2025/2532

17.12.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/2532 DELLA COMMISSIONE

del 16 dicembre 2025

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 applicabili ai servizi di archiviazione elettronica qualificati

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione 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 45 *undecies*, paragrafo 2,

considerando quanto segue:

(1) Con il regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio ([2]) è stato introdotto nel regolamento (UE) n. 910/2014 un elenco di nuovi servizi fiduciari e servizi fiduciari qualificati, tra cui il servizio di archiviazione elettronica qualificato. La Commissione deve redigere un elenco di norme di riferimento e, se necessario, stabilire specifiche per tali servizi.

(2) L'archiviazione elettronica è un servizio che consente la ricezione, la conservazione, la consultazione e la cancellazione di dati elettronici e documenti elettronici al fine di garantirne la durabilità e leggibilità nonché di preservarne l'integrità, la riservatezza e la prova dell'origine per tutto il periodo di conservazione; I servizi di archiviazione elettronica qualificati svolgono un ruolo cruciale nell'ambiente imprenditoriale digitale, promuovendo la transizione dai processi cartacei tradizionali ai loro equivalenti elettronici. Per garantire che i dati elettronici e i documenti elettronici mantengano la presunzione della loro integrità e della correttezza della loro origine per la durata del periodo di conservazione da parte del prestatore di servizi fiduciari qualificato e per conseguire un elevato livello di trasparenza e fiducia tra tutti i partecipanti al ciclo di vita delle informazioni, è necessario stabilire una serie comune di specifiche per i servizi di archiviazione elettronica qualificati.

(3) Per aumentare il valore probatorio, la sicurezza e l'affidabilità dei servizi di archiviazione elettronica qualificati, laddove le firme elettroniche, i sigilli elettronici o le validazioni temporali elettroniche siano utilizzati per creare, firmare, sigillare o attestare la data e l'ora, ad esempio, dell'archiviazione di prove, delle registrazioni di prove, delle registrazioni di eventi, delle registrazioni della corretta attuazione di procedure o dell'archiviazione di relazioni di conferma, dovrebbero essere utilizzati servizi fiduciari qualificati.

(4) La presunzione di conformità di cui all'articolo 45 *undecies*, paragrafo 2, del regolamento (UE) n. 910/2014 dovrebbe applicarsi solo se i servizi di archiviazione elettronica qualificati soddisfano i requisiti stabiliti nel presente regolamento. Le norme di riferimento applicabili ai servizi di archiviazione elettronica qualificati dovrebbero rispecchiare le prassi consolidate ed essere ampiamente riconosciute nei settori pertinenti. Dette norme dovrebbero essere adattate in modo da includere controlli supplementari che garantiscano la sicurezza e l'affidabilità dei servizi di archiviazione elettronica qualificati.

(5) Se un prestatore di servizi fiduciari rispetta i requisiti di cui al presente regolamento, gli organismi di vigilanza dovrebbero presumere la conformità ai pertinenti requisiti del regolamento (UE) n. 910/2014 e tenere debitamente conto di tale presunzione per la concessione o la conferma della qualifica del servizio fiduciario. Un prestatore di servizi fiduciari qualificato può comunque fare affidamento su altre pratiche per dimostrare la conformità ai requisiti del regolamento (UE) n. 910/2014.

(6) Per preservare l'integrità e la prova dell'origine dei dati elettronici e dei documenti elettronici contenenti una o più firme elettroniche qualificate o sigilli elettronici qualificati, i servizi di archiviazione elettronica qualificati dovrebbero utilizzare procedure e tecnologie in grado di estendere l'affidabilità di tali firme elettroniche e sigilli elettronici oltre il periodo di validità tecnologica, almeno per tutto il periodo di conservazione.

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

([2]) 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.

(7) La Commissione valuta periodicamente le nuove tecnologie, pratiche, norme o specifiche tecniche. Conformemente al considerando 75 del regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio, la Commissione dovrebbe riesaminare e, se necessario, aggiornare il presente regolamento per mantenerlo in linea con gli sviluppi globali e le nuove tecnologie, pratiche, norme o specifiche tecniche e per seguire le migliori pratiche nel mercato interno.

(8) Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([3]) e, se del caso, la direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([4]) si applicano a tutte le attività di trattamento di dati personali a norma del presente regolamento.

(9) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([5]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere il 21 ottobre 2025 ([6]).

(10) Le misure di cui al presente regolamento sono conformi al parere del comitato istituito dall'articolo 48 del regolamento (UE) n. 910/2014,

HA ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Archiviazione elettronica di documenti recanti una firma elettronica qualificata o un sigillo elettronico qualificato

1. Nell'archiviare dati elettronici o documenti elettronici recanti firme elettroniche qualificate o sigilli elettronici qualificati, i prestatori di servizi di archiviazione elettronica qualificati garantiscono che sia mantenuta l'affidabilità di tali firme elettroniche qualificate o sigilli elettronici qualificati, anche oltre il loro periodo di validità tecnologica, e che siano mantenute l'integrità e l'esattezza dell'origine delle firme elettroniche qualificate e dei sigilli elettronici qualificati, almeno fino alla fine del periodo di conservazione legale o contrattuale.

2. Ai fini del paragrafo 1, i prestatori di servizi di archiviazione elettronica qualificati possono avvalersi di un servizio di conservazione qualificato delle firme elettroniche qualificate o di un servizio di conservazione qualificato dei sigilli elettronici qualificati.

Articolo 2

Norme di riferimento e specifiche per la prestazione di servizi di archiviazione elettronica qualificati

Le norme di riferimento e le specifiche di cui all'articolo 45 *undecies*, paragrafo 2, del regolamento (UE) n. 910/2014 figurano nell'allegato del presente regolamento.

([3]) 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).

([4]) 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).

([5]) 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).

([6]) «EDPS Formal comments on the draft Implementing Regulation laying down rules for the application of Regulation (EU) No 910/2014 as regards reference standards and specifications for qualified electronic archiving services».

Articolo 3

Entrata in vigore

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 16 dicembre 2025

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO

Elenco delle norme di riferimento e delle specifiche per i servizi di archiviazione elettronica qualificati

CEN/TS 18170: 2025 («CEN/TS 18170»), si applica con i seguenti adattamenti:

a) riferimenti normativi (punto 2)

— ETSI EN 319 401 V3.1.1 (2024-06), «Electronic Signatures and Trust Infrastructures (ESI)»; «General Policy Requirements for Trust Service Providers».

— ETSI EN 319 421 V1.3.1 (2025-07), «Electronic Signatures and Infrastructures (ESI)»; «Policy and Security Requirements for Trust Service Providers issuing Time-Stamps».

— ISO 14721:2025, «Space Data System Practices — Reference model for an open archival information system (OAIS)».

— ACM-ECCG; gruppo europeo per la certificazione della cibersicurezza, sottogruppo sulla crittografia: «Agreed Cryptographic Mechanisms» (meccanismi crittografici concordati) pubblicati dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA).

— Regolamento (UE) 2024/482; regolamento di esecuzione (UE) 2024/482 della Commissione ([1]).

— Regolamento (UE) 2024/3144; regolamento di esecuzione (UE) 2024/3144 della Commissione ([2]).

— ISO/IEC 15408:2022 (parti da 1 a 5), «Information security, cybersecurity and privacy protection – Evaluation criteria for IT security».

— FIPS PUB 140-3 (2019) «Security Requirements for Cryptographic Modules»;

b) dichiarazione sulla politica e sulla pratica (punto 6.1)

— Si applicano i requisiti della norma CEN/TS 18170, punto 6.1.

— Si applicano i requisiti della norma ETSI EN 319 401, punto 5.

— L'EATSP stabilisce procedure per notificare all'organismo di vigilanza eventuali modifiche nella prestazione del servizio fiduciario di archiviazione elettronica e l'intenzione di cessare tali attività, conformemente ai requisiti commerciali e alle disposizioni legislative e regolamentari pertinenti, anche conformemente ai requisiti degli atti di esecuzione adottati a norma dell'articolo 24, paragrafo 5, del regolamento (UE) n. 910/2014 [i.2].

— L'EATSP effettua la notifica all'organismo di vigilanza competente almeno:

— un mese prima dell'attuazione di qualsiasi modifica;

— tre mesi prima della cessazione prevista di una prestazione di servizi fiduciari;

c) termini e condizioni (punto 6.2)

— Si applicano i requisiti della norma CEN/TS 18170, punto 6.2.

— Prima di avviare una relazione contrattuale gli abbonati e le parti facenti affidamento sul servizio fiduciario di archiviazione elettronica sono informati in modo chiaro, completo e facilmente accessibile, in uno spazio accessibile al pubblico e individualmente, di termini e condizioni precisi;

([1]) Regolamento (UE) 2024/482 della Commissione, del 31 gennaio 2024, recante modalità di applicazione del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio per quanto riguarda l'adozione del sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (EUCC) (GU L, 2024/482, 7.2.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/482/oj).

([2]) Regolamento (UE) 2024/3144 della Commissione, del 18 dicembre 2024, che modifica il regolamento di esecuzione (UE) 2024/482 per quanto riguarda le norme internazionali applicabili e che rettifica tale regolamento di esecuzione (GU L, 2024/3144, 19.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/3144/oj).

d) risorse umane (punto 7.3)

— Si applicano i requisiti della norma CEN/TS 18170, punto 7.3.

— Il personale dell'EATSP in ruoli di fiducia e, se del caso, i subcontraenti dell'EATSP in ruoli di fiducia sono in grado di soddisfare il requisito in materia di «competenze, esperienza e qualifiche» mediante formazione e credenziali formali, o effettiva esperienza, o una combinazione di entrambe. Sono compresi aggiornamenti periodici (almeno ogni 12 mesi) sulle nuove minacce e sulle attuali pratiche di sicurezza;

e) controlli e monitoraggio crittografici (punto 7.6)

— Il sistema di archiviazione deve garantire la riservatezza dei dati e dei documenti durante l'intero ciclo di vita dell'archivio, dal deposito all'eliminazione.

— Si applicano i requisiti specificati nella norma ETSI EN 319 401, sottopunto 7.5 «Controlli crittografici».

— L'origine dei dati da archiviare nel sistema di archiviazione elettronica è stabilita dall'EATSP. Se a tal fine sono utilizzati firme elettroniche o sigilli elettronici, tali firme elettroniche o sigilli elettronici sono qualificati.

— Quando l'EATSP appone una firma digitale su (parte di) un oggetto o una registrazione digitale, la chiave di firma privata dell'EATSP è conservata e utilizzata all'interno di un dispositivo qualificato per la creazione di una firma elettronica o di un sigillo elettronico o di un dispositivo crittografico sicuro che è un sistema affidabile certificato conformemente:

  a) ai criteri comuni per la valutazione della sicurezza delle tecnologie informatiche, quali definiti nella norma ISO/IEC 15408 o nel documento «Common Criteria for Information Technology Security Evaluation», versione CC:2022, parti da 1 a 5, pubblicato dai partecipanti all'accordo «Arrangement on the Recognition of Common Criteria Certificates in the field of IT Security», e certificato a livello EAL 4 o superiore; o

  b) al sistema europeo di certificazione della cibersicurezza basato sui criteri comuni (regolamento (UE) 2024/482, regolamento (UE) 2024/3144) e certificato a livello EAL 4 o superiore; o

  c) fino al 31.12.2030, al FIPS PUB 140-3 livello 3.

— Tale certificazione riguarda un obiettivo di sicurezza o un profilo di protezione, o la progettazione di un modulo e la documentazione di sicurezza, che soddisfano i requisiti del presente documento, sulla base di un'analisi dei rischi e tenendo conto delle misure di sicurezza fisiche e di altre misure di sicurezza non tecniche.

— Se il dispositivo crittografico sicuro beneficia di una certificazione EUCC (regolamento (UE) 2024/482, regolamento (UE) 2024/3144), tale dispositivo è configurato e utilizzato conformemente a tale certificazione.

— L'EATSP monitora la resistenza dell'algoritmo crittografico che è stato ed è utilizzato. Nel caso in cui si ritenga che uno degli algoritmi o dei parametri utilizzati diventi inadeguato come definito nella gestione dei rischi, l'EATSP aggiorna la relativa politica di archiviazione o crea un nuovo profilo di archiviazione per gestire i pacchetti di archiviazione (*Archive Information Package*, AIP) e definire ed eseguire misure adeguate.

— La valutazione degli algoritmi crittografici e il loro utilizzo da parte dell'EATSP sono conformi ai meccanismi crittografici concordati approvati dal gruppo europeo per la certificazione della cibersicurezza e pubblicati dall'ENISA (ACM-ECCG).

— I componenti tecnici dell'EATS si autenticano reciprocamente sulla base di tecniche crittografiche prima di comunicare;

f) rete (punto 7.9)

— Si applicano i requisiti specificati nella norma ETSI EN 319 401, sottopunto 7.8 «Sicurezza della rete».

— La scansione delle vulnerabilità richiesta dal requisito REQ-7.8-13 della norma ETSI EN 319 401 è eseguita almeno una volta a trimestre.

— Il test di penetrazione richiesto dal requisito REQ-7.8-17X della norma ETSI EN 319 401 è eseguito almeno una volta all'anno.

— I firewall sono configurati in modo da bloccare tutti i protocolli e gli accessi non richiesti per il funzionamento dell'EATSP;

g) raccolta delle prove (punto 7.11)

— Si applicano i requisiti specificati nella norma ETSI EN 319 401, sottopunto 7.10 «Raccolta di prove», anche per gli eventi critici e non critici (cfr. sottopunto 13.2);

h) cessazione dell'EATSP e piano di cessazione (punto 7.13)

— Si applicano i requisiti della norma CEN/TS 18170, punto 7.13.

— Il piano di cessazione dell'EATSP è conforme ai requisiti stabiliti negli atti di esecuzione adottati a norma dell'articolo 24, paragrafo 5, del regolamento (UE) n. 910/2014;

i) orario affidabile degli eventi (punto 13.3.1)

— Si applicano i requisiti della norma CEN/TS 18170, punto 13.3.1.

— Quando utilizza la marcatura temporale, l'EATSP utilizza una marcatura temporale qualificata.