REGOLAMENTO DI ESECUZIONE (UE) 2026/798 DELLA COMMISSIONE

del 7 aprile 2026

recante modalità di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda le norme di riferimento e le specifiche per l'onboarding a distanza degli utenti nei portafogli europei di identità digitale tramite mezzi di identificazione elettronica conformi al livello di garanzia significativo unitamente a ulteriori procedure di onboarding a distanza la cui combinazione soddisfa i requisiti del livello di garanzia elevato

LA COMMISSIONE EUROPEA,

visto il regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE ([1]), in particolare l'articolo 5 *bis*, paragrafo 24,

considerando quanto segue:

(1) L'onboarding degli utenti nei portafogli europei di identità digitale («portafogli») è un passaggio cruciale per quanto riguarda la verifica dell'identità degli utenti dei portafogli e il collegamento dei dati di identificazione personale degli utenti ai rispettivi portafogli e al dispositivo dell'utente in cui sono installate le unità di portafoglio.

(2) Al fine di promuovere un elevato livello di fiducia e sicurezza e un approccio armonizzato in tutti gli Stati membri per l'onboarding degli utenti dei portafogli con procedure di onboarding a distanza unitamente ai mezzi di identificazione elettronica conformi al livello di garanzia significativo, il presente atto di esecuzione stabilisce specifiche e procedure per facilitare l'onboarding degli utenti nel portafoglio europeo di identità digitale tramite mezzi di identificazione elettronica conformi al livello di garanzia significativo unitamente a ulteriori procedure di onboarding a distanza che, insieme, soddisfano i requisiti del livello di garanzia elevato.

(3) Tali norme dovrebbero rispecchiare le pratiche consolidate ed essere ampiamente riconosciute nei settori pertinenti. Esse dovrebbero essere adattate in modo da includere requisiti che garantiscano la sicurezza e l'affidabilità dell'onboarding degli utenti.

(4) Il regolamento di esecuzione (UE) 2015/1502 della Commissione ([2]) stabilisce che, se i mezzi di identificazione elettronica sono rilasciati a un livello di garanzia elevato, e tenendo conto dei rischi di variazione dei dati di identificazione personale, non è necessario ripetere i processi di controllo e verifica dell'identità. In tal caso gli Stati membri dovrebbero pertanto ricorrere ai mezzi di identificazione elettronica rilasciati a un livello di garanzia elevato anche per il processo di onboarding ai fini del presente regolamento.

(5) Qualora gli Stati membri eseguano l'onboarding degli utenti nei portafogli utilizzando un mezzo di identificazione elettronica che non è stato notificato alla Commissione, il livello di garanzia di tale mezzo dovrebbe essere confermato da un organismo di valutazione della conformità definito all'articolo 2, punto 13), del regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio ([3]) o da un organismo equivalente e dovrebbe essere dimostrato che i risultati di tale precedente procedura di rilascio di un mezzo di identificazione elettronica sono ancora validi.

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

([2]) Regolamento di esecuzione (UE) 2015/1502 della Commissione, dell'8 settembre 2015, relativo alla definizione delle specifiche e procedure tecniche minime riguardanti i livelli di garanzia per i mezzi di identificazione elettronica ai sensi dell'articolo 8, paragrafo 3, del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno (GU L 235 del 9.9.2015, pag. 7, ELI: http://data.europa.eu/eli/reg_impl/2015/1502/oj).

([3]) Regolamento (CE) n. 765/2008 del Parlamento europeo e del Consiglio, del 9 luglio 2008, che pone norme in materia di accreditamento e vigilanza del mercato per quanto riguarda la commercializzazione dei prodotti e che abroga il regolamento (CEE) n. 339/93 (GU L 218 del 13.8.2008, pag. 30, ELI: http://data.europa.eu/eli/reg/2008/765/oj).

(6) Sebbene l'allegato stabilisca i requisiti da soddisfare per conseguire un livello specifico di controllo dell'identità, non è stata stabilita l'equivalenza per quanto riguarda il livello di garanzia di cui all'articolo 8 del regolamento (UE) n. 910/2014. I requisiti stabiliti nell'allegato dovrebbero pertanto essere considerati l'attuazione di quelli del regolamento di esecuzione (UE) 2015/1502 ed essere soddisfatti dal fornitore di dati di identificazione personale o da un soggetto che fornisce servizi di controllo dell'identità per conto di tale fornitore.

(7) La Commissione valuta periodicamente le nuove tecnologie, pratiche e specifiche tecniche. Conformemente al considerando 75 del regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio ([4]), la Commissione dovrebbe riesaminare e, se necessario, aggiornare il presente regolamento di esecuzione per mantenerlo in linea con gli sviluppi globali e le nuove tecnologie, norme o specifiche tecniche e per seguire le migliori pratiche sul mercato interno, in particolare per quanto riguarda l'onboarding degli utenti nel portafoglio.

(8) Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([5]) e, se del caso, il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([6]) e la direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([7]) si applicano alle attività di trattamento di dati personali a norma del presente regolamento.

(9) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725, il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 30 gennaio 2026 ([8]).

(10) Il comitato istituito dall'articolo 48 del regolamento (UE) n. 910/2014 non ha espresso alcun parere entro il termine fissato dal suo presidente,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Le norme di riferimento e le specifiche di cui all'articolo 5 *bis*, paragrafo 24, del regolamento (UE) n. 910/2014 figurano nell'allegato del presente regolamento.

([4]) Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, dell'11 aprile 2024, che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale (GU L, 2024/1183, 30.4.2024, ELI: http://data.europa.eu/eli/reg/2024/1183/oj).

([5]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1, ELI: http://data.europa.eu/eli/reg/2016/679/oj).

([6]) Regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio, del 23 ottobre 2018, sulla tutela delle persone fisiche in relazione al trattamento dei dati personali da parte delle istituzioni, degli organi e degli organismi dell'Unione e sulla libera circolazione di tali dati, e che abroga il regolamento (CE) n. 45/2001 e la decisione n. 1247/2002/CE (GU L 295 del 21.11.2018, pag. 39, ELI: http://data.europa.eu/eli/reg/2018/1725/oj).

([7]) Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37, ELI: http://data.europa.eu/eli/dir/2002/58/oj).

([8]) EDPS Formal comments on the draft Commission Implementing Regulation as regards onboarding of users to the European Digital Identity Wallets.

Articolo 2

Il presente regolamento entra in vigore il ventesimo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Il presente regolamento è obbligatorio in tutti i suoi elementi e direttamente applicabile in ciascuno degli Stati membri.

Fatto a Bruxelles, il 7 aprile 2026

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO

Elenco delle norme di riferimento e delle specifiche

La conformità è valutata rispetto ai punti della norma ETSI TS 119 461 V2.1.1 (2025-02) elencati nella sezione 1, subordinatamente agli adeguamenti elencati nella sezione 2.

Sezione 1 Punti applicabili

—	5	Operational risk assessment;
—	6	Policies and practices;
—	7	Identity proofing service management and operation;
—	8	Identity proofing service requirements;
—	9.1	Introduction, compliance with the present document, general requirements for all use cases;
—	9.2.2	Use cases using an identity document for attended remote identity proofing;
—	9.2.3	Use cases using an identity document for unattended remote identity proofing;
—	9.2.4	Use case for identity proofing by authentication using eID means;
—	9.5	Use cases for additional identity proofing to enhance an identity proven by use of an eID from Baseline LoIP to Extended LoIP.

Sezione 2 Adeguamenti

1) 5 Operational risk assessment

— OVR-5-01: si applicano i requisiti specificati nella norma ETSI EN 319 401 [1], punto 5.

— *Nota 1:* quando il controllo dell'identità è eseguito direttamente dal fornitore di dati di identificazione personale, la valutazione del rischio del fornitore di dati di identificazione personale può riguardare il controllo dell'identità.

2) 6.1 Identity proofing service practice statement

— OVR-6.1-02: nella sua dichiarazione sulla pratica, il prestatore di servizi di controllo dell'identità (IPSP) deve indicare i casi d'uso per i quali è dichiarata la conformità al presente documento.

— *Nota 1:* quando il controllo dell'identità è eseguito direttamente dal fornitore di dati di identificazione personale, la dichiarazione sulla pratica del servizio di controllo dell'identità del fornitore di dati di identificazione personale può riguardare le informazioni sul controllo dell'identità e non è necessaria una dichiarazione sulla pratica specifica per il controllo dell'identità.

3) 7.9 Vulnerabilities and incident management

— OVR-7.9-02: gli obblighi di comunicazione conformemente alla norma ETSI EN 319401 [1] REQ-7.9.2-02X e al punto 7.9.3 devono essere soddisfatti come richiesto dal contesto del controllo dell'identità e dagli obblighi del fornitore di dati di identificazione personale che fa affidamento sul servizio dell'IPSP.

— Esempio: la comunicazione all'autorità di vigilanza che vigila su un fornitore di portafogli europei di identità digitale stabilito nello Stato membro designante può essere effettuata in cooperazione tra l'IPSP e il fornitore di dati di identificazione personale.

4) 7.10 Collection of evidence

— OVR-7.10-01: si applicano i requisiti specificati nella norma ETSI EN 319 401 [1], punto 7.10.

— *Nota 1:* i requisiti a lungo termine per la conservazione delle prove possono essere soddisfatti dal fornitore di dati di identificazione personale che richiede il controllo dell'identità anziché dall'IPSP qualora essi siano soggetti diversi.

— *Nota 2:* si applicano i requisiti del punto 8.5.2 del presente documento.

5) 7.11 Business continuity management

— OVR-7.11-02: i processi per la gestione delle crisi conformemente alla norma ETSI EN 319401 [1] REQ-7.11.3-01X devono corrispondere a quanto richiesto dal contesto del controllo dell'identità e dagli obblighi del fornitore di dati di identificazione personale che fa affidamento sul servizio dell'IPSP.

6) 7.12 Termination and termination plans

— OVR-7.12-01: si applicano i requisiti specificati nella norma ETSI EN 319401 [1], punto 7.12, eccetto REQ-7.12-11.

— *Nota:* se sono soggetti diversi, l'IPSP e il fornitore di dati di identificazione personale che richiede il controllo dell'identità possono concordare un'assistenza reciproca o unilaterale nella definizione dei piani di cessazione.

7) 8.1 Initiation

— INI-8.1-05: se il processo di controllo dell'identità a distanza è interrotto o non va a buon fine, l'IPSP deve garantire che le persone dispongano di sufficienti spiegazioni e mezzi di ricorso, specialmente in caso di controllo dell'identità a distanza non assistito. Le informazioni dovrebbero garantire che le persone interessate possano contribuire efficacemente alla rapida risoluzione del problema e, se necessario, esercitare i propri diritti, ad esempio il diritto di rettifica o la possibilità di contestare la decisione, nei confronti del titolare del trattamento.

8) 8.2.1 General requirements

— COL-8.2.1-08: l'IPSP deve attuare misure per garantire la conformità ai requisiti della protezione dei dati fin dalla progettazione e della protezione dei dati per impostazione predefinita conformemente all'articolo 25 del regolamento (UE) 2016/679 durante il processo di onboarding, soprattutto per quanto riguarda il trattamento di dati biometrici. Misure pertinenti possono consistere in adeguati controlli crittografici, dispositivi e misure organizzative che rafforzano la tutela della vita privata. Tali misure dovrebbero limitare la raccolta dei dati a quanto strettamente necessario per il trattamento dei dati biometrici e di qualsiasi altro dato personale da raccogliere dalle fonti fisiche e digitali di identificazione per collegare i dati di identificazione personale dell'utente ai suoi portafogli e al dispositivo dell'utente in cui è installata l'unità di portafoglio.

9) 8.2.4 Use of existing eID means as evidence

— [CONDIZIONALE] COL-8.2.4-02X: se ad essere interessato è il livello di controllo dell'identità (LoIP) di base, i mezzi di identificazione elettronica (eID) devono essere stati notificati almeno a un livello di garanzia (LoA) eIDAS significativo, oppure il relativo livello di garanzia deve essere stato confermato da un organismo di valutazione della conformità accreditato definito all'articolo 2, punto 13), del regolamento (CE) n. 765/2008 o da un organismo equivalente e, se sono soddisfatti tutti i requisiti applicabili, la valutazione deve dar luogo a un certificato di conformità basato su una verifica della certificazione. Tale processo di certificazione formale deve essere basato su un processo di valutazione della sicurezza che fa riferimento ai livelli di garanzia definiti per i mezzi di identificazione elettronica notificati o per i portafogli europei di identità digitale certificati a norma del regolamento (UE) n. 910/2014 [i.25].

— COL-8.2.4-02 A: vuoto.

10) 8.3.1 General requirements

— VAL-8.3.1-11X: il processo di controllo dell'identità deve verificare che le prove siano valide al momento del controllo dell'identità.

11) 8.3.3 Validation of physical identity document

— VAL-8.3.3-21: l'efficacia delle misure per conformarsi ai requisiti VAL-8.3.3-05X, VAL-8.3.3-05 A, VAL-8.3.3-05B, VAL-8.3.3-05C, VAL-8.3.3-07 A e VAL-8.3.3-07X deve essere confermata da un organismo di valutazione della conformità accreditato definito all'articolo 2, punto 13), del regolamento (CE) n. 765/2008 o da un organismo equivalente.

— VAL-8.3.3-22: l'immagine facciale di riferimento proveniente dal documento di identità fisico deve essere ottenuta utilizzando la comunicazione in prossimità (*near field communication*) e il processo deve eseguire l'autenticazione passiva o attiva del chip sul documento di identità fisico.

12) 9.1 Introduction, compliance with the present document, general requirements for all use cases

— USE-9.1-01X: per essere conforme al presente documento, un processo di controllo dell'identità deve conformarsi al caso d'uso di cui al punto 9.5 del presente documento per il LoIP esteso.

— USE-9.1-03X: vuoto.

13) 9.2.3.4 Use case for automated operation

— USE-9.2.3.4-04: l'IPSP deve stabilire valori target per i falsi positivi (FAR) e i falsi negativi (FAS), sulla base di un'analisi dei rischi e della relativa procedura di intelligence sulle minacce, seguendo la metodologia stabilita nella relazione dell'ENISA «Methodology for sector cybersecurity assessment» [i.28] o una metodologia equivalente, nei processi di controllo dell'identità completamente automatizzati. I valori target usati dall'IPSP devono essere pari o inferiori a quelli fissati per i casi d'uso ibridi, se esistenti. L'IPSP deve mantenere coerentemente tali valori target per i FAR e i FAS, supportato da un'analisi dei rischi e dalla relativa procedura di intelligence sulle minacce.

14) 9.5.1 General requirements

— Primo comma: se il richiedente è una persona fisica, compresa una persona fisica che rappresenta una persona giuridica, e l'identità del richiedente è stata dimostrata al LoIP di base mediante autenticazione tramite un'eID, ed è richiesto un rafforzamento fino al LoIP esteso, si applicano i requisiti seguenti.

— USE-9.5.1-08: il controllo aggiuntivo dell'identità richiesto per rafforzare l'affidabilità di un'identità è applicabile solo all'eID che non è stata rilasciata facendo affidamento su un confronto automatizzato tra immagini facciali per il processo di rilascio iniziale.

15) 9.5.2 Use case for enhancing identity proofing to Extended LoIP by a full identity proofing using an identity document

— USE-9.5.2-01: il rafforzamento del controllo dell'identità dal LoIP di base a quello esteso deve essere conforme ai requisiti per il LoIP esteso di uno dei casi d'uso descritti ai punti 9.2.2 o 9.2.3 del presente documento per il LoIP esteso.

16) 9.5.3 Use case for enhancing identity proofing to Extended LoIP by use of a previously captured reference face image

— USE-9.5.3-01: per acquisire un'immagine facciale di riferimento e collegare i necessari attributi di identità a tale immagine deve essere utilizzato un processo di controllo dell'identità che soddisfi i requisiti del LoIP esteso di uno dei casi d'uso descritti ai punti 9.2.2 o 9.2.3 del presente documento, o un processo di controllo dell'identità che è stato sottoposto a valutazione tra pari o certificato da un organismo di valutazione della conformità accreditato definito all'articolo 2, punto 13), del regolamento (CE) n. 765/2008 o da un organismo equivalente per rispettare un livello di garanzia elevato conformemente al regolamento (UE) n. 910/2014 [i.25].