2026/1735

22.7.2026

REGULAMENTUL DE PUNERE ÎN APLICARE (UE) 2026/1735 AL COMISIEI

din 15 iulie 2026

de modificare a Regulamentului de punere în aplicare (UE) 2025/1569 în ceea ce privește standardele și specificațiile aplicabile

COMISIA EUROPEANĂ,

având în vedere Tratatul privind funcționarea Uniunii Europene,

având în vedere 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 ([1]), în special articolul 45d alineatul (5), articolul 45e alineatul (2), articolul 45f alineatul (6) și articolul 45f alineatul (7),

întrucât:

(1) Pentru a asigura cel mai înalt nivel de armonizare între statele membre în ceea ce privește dezvoltarea portofelelor europene pentru identitatea digitală, specificațiile tehnice aferente portofelelor se întemeiază pe activitatea desfășurată pe baza Recomandării (UE) 2021/946 a Comisiei ([2]) și în special pe arhitectura și pe cadrul de referință. Întrucât arhitectura și cadrul de referință au evoluat semnificativ de la adoptarea Regulamentului de punere în aplicare (UE) 2025/1569 al Comisiei ([3]), Regulamentul de punere în aplicare (UE) 2025/1569 ar trebui acum modificat pentru a-l alinia la noile standarde și specificații.

(2) În conformitate cu obiectivele Regulamentului (UE) nr. 910/2014, au fost selectate o serie de standarde pentru a îndeplini cerințele aplicabile în cazul emiterii, gestionării și verificării atestatelor electronice ale atributelor. Aceste standarde ar trebui să reflecte practicile consacrate și să fie recunoscute pe scară largă în sectoarele relevante. Dacă este necesar, respectivele standarde ar trebui adaptate sau completate pentru a asigura un nivel înalt de securitate și integritate în ceea ce privește atestatele electronice ale atributelor, facilitând în același timp interoperabilitatea transfrontalieră și funcționarea eficace a pieței interne. În concordanță cu acest obiectiv, prezentul regulament actualizează cerințele aplicabile emiterii și revocării de atestate electronice calificate ale atributelor și de atestate electronice ale atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism și introduce cerințe privind semnarea și sigilarea rezultatelor verificării prin raportarea la surse autentice.

(3) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului ([4]) și, după caz, Directiva 2002/58/CE a Parlamentului European și a Consiliului ([5]) se aplică tuturor activităților de prelucrare a datelor cu caracter personal efectuate în temeiul prezentului regulament.

([1]) JO L 257, 28.8.2014, p. 73, ELI: http://data.europa.eu/eli/reg/2014/910/oj.

([2]) Recomandarea (UE) 2021/946 a Comisiei din 3 iunie 2021 privind un set de instrumente comun al Uniunii pentru o abordare coordonată în direcția unui cadru european al identității digitale (JO L 210, 14.6.2021, p. 51, ELI: http://data.europa.eu/eli/reco/2021/946/oj).

([3]) Regulamentul de punere în aplicare (UE) 2025/1569 al Comisiei din 29 iulie 2025 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește atestatele electronice calificate ale atributelor și atestatele electronice ale atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism (JO L, 2025/1569, 30.7.2025, ELI: http://data.europa.eu/eli/reg_impl/2025/1569/oj).

([4]) Regulamentul (UE) 2016/679 al Parlamentului European și al Consiliului din 27 aprilie 2016 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal și privind libera circulație a acestor date și de abrogare a Directivei 95/46/CE (Regulamentul general privind protecția datelor) (JO L 119, 4.5.2016, p. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([5]) Directiva 2002/58/CE a Parlamentului European și a Consiliului din 12 iulie 2002 privind prelucrarea datelor personale și protejarea confidențialității în sectorul comunicațiilor publice (Directiva asupra confidențialității și comunicațiilor electronice) (JO L 201, 31.7.2002, p. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

(4) Autoritatea Europeană pentru Protecția Datelor a fost consultată în conformitate cu articolul 42 alineatul (1) din Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului ([6]) și a emis un aviz la 17 aprilie 2026 ([7]).

(5) Măsurile prevăzute în prezentul regulament sunt conforme cu avizul comitetului instituit prin articolul 48 din Regulamentul (UE) nr. 910/2014,

ADOPTĂ PREZENTUL REGULAMENT:

Articolul 1

Modificări ale Regulamentului de punere în aplicare (UE) 2025/1569

Regulamentul de punere în aplicare (UE) 2025/1569 se modifică după cum urmează:

1. La articolul 3, alineatul (2) se înlocuiește cu următorul text:

„(2) În cazul în care furnizorii de atestate electronice calificate ale atributelor și furnizorii de atestate electronice ale atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism emit atestate electronice autentice ale atributelor care sunt incluse în sisteme înregistrate în catalogul sistemelor de atestare a atributelor, aceștia trebuie să respecte cerințele sistemului corespunzător de atestare a atributelor. Politicile și procedurile stabilite de emitenții de atestate pentru a asigura respectarea cerințelor sistemelor de atestare a atributelor fac parte din evaluarea conformității stabilită în Regulamentul (UE) nr. 910/2014.”

2. Articolul 4 se modifică după cum urmează:

(a) alineatul (1) se elimină;

(b) alineatul (3) se înlocuiește cu următorul text:

„(3) În cazul în care perioada de valabilitate a atestatelor electronice calificate ale atributelor și a atestatelor electronice ale atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism este mai mare de 24 de ore, furnizorii respectivelor atestate le revocă cel puțin în următoarele situații:

(a) la cererea persoanei pentru care s-a emis atestatul electronic al atributelor sau, după caz, la cererea persoanei care a făcut obiectul atestatului respectiv;

(b) în cazul în care furnizorul ia cunoștință de faptul că a fost compromisă securitatea sau credibilitatea atestatelor electronice calificate ale atributelor sau a atestatelor electronice ale atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism;

(c) în alte situații, astfel cum se prevede în dreptul Uniunii sau în dreptul intern.”;

(c) alineatul (4) se înlocuiește cu următorul text:

„(4) Furnizorii de atestate electronice calificate ale atributelor și furnizorii de atestate electronice ale atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism stabilesc tehnici de revocare și metode de gestionare a revocării care respectă confidențialitatea și împiedică stabilirea de legături sau trasabilitatea. Tehnicile de revocare trebuie să respecte cerințele prevăzute în anexa II.”

([6]) Regulamentul (UE) 2018/1725 al Parlamentului European și al Consiliului din 23 octombrie 2018 privind protecția persoanelor fizice în ceea ce privește prelucrarea datelor cu caracter personal de către instituțiile, organele, oficiile și agențiile Uniunii și privind libera circulație a acestor date și de abrogare a Regulamentului (CE) nr. 45/2001 și a Deciziei nr. 1247/2002/CE (JO L 295, 21.11.2018, p. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Observațiile formale ale AEPD cu privire la proiectul de regulament de punere în aplicare al Comisiei referitor la standardele și specificațiile aplicabile pentru înregistrarea beneficiarilor portofelelor | Autoritatea Europeană pentru Protecția Datelor.

3. Articolul 9 se modifică după cum urmează:

   (a) după alineatul (2) se introduc următorul alineat (2a):

   „(2a) Mecanismul de verificare trebuie să respecte cerințele prevăzute în anexa IV.”;

   (b) alineatul (4) se înlocuiește cu următorul text:

   „(4) Rezultatul verificării indică dacă atributul a fost verificat sau nu și specifică organismul din sectorul public responsabil de sursa autentică sau, după caz, organismul din sectorul public desemnat să acționeze în numele sursei autentice în raport cu care a fost verificat atributul.

   Rezultatul verificării este semnat sau sigilat de organismul din sectorul public responsabil de o sursă autentică sau de intermediarul desemnat recunoscut la nivel național, cu utilizarea a cel puțin unei semnături electronice avansate bazată pe un certificat calificat pentru semnăturile electronice sau, respectiv, a unui sigiliu electronic avansat bazat pe un certificat calificat pentru sigiliile electronice.”

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

5. Anexa II se înlocuiește cu textul din anexa II la prezentul regulament.

6. Textul din anexa III la prezentul regulament se adaugă ca anexa IV.

Articolul 2

Intrarea în vigoare

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

Articolul 1 alineatul (3) se aplică de la 1 ianuarie 2027.

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

Adoptat la Bruxelles, 15 iulie 2026.

Pentru Comisie
Președinta
Ursula VON DER LEYEN

ANEXA I

„ANEXA I

Lista standardelor de referință și a specificațiilor menționate la articolul 3

ETSI TS 119 471 V1.1.1 (2025-05) se aplică cu următoarele adaptări:

1. 2.1. Referințe normative:

   [1] ETSI EN 319 401 V3.2.1 (2026-01): «Semnăturile electronice și infrastructurile de încredere (ESI); Cerințele privind politica generală a prestatorilor de servicii de încredere»;

   [2] Grupul european pentru certificarea securității cibernetice, Subgrupul privind criptografia: «Mecanisme criptografice convenite», publicat de Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA);

   [3] FIPS PUB 140-3 (2019) «Cerințe de securitate pentru modulele criptografice»;

   [4] Regulamentul de punere în aplicare (UE) 2024/482 al Comisiei ([1]);

   [5] Regulamentul de punere în aplicare (UE) 2024/3144 al Comisiei ([2]);

   [6] ISO/IEC 15408:2022 (părțile 1-5): «Securitatea informațiilor, securitatea cibernetică și protecția vieții private – Criterii de evaluare a securității IT».

2. 3.1. Termeni:
   Se adaugă următorul termen:

   — dispozitiv criptografic securizat: dispozitiv care stochează cheia privată a utilizatorului, protejează această cheie împotriva compromiterii și îndeplinește funcții de semnare sau decriptare în numele utilizatorului

3. 4. Servicii EAA (*electronic attestation of attributes* – atestat electronic al atributelor) de încredere

   — Clauza 4.2.2.2: «*Verification of attributes against authentic sources*» nu se aplică.

   — REQ-EAASP-4.2.2.3-02: EAASP se autentifică la instanța EUDIW implementând mecanisme de autentificare reciprocă care utilizează un certificat de acces valabil.

   — REQ-EAASP-4.2.2.3-03: EAASP validează unitatea EUDIW și verifică dacă instanța EUDIW a fost revocată.

   — Clauza 4.3.2: «*EUDIW Specific*» nu se aplică.

4. 6.1. Declarația de practică a EAAS (*electronic attestation of attributes service* – serviciul de emitere a atestatelor electronice ale atributelor):

   — REQ-EAASP-6.1-02: EAASP (*electronic attestation of attributes service provider* – prestatorul de servicii care emite atestatul electronic al atributelor) documentează mecanismul de revocare în declarația de practică a EAAS

5. 6.3. Politica în domeniul securității informațiilor:

   — REQ-EAASP-6.3-02: EAASP stabilește proceduri de notificare a organismului de supraveghere cu privire la orice modificare survenită în prestarea serviciului de încredere de emitere a atestatului electronic al atributelor și cu privire la intenția sa de a înceta aceste activități, în conformitate cu cerințele comerciale și cu actele cu putere de lege și normele administrative relevante, inclusiv în conformitate cu cerințele prevăzute în actele de punere în aplicare adoptate în temeiul articolului 24 alineatul (5) din Regulamentul (UE) nr. 910/2014. EAASP transmite notificări organismului de supraveghere cel puțin:

     — cu o lună înainte de punerea în aplicare a oricărei modificări;

     — cu trei luni înainte de încetarea planificată a prestării unui serviciu de încredere.

([1]) 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).

([2]) 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 (JO L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

6. 7.5. Controale criptografice:

   — REQ-EAASP-7.5.2-05: necompletat

   — REQ-EAASP-7.5.2-06: necompletat

   — REQ-EAASP-7.5.3-01A: Trebuie instituite controale de securitate adecvate pentru gestionarea oricăror chei criptografice, algoritmi criptografici și dispozitive criptografice pe parcursul întregului lor ciclu de viață, urmând, după caz, o abordare bazată pe agilitatea criptografică.

   — REQ-EAASP-7.5.3-01B: În vederea prestării serviciilor de încredere, EAASP selectează și utilizează tehnici criptografice adecvate, conforme cu documentul «Mecanisme criptografice convenite» aprobat de Grupul european pentru certificarea securității cibernetice și publicat de ENISA [2].

   — REQ-EAASP-7.5.3-02: EAASP se asigură că dispozitivul criptografic securizat pe care îl utilizează pentru semnătura digitală sau sigiliul digital al EAA este un dispozitiv calificat de creare a semnăturii sau a sigiliului și că toate celelalte semnături sau sigilii digitale utilizate pentru a furniza atestatul electronic corespunzător al atributelor serviciului de încredere, sau o parte din acestea, sunt create prin intermediul unui dispozitiv criptografic securizat care este un sistem de încredere certificat în conformitate cu:

     (a) criteriile comune de evaluare a securității IT, astfel cum sunt stabilite în criteriile comune de evaluare a securității IT, versiunea 3.1 (CC3.1) până la 31.8.2027 sau în versiunea CC:2022, părțile 1-5, publicate de participanții la Acordul privind recunoașterea certificatelor de criterii comune în domeniul securității informatice sau astfel cum sunt stabilite în ISO/IEC 15408 [6], și certificat la nivelul EAL 4 sau la un nivel de securitate mai ridicat sau

     (b) sistemul european de certificare a securității cibernetice bazat pe criterii comune (EUCC) [4] [5] și certificat la nivelul EAL 4 sau la un nivel de securitate mai ridicat sau

     (c) FIPS-140-2 nivelul 3 de utilizat până la 31.8.2027 pentru sistemele certificate existente sau FIPS PUB 140-3 [3] nivelul 3 până la 31.12.2030.

     Această certificare se referă la un obiectiv de securitate sau un profil de protecție ori la un proiect de modul și o documentație de securitate care îndeplinesc cerințele prezentului document, pe baza unei analize a riscurilor și ținând seama de măsurile de securitate fizice și de altă natură fără caracter tehnic.

     În cazul în care dispozitivul criptografic securizat beneficiază de o certificare EUCC [4] [5], dispozitivul respectiv se configurează și se utilizează în conformitate cu certificarea respectivă.

   — REQ-EAASP-7.5.5-01: necompletat

   — REQ-EAASP-7.5.5-02: necompletat

   — REQ-EAASP-7.5.5-04: necompletat

7. 7.9. Vulnerabilități și gestionarea incidentelor:

   — REQ-EAASP-7.9-02: Activitățile de monitorizare țin seama de sensibilitatea oricăror informații colectate sau analizate.

8. 7.12. Încetarea serviciilor și planuri de încetare a serviciilor ale EAASP și EAAS:

   — REQ-EAASP-7.12-04: Planul EAASP în caz de încetare a serviciilor trebuie să respecte cerințele prevăzute în actele de punere în aplicare adoptate în temeiul articolului 24 alineatul (5) din Regulamentul (UE) nr. 910/2014 [i.1]."

ANEXA II

„ANEXA II

Specificațiile tehnice menționate la articolele 3 și 4

Furnizorii de atestate electronice calificate ale atributelor și furnizorii de atestate electronice ale atributelor emise de un organism din sectorul public responsabil de o sursă autentică sau în numele unui astfel de organism își emit atestatele în conformitate cu cel puțin unul dintre standardele enumerate în anexa II la Regulamentul de punere în aplicare (UE) 2024/2979 al Comisiei ([1]) și aplică tehnicile de revocare relevante prevăzute tot în anexa II la Regulamentul de punere în aplicare (UE) 2024/2979 al Comisiei.”

([1]) Regulamentul de punere în aplicare (UE) 2024/2979 al Comisiei din 28 noiembrie 2024 de stabilire a normelor de aplicare a Regulamentului (UE) nr. 910/2014 al Parlamentului European și al Consiliului în ceea ce privește integritatea și funcționalitățile de bază ale portofelelor europene pentru identitatea digitală (JO L, 2024/2979, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2979/oj).

ANEXA III

„ANEXA IV

Lista standardelor și a specificațiilor tehnice menționate la articolul 9

Mecanismele de verificare menționate la articolul 9 trebuie să respecte una sau ambele specificații de mai jos, cu următoarele adaptări:

(a) specificații tehnice prevăzute în clauza 6.1.1 din ETSI TS 119 478 V1.1.1 (2026-01) – *Electronic Signatures and Trust Infrastructures (ESI)*; specificațiile interfețelor aferente surselor autentice;

— REQ-ASIP-6.1.1.2-04-01 [CONDIȚIONAT]: În cazul în care atributul attributeVerificationResult este fie http://uri.etsi.org/19478/VerificationResult/Match, fie http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, atributul attributeVerificationResult poate conține un element attributeValue.

— REQ-ASIP-6.1.1.2-04-02 [CONDIȚIONAT]: În cazul în care atributeVerificationResult returnat este http://uri.etsi.org/19478/VerificationResult/Match, iar atributeVerificationResult conține un element atributeValue, atunci elementul atributeValue trebuie să conțină valoarea din cerere.

— REQ-ASIP-6.1.1.2-04-03 [CONDIȚIONAT]: În cazul în care atributeVerificationResult returnat este http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, iar attributeVerificationResult conține un element atributeValue, atunci elementul atributeValue trebuie să conțină valoarea atributului astfel cum este stocată în sursa autentică.

— REQ-ASIP-6.1.1.2-06-04-01 [CONDIȚIONAT]: În cazul în care fragmentVerificationResult este fie http://uri.etsi.org/19478/VerificationResult/Match, fie http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, atributul attributeVerificationResult poate conține un element fragmentValue.

— REQ-ASIP-6.1.1.2-06-04-02 [CONDIȚIONAT]: În cazul în care fragmentVerificationResult returnat este http://uri.etsi.org/19478/VerificationResult/Match, iar atributeVerificationResult conține un element fragmentValue, atunci elementul fragmentValue trebuie să conțină valoarea din cerere.

— REQ-ASIP-6.1.1.2-06-04-03 [CONDIȚIONAT]: În cazul în care fragmentVerificationResult returnat este http://uri.etsi.org/19478/VerificationResult/MatchWithVariation, iar attributeVerificationResult conține un element fragmentValue, atunci elementul fragmentValue trebuie să conțină valoarea fragmentului atributului astfel cum este stocată în sursa autentică.

(b) specificații tehnice prevăzute în clauza 6.2.3 din ETSI TS 119 478 V1.1.1 (2026-01) – *Electronic Signatures and Trust Infrastructures (ESI)*; specificațiile interfețelor aferente surselor autentice.

— REQ-ASIP-6.2.3.2.1-08-04: Elementul AttributeVerificationResponse poate include exact un singur element copil din gama TextValue, XMLValue sau AttributeProperties.”