2025/2160

28.10.2025

REGOLAMENTO DI ESECUZIONE (UE) 2025/2160 DELLA COMMISSIONE

del 27 ottobre 2025

recante modalità di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda le norme, le specifiche e le procedure di riferimento per la gestione dei rischi connessi alla prestazione di servizi fiduciari non 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 19 *bis*, paragrafo 2,

considerando quanto segue:

(1) I prestatori di servizi fiduciari non qualificati svolgono un ruolo importante nell'ambiente digitale fornendo servizi fiduciari che facilitano le transazioni elettroniche sicure. Il regolamento (UE) n. 910/2014 impone meno requisiti normativi ai prestatori di servizi fiduciari non qualificati rispetto a quelli previsti per i prestatori di servizi fiduciari qualificati. Tuttavia tutti i prestatori di servizi fiduciari sono soggetti a requisiti in materia di sicurezza e responsabilità per garantire il dovere di diligenza, la trasparenza e l'assunzione di responsabilità in relazione alle loro operazioni e ai loro servizi.

(2) I prestatori di servizi fiduciari non qualificati possono essere considerati soggetti importanti o essenziali ai sensi dell'articolo 3 della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio ([2]). Pertanto il regolamento di esecuzione (UE) 2024/2690 della Commissione ([3]), che stabilisce i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza, si applica a tali prestatori. Tuttavia l'ambito di applicazione dei requisiti di cui all'articolo 19 *bis*, paragrafo 1, lettera a), del regolamento (UE) n. 910/2014 riguarda le procedure di gestione dei rischi giuridici, commerciali, operativi e di altro tipo, sia diretti che indiretti, per la prestazione di servizi fiduciari non qualificati. Per integrare il quadro di gestione dei rischi di cui al regolamento di esecuzione (UE) 2024/2690 e consentire un approccio coerente alla gestione di tutte le tipologie pertinenti di rischi, è opportuno stabilire specifiche e procedure relative alla gestione di tali rischi da parte dei prestatori di servizi fiduciari non qualificati. Gli orientamenti forniti dall'Agenzia dell'Unione europea per la cibersicurezza (ENISA) o dalle autorità nazionali competenti a norma della direttiva (UE) 2022/2555 possono sostenere i prestatori di servizi fiduciari non qualificati nella progettazione e nell'attuazione di adeguate politiche di gestione dei rischi.

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

([2]) Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80, ELI: http://data.europa.eu/eli/dir/2022/2555/oj).

([3]) Regolamento di esecuzione (UE) 2024/2690 della Commissione, del 17 ottobre 2024, recante modalità di applicazione della direttiva (UE) 2022/2555 per quanto riguarda i requisiti tecnici e metodologici delle misure di gestione dei rischi di cibersicurezza e l'ulteriore specificazione dei casi in cui un incidente è considerato significativo per quanto riguarda i fornitori di servizi DNS, i registri dei nomi di dominio di primo livello, i fornitori di servizi di cloud computing, i fornitori di servizi di data center, i fornitori di reti di distribuzione dei contenuti, i fornitori di servizi gestiti, i fornitori di servizi di sicurezza gestiti, i fornitori di mercati online, di motori di ricerca online e di piattaforme di servizi di social network e i prestatori di servizi fiduciari (GU L, 2024/2690, 18.10.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2690/oj).

(3) La presunzione di conformità di cui all'articolo 19 *bis*, paragrafo 2, del regolamento (UE) n. 910/2014 dovrebbe applicarsi solo se i prestatori di servizi fiduciari non qualificati soddisfano i requisiti stabiliti nel presente regolamento. Le norme di riferimento di cui all'allegato dovrebbero rispecchiare le prassi consolidate ed essere ampiamente riconosciute nei settori pertinenti. Al fine di garantire che i prestatori di servizi fiduciari non qualificati gestiscano rischi giuridici, commerciali, operativi e di altro tipo, sia diretti che indiretti, per la prestazione del servizio fiduciario non qualificato conformemente all'articolo 19 *bis*, paragrafo 1, del regolamento (UE) n. 910/2014, tali prestatori dovrebbero conformarsi agli elementi di riferimento delle norme di cui all'allegato e ai requisiti di gestione dei rischi di cui al presente regolamento per la presunzione di conformità.

(4) Se un prestatore di servizi fiduciari non qualificato rispetta i requisiti di cui al presente regolamento di esecuzione, gli organismi di vigilanza dovrebbero presumere la conformità ai pertinenti requisiti del regolamento (UE) n. 910/2014. Un prestatore di servizi fiduciari non qualificato può comunque fare affidamento su altre pratiche per dimostrare la conformità ai requisiti del regolamento (UE) n. 910/2014.

(5) Per garantire che i rischi individuati siano affrontati in modo adeguato, le politiche di gestione dei rischi seguite dai prestatori di servizi fiduciari non qualificati dovrebbero includere procedure in materia di documentazione e valutazione dei rischi, nonché di individuazione, selezione e attuazione di misure di trattamento dei rischi idonee. L'attuazione delle misure di trattamento dei rischi dovrebbe essere costantemente monitorata. Per quanto riguarda le informazioni che registrano e conservano nell'ambito delle loro misure di trattamento dei rischi, i prestatori di servizi fiduciari non qualificati dovrebbero garantire l'integrità e la riservatezza di tali dati. Inoltre, al fine di migliorare la trasparenza e sostenere le attività di vigilanza, è opportuno che i prestatori di servizi fiduciari non qualificati pubblichino i metodi di verifica dell'identità da essi applicati. Poiché non tutti i rischi individuati possono essere pienamente affrontati attraverso misure di prevenzione, attenuazione o trasferimento ad altri soggetti, gli eventuali rischi residui dovrebbero essere approvati dagli organi di gestione dei prestatori di servizi fiduciari non qualificati. I criteri per l'accettazione dei rischi residui dovrebbero essere giustificati in modo comprensibile.

(6) 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 ([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, pratiche, norme o specifiche tecniche e per seguire le migliori pratiche nel mercato interno.

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

(8) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([7]), il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere l'8 agosto 2025 ([8]).

([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]) 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).

([7]) 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).

([8]) *EDPS Formal comments on the draft Implementing Regulation as regards specifications and procedures for the management of risks to the provision of non-qualified trust services*, Garante europeo della protezione dei dati.

(9) 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

Norme di riferimento

Le norme di riferimento di cui all'articolo 19 *bis*, paragrafo 2, del regolamento (UE) n. 910/2014 figurano nell'allegato del presente regolamento.

Articolo 2

Politiche di gestione dei rischi

1. Le politiche di gestione dei rischi di cui all'articolo 19 *bis*, paragrafo 1, del regolamento (UE) n. 910/2014 individuano chiaramente i servizi fiduciari cui si applicano, sono specifiche per i servizi fiduciari interessati e sono approvate dall'organo di gestione del prestatore di servizi fiduciari non qualificato.

2. Le politiche di gestione dei rischi comprendono almeno gli elementi seguenti:

a) il livello complessivo di tolleranza per i rischi conformemente alla criticità e al livello richiesto di sicurezza dei servizi fiduciari, tenendo conto dei più recenti sviluppi tecnologici;

b) i pertinenti criteri di rischio, comprendenti almeno la probabilità, l'impatto e il livello del rischio, tenendo conto dei dati sulle minacce informatiche e delle vulnerabilità;

c) un approccio all'individuazione e alla documentazione dei rischi per la prestazione dei servizi fiduciari, che tenga conto dell'intero ambito di applicazione del sistema informativo utilizzato dal prestatore di servizi fiduciari non qualificato, compresi i rischi associati alle componenti del sistema, nonché a qualsiasi parte attiva o passiva coinvolta nell'attuazione del sistema o nella prestazione dei servizi fiduciari;

d) un processo di valutazione dei rischi individuati sulla base dei criteri di rischio di cui alla lettera b);

e) un processo di individuazione, definizione delle priorità e monitoraggio continuo dell'attuazione di misure di trattamento dei rischi idonee;

f) un processo di monitoraggio continuo dell'attuazione delle politiche di gestione dei rischi.

3. I prestatori di servizi fiduciari non qualificati stabiliscono procedure adeguate e conservano i documenti per garantire l'attuazione dei requisiti previsti dalla normativa applicabile.

4. I prestatori di servizi fiduciari non qualificati stabiliscono procedure adeguate e documentate atte a garantire il monitoraggio delle modifiche legislative e regolamentari dell'Unione e nazionali che possono incidere sulla prestazione di servizi fiduciari.

Articolo 3

Individuazione, documentazione e valutazione dei rischi

I prestatori di servizi fiduciari non qualificati individuano, documentano e valutano tutti i rischi di cui all'articolo 19 *bis*, paragrafo 1, del regolamento (UE) n. 910/2014 conformemente alle politiche di gestione dei rischi di cui all'articolo 2 e in particolare:

a) individuano i rischi in relazione a terzi;

b) individuano i singoli punti di vulnerabilità potenziali nella prestazione di servizi fiduciari;

c) valutano i rischi individuati sulla base dei criteri di rischio di cui all'articolo 2, paragrafo 2, lettera b).

Articolo 4

Misure di trattamento dei rischi

1. In conformità alle politiche di cui all'articolo 2, i prestatori di servizi fiduciari non qualificati pianificano, documentano e attuano misure di trattamento dei rischi e, in particolare, svolgono i seguenti compiti:

a) individuare le misure adeguate per il trattamento dei rischi e attribuirvi la priorità;

b) selezionare, approvare e documentare le misure di trattamento dei rischi prescelte, compresi i relativi requisiti di sicurezza e procedure operative, in un piano di trattamento dei rischi, e individuare il responsabile dell'attuazione di tali misure e i tempi di attuazione ad esse associati;

c) monitorare costantemente l'attuazione delle misure di trattamento dei rischi.

2. Il piano di trattamento dei rischi di cui al paragrafo 1, lettera b), fornisce in modo comprensibile i motivi che giustificano l'accettazione dei rischi residui.

3. Nell'ambito delle misure di trattamento dei rischi di cui al paragrafo 1, i prestatori di servizi fiduciari non qualificati provvedono altresì a:

a) verificare, se del caso, l'identità degli utenti del servizio fiduciario in maniera diretta o tramite terzi e pubblicare informazioni sui metodi di verifica dell'identità utilizzati;

b) al fine di fornire prove nei procedimenti giudiziari e di garantire la continuità del servizio, registrare e conservare in modo sicuro per il tempo necessario conformemente al diritto dell'Unione o nazionale, anche dopo la cessazione delle attività del prestatore di servizi fiduciari non qualificato, le seguenti informazioni:

   — tutte le informazioni pertinenti raccolte durante il processo di registrazione e di onboarding degli utenti di servizi fiduciari, compresa, se del caso, la verifica dell'identità di tali utenti,

   — i dati di autenticazione assegnati all'utente del servizio fiduciario, se del caso, e

   — qualsiasi modifica dello stato dei certificati a chiave pubblica o di altro materiale crittografico utilizzato nella prestazione del servizio fiduciario;

c) garantire, se del caso, che i dati di autenticazione assegnati all'utente del servizio fiduciario siano univoci.

4. Nell'individuare, selezionare e approvare le misure di trattamento dei rischi idonee, come pure nel definirne l'ordine di priorità, i prestatori di servizi fiduciari non qualificati tengono conto dei seguenti elementi:

a) i risultati della valutazione dei rischi di cui all'articolo 3;

b) l'efficacia delle misure di trattamento dei rischi;

c) le valutazioni della conformità;

d) gli incidenti significativi;

e) i costi di attuazione in relazione ai benefici attesi;

f) la classificazione appropriata delle risorse applicabile;

g) l'analisi dell'impatto sulle attività aziendali dei rischi individuati conformemente all'articolo 3.

5. Gli organi di gestione dei prestatori di servizi fiduciari non qualificati approvano i rischi residui che permangono dopo l'attuazione delle misure di trattamento dei rischi previste dal piano di trattamento dei rischi.

6. I prestatori di servizi fiduciari non qualificati esaminano, documentano e, se del caso, aggiornano i risultati della valutazione dei rischi e il piano di trattamento dei rischi a intervalli pianificati, e almeno una volta all'anno, nonché in caso di cambiamenti significativi dell'infrastruttura, delle operazioni o dei rischi, o di incidenti significativi.

7. I prestatori di servizi fiduciari non qualificati garantiscono la disponibilità, l'integrità e la riservatezza delle informazioni di cui al paragrafo 3, lettera b).

Articolo 5

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 27 ottobre 2025

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO

Elenco delle norme di riferimento per i prestatori di servizi fiduciari non qualificati

Si applicano i requisiti di cui alle seguenti clausole della norma ETSI EN 319 401, V3.1.1 (2024-06): «Firme elettroniche e infrastrutture fiduciarie (ESI); Requisiti di politica generale per i prestatori di servizi fiduciari»:

5. Valutazione dei rischi;
6. Politiche e pratiche;
7.1 Organizzazione interna;
7.2 Risorse umane;
7.3 Gestione delle risorse;
7.4 Controllo dell'accesso;
7.6 Sicurezza fisica e ambientale.