subset al raportului de analiză a impactului, cu următoarele secțiuni:

(a) introducere;

(b) descrierea modificărilor;

(c) elementele de probă ale dezvoltatorului în cauză.

6. Raportul de menținere menționat la punctul 5 se pune la dispoziția ENISA în vederea publicării pe site-ul acesteia de certificare a securității cibernetice.”