REGOLAMENTO DI ESECUZIONE (UE) 2025/847 DELLA COMMISSIONE

del 6 maggio 2025

recante modalità di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda le reazioni a violazioni della sicurezza dei portafogli europei di identità digitale

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 5 *sexies*, paragrafo 5,

considerando quanto segue:

(1) Il quadro europeo relativo a un'identità digitale («quadro») istituito dal regolamento (UE) n. 910/2014 costituisce un componente essenziale per la creazione di un ecosistema per l'identità digitale sicuro e interoperabile in tutta l'Unione. Il quadro, di cui i portafogli europei di identità digitale («portafogli») sono la pietra angolare, mira a facilitare l'accesso ai servizi in tutti gli Stati membri, garantendo nel contempo la protezione dei dati personali e della vita privata.

(2) I regolamenti (UE) 2016/679 ([2]) e (UE) 2018/1725 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 alle attività di trattamento di dati personali a norma del presente regolamento. Le norme sulla valutazione e la comunicazione delle informazioni stabilite dal presente regolamento lasciano impregiudicati l'obbligo di notificare le violazioni dei dati personali all'autorità di controllo competente, se del caso, a norma del regolamento (UE) 2016/679 o del regolamento (UE) 2018/1725, e l'obbligo di comunicare tali violazioni agli interessati, se del caso, a norma di tali regolamenti.

(3) La Commissione valuta periodicamente tecnologie, pratiche, norme e specifiche tecniche nuove. Al fine di garantire il massimo livello di armonizzazione tra gli Stati membri per lo sviluppo e la certificazione dei portafogli, le specifiche tecniche di cui al presente regolamento si fondano sul lavoro svolto nell'ambito della raccomandazione (UE) 2021/946 ([5]), in particolare l'architettura e il quadro di riferimento che ne fanno parte. Conformemente al considerando 75 del regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio ([6]), la Commissione dovrebbe riesaminare e, se necessario, aggiornare il presente regolamento per mantenerlo in linea con gli sviluppi globali, l'architettura e il quadro di riferimento e per seguire le migliori pratiche sul mercato interno.

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

([2]) 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).

([3]) 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).

([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]) Raccomandazione (UE) 2021/946 della Commissione del 3 giugno 2021 relativa a un pacchetto di strumenti comuni dell'Unione per un approccio coordinato verso un quadro europeo relativo a un'identità digitale (GU L 210 del 14.6.2021, pag. 51, ELI: http://data. europa.eu/eli/reco/2021/946/oj).

([6]) 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).

(4) In caso di violazione della sicurezza o di compromissione delle soluzioni di portafoglio o dei meccanismi di convalida di cui all'articolo 5 *bis*, paragrafo 8, del regolamento (UE) n. 910/2014, o del regime di identificazione elettronica nell'ambito del quale sono fornite le soluzioni di portafoglio, è necessario che a tali violazioni della sicurezza e compromissioni faccia seguito una reazione rapida, coordinata e sicura in tutti gli Stati membri, volta a proteggere gli utenti e mantenere la fiducia nell'ecosistema dell'identità digitale. Ciò non pregiudica la direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio ([7]) e i regolamenti (UE) 2019/881 ([8]) e (UE) 2024/2847 ([9]) del Parlamento europeo e del Consiglio, in particolare per quanto riguarda la gestione degli incidenti o delle vulnerabilità e il fatto che siano considerati violazioni della sicurezza. Gli Stati membri dovrebbero pertanto provvedere affinché la fornitura e l'uso dei portafogli interessati da una violazione della sicurezza o da una compromissione siano tempestivamente sospesi o, se del caso, tali portafogli siano ritirati.

(5) Affinché le reazioni a una violazione della sicurezza o a una compromissione siano adeguate, gli Stati membri dovrebbero valutare se una violazione della sicurezza o la compromissione di una soluzione di portafoglio, dei meccanismi di convalida di cui all'articolo 5 *bis*, paragrafo 8, del regolamento (UE) n. 910/2014 o del regime di identificazione elettronica nell'ambito del quale è fornita una soluzione di portafoglio pregiudichi l'affidabilità di tale soluzione o di altre soluzioni di portafoglio. Tale valutazione dovrebbe basarsi su criteri uniformi, quali il numero e la categoria degli utenti del portafoglio, delle persone fisiche e delle parti facenti affidamento sul portafoglio interessati, la natura dei dati interessati, la durata della compromissione o della violazione della sicurezza, la disponibilità limitata di un servizio e le perdite finanziarie, nonché la potenziale compromissione dei dati personali. Tali criteri dovrebbero fornire agli Stati membri flessibilità e discrezionalità per stabilire in modo proporzionato se l'affidabilità di una soluzione di portafoglio sia pregiudicata e se la sospensione o, ove giustificato dalla gravità della violazione o della compromissione, il ritiro della soluzione di portafoglio siano appropriati. Tali criteri non dovrebbero comportare automaticamente il ritiro o la sospensione della fornitura e dell'uso di una soluzione di portafoglio, ma dovrebbero essere debitamente presi in considerazione dagli Stati membri al momento di decidere se tali ritiro o sospensione siano necessari.

(6) In considerazione dell'impatto e dei disagi causati dalla sospensione dell'uso delle soluzioni di portafoglio, gli Stati membri dovranno valutare se, per rispondere in modo adeguato alla violazione della sicurezza o alla compromissione, sia necessaria la revoca degli attestati di unità di portafoglio o altre misure supplementari.

(7) Per tenere informati gli utenti del portafoglio in merito allo stato dei loro portafogli, è necessario fornire loro informazioni adeguate sulle violazioni della sicurezza o sulle compromissioni che interessano i loro portafogli. Poiché anche le parti facenti affidamento sul portafoglio registrate nell'Unione possono essere interessate da violazioni della sicurezza e da compromissioni, le informazioni pertinenti riguardanti violazioni della sicurezza e compromissioni devono essere condivise anche con loro.

(8) Al fine di accrescere la trasparenza e rafforzare la fiducia nell'ecosistema dell'identità digitale, le informazioni in merito alle violazioni della sicurezza o alle compromissioni e alle relative conseguenze dovrebbero quanto meno comprendere le informazioni richieste a norma del presente regolamento. Le informazioni riguardanti violazioni della sicurezza o compromissioni, condivise con gli utenti del portafoglio e le parti facenti affidamento sul portafoglio, dovrebbero tuttavia essere attentamente valutate al fine di prevenire e ridurre al minimo il rischio che possano essere sfruttate da aggressori.

([7]) 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).

([8]) Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 («regolamento sulla cibersicurezza») (GU L 151 del 7.6.2019, pag. 15, ELI: http://data.europa.eu/eli/reg/2019/881/oj).

([9]) Regolamento (UE) 2024/2847 del Parlamento europeo e del Consiglio, del 23 ottobre 2024, relativo a requisiti orizzontali di cibersicurezza per i prodotti con elementi digitali e che modifica i regolamenti (UE) n. 168/2013 e (UE) 2019/1020 e la direttiva (UE) 2020/1828 (regolamento sulla ciberresilienza) (GU L, 2024/2847, 20.11.2024, ELI: http://data.europa.eu/eli/reg/2024/2847/oj).

(9) Per consentire agli utenti di accedere nuovamente alle proprie unità di portafoglio una volta posto rimedio a una violazione della sicurezza o a una compromissione, lo Stato membro che ha fornito le soluzioni di portafoglio dovrà ripristinarne la fornitura e l'uso senza indebito ritardo. A tale scopo è possibile ripristinare le unità di portafoglio, rilasciare unità di portafoglio fornite nell'ambito di una nuova versione delle soluzioni di portafoglio o rilasciare nuovi attestati di unità di portafoglio validi. Gli utenti del portafoglio interessati, le parti facenti affidamento sul portafoglio, i punti di contatto unici designati a norma dell'articolo 46 *quater*, paragrafo 1, del regolamento (UE) n. 910/2014 e la Commissione devono essere informati di conseguenza.

(10) Per garantire il ritiro dei portafogli qualora non sia stato posto rimedio a una violazione della sicurezza o a una compromissione entro tre mesi dalla sospensione o qualora ciò sia giustificato dalla gravità della violazione della sicurezza o della compromissione, lo Stato membro dovrebbe provvedere affinché gli attestati di unità di portafoglio pertinenti siano revocati e non possano tornare in stato di validità né essere rilasciati o forniti a unità di portafoglio esistenti. È inoltre opportuno non fornire nuove unità di portafoglio nell'ambito della soluzione di portafoglio interessata. A fini di trasparenza, gli utenti, le parti facenti affidamento sulla certificazione, i punti di contatto unici designati a norma dell'articolo 46 *quater*, paragrafo 1, del regolamento (UE) n. 910/2014 e la Commissione devono essere informati del ritiro. Tali comunicazioni includono una descrizione dei potenziali impatti sugli utenti del portafoglio, in particolare sulla gestione degli attestati rilasciati, o sulle parti facenti affidamento sul portafoglio.

(11) Il periodo di tre mesi successivo alla sospensione della fornitura e dell'uso di una soluzione di portafoglio, e durante il quale deve essere posto rimedio alla violazione della sicurezza o alla compromissione che ha portato a tale sospensione, dovrebbe rappresentare un termine oltre il quale la soluzione di portafoglio deve essere ritirata a meno che non sia stato adottato un rimedio adeguato. Gli Stati membri sono tuttavia liberi di esigere che sia posto rimedio alla violazione della sicurezza o alla compromissione entro un termine inferiore a tre mesi, tenendo conto, in particolare e se del caso, della portata, della durata e delle conseguenze di tale violazione della sicurezza o compromissione. Se non è possibile porre rimedio alla violazione della sicurezza o alla compromissione entro il termine da esso stabilito, lo Stato membro può esigere che la soluzione di portafoglio sia ritirata prima della scadenza del periodo di tre mesi. Gli Stati membri dovrebbero utilizzare il periodo di tempo durante il quale è necessario porre rimedio a una violazione della sicurezza o a una compromissione che ha portato alla sospensione della fornitura e dell'uso di una soluzione di portafoglio per preparare il possibile ritiro di tale soluzione di portafoglio e le relative comunicazioni.

(12) Al fine di ridurre gli oneri amministrativi a carico degli Stati membri per quanto riguarda le informazioni da fornire alla Commissione e agli altri Stati membri a norma del presente regolamento, gli Stati membri dovrebbero utilizzare gli strumenti di notifica esistenti, come il sistema di segnalazione e analisi degli incidenti informatici (*Cyber Incident Reporting and Analysis System*, «CIRAS») gestito dall'Agenzia dell'Unione europea per la cibersicurezza («ENISA»). Per quanto riguarda i canali o i mezzi alternativi da utilizzare per informare gli utenti del portafoglio interessati da una violazione della sicurezza o da una compromissione e le parti facenti affidamento sul portafoglio, gli Stati membri dovrebbero provvedere affinché le informazioni pertinenti siano fornite in modo chiaro, completo e facilmente accessibile. I canali per fornire tali informazioni agli utenti del portafoglio interessati e alle parti facenti affidamento sul portafoglio dovrebbero comprendere soluzioni adeguate per la trasmissione basata su siti web, il monitoraggio in tempo reale di aggiornamenti di siti web e l'aggregazione delle notizie.

(13) 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 31 gennaio 2025.

(14) 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

Oggetto

Il presente regolamento stabilisce le norme per la reazione alle violazioni della sicurezza dei portafogli, dei meccanismi di convalida di cui all'articolo 5 *bis*, paragrafo 8, del regolamento (UE) n. 910/2014 e del regime di identificazione elettronica nell'ambito del quale sono forniti i portafogli.

Articolo 2

Definizioni

Ai fini del presente regolamento si applicano le definizioni seguenti:

1) «soluzione di portafoglio»: una combinazione di software, hardware, servizi, impostazioni e configurazioni, comprese le istanze di portafoglio, una o più applicazioni crittografiche sicure per il portafoglio e uno o più dispositivi crittografici sicuri per il portafoglio;

2) «utente del portafoglio»: un utente che ha il controllo dell'unità di portafoglio;

3) «parte facente affidamento sul portafoglio»: una parte facente affidamento sulla certificazione che intende fare affidamento sulle unità di portafoglio per la prestazione di servizi pubblici o privati mediante interazione digitale;

4) «istanza di portafoglio»: l'applicazione installata e configurata su un dispositivo o su un ambiente di un utente del portafoglio, che fa parte di un'unità di portafoglio, e che l'utente del portafoglio utilizza per interagire con l'unità di portafoglio;

5) «applicazione crittografica sicura per il portafoglio»: un'applicazione che gestisce risorse critiche tramite un collegamento alle funzioni crittografiche e non crittografiche fornite dal dispositivo crittografico sicuro per il portafoglio e l'uso di tali funzioni;

6) «dispositivo crittografico sicuro per il portafoglio»: un dispositivo resistente alle manomissioni che fornisce un ambiente collegato all'applicazione crittografica sicura per il portafoglio e da essa utilizzato per proteggere le risorse critiche e fornire funzioni crittografiche per l'esecuzione sicura di operazioni critiche;

7) «fornitore del portafoglio»: una persona fisica o giuridica che fornisce soluzioni di portafoglio;

8) «unità di portafoglio»: una configurazione unica di una soluzione di portafoglio che comprende istanze di portafoglio, applicazioni crittografiche sicure per il portafoglio e dispositivi crittografici sicuri per il portafoglio forniti da un fornitore del portafoglio a un singolo utente del portafoglio;

9) «risorse critiche»: risorse all'interno di un'unità di portafoglio o ad essa relative, di importanza tale che un'eventuale compromissione della loro disponibilità, riservatezza o integrità avrebbe un effetto estremamente grave e debilitante sulla possibilità di fare affidamento sull'unità di portafoglio;

10) «attestato di unità di portafoglio»: un oggetto di dati che descrive i componenti dell'unità di portafoglio o consente la loro autenticazione e convalida.

Articolo 3

Accertamento di una violazione della sicurezza o di una compromissione

1. Fatti salvi la direttiva (UE) 2022/2555 e i regolamenti (UE) 2019/881 e (UE) 2024/2847, gli Stati membri tengono debitamente conto dei criteri di cui all'allegato I del presente regolamento al fine di valutare se una violazione della sicurezza o una compromissione di una soluzione di portafoglio, dei meccanismi di convalida di cui all'articolo 5 *bis*, paragrafo 8, del regolamento (UE) n. 910/2014 o del regime di identificazione elettronica nell'ambito del quale è fornita la soluzione di portafoglio pregiudichi la loro affidabilità o l'affidabilità di altre soluzioni di portafoglio.

2. Qualora accerti, sulla base della valutazione di cui al paragrafo 1, che una violazione della sicurezza o una compromissione pregiudica l'affidabilità di una soluzione di portafoglio e sospenda la fornitura e l'uso di tale soluzione di portafoglio, uno Stato membro adotta le misure di cui agli articoli 4 e 5. Qualora ritiri la soluzione di portafoglio, lo Stato membro adotta le misure di cui agli articoli 8 e 9.

3. Uno Stato membro che venga a conoscenza di informazioni relative a una possibile violazione della sicurezza o a una possibile compromissione, che potrebbe pregiudicare l'affidabilità di una o più soluzioni di portafoglio fornite da un altro Stato membro, ne dà comunicazione senza indebito ritardo alla Commissione e ai punti di contatto unici degli Stati membri interessati designati a norma dell'articolo 46 *quater*, paragrafo 1, del regolamento (UE) n. 910/2014. Detta comunicazione comprende le informazioni di cui all'articolo 5, paragrafo 2.

4. Lo Stato membro che riceve le informazioni fornite a norma del paragrafo3 adotta le misure di cui ai paragrafi 1 e 2 senza indebito ritardo.

Articolo 4

Sospensione della fornitura e dell'uso dei portafogli e altri rimedi

1. Gli Stati membri provvedono affinché non siano fornite, utilizzate o attivate unità di portafoglio nell'ambito della soluzione di portafoglio sospesa.

2. Gli Stati membri valutano se, per reagire adeguatamente alla violazione della sicurezza o alla compromissione, sia necessaria la revoca degli attestati di unità di portafoglio delle unità di portafoglio interessate dalla sospensione di una soluzione di portafoglio, o qualsiasi altro rimedio supplementare.

3. Le misure di cui ai paragrafi 1 e 2 sono adottate senza indebito ritardo e in ogni caso entro 24 ore dalla sospensione della fornitura e dell'uso della soluzione di portafoglio interessata dalla violazione della sicurezza o dalla compromissione.

4. Le misure di cui ai paragrafi 1 e 2 non impediscono agli utenti del portafoglio interessati di esercitare il diritto alla portabilità dei dati di cui all'articolo 5 *bis*, paragrafo 4, lettera g), del regolamento (UE) n. 910/2014. Ciò è subordinato alla condizione che gli utenti del portafoglio possano esercitare tale diritto senza pregiudicare la sicurezza delle risorse critiche delle unità di portafoglio interessate, in particolare tenendo conto dei motivi della sospensione e della necessità di garantire che tali risorse siano efficacemente protette da un uso improprio.

Articolo 5

Informazioni relative alle sospensioni e ai rimedi

1. Senza indebito ritardo, e in ogni caso entro 24 ore dalla sospensione della fornitura e dell'uso della soluzione di portafoglio, sono fornite informazioni chiare, complete e facilmente accessibili in merito alla sospensione della fornitura e dell'uso della soluzione di portafoglio:

a) ai punti di contatto unici designati a norma dell'articolo 46 *quater*, paragrafo 1, del regolamento (UE) n. 910/2014;

b) alla Commissione;

c) agli utenti del portafoglio interessati;

d) alle parti facenti affidamento sul portafoglio registrate conformemente all'articolo 5 *ter* del regolamento (UE) n. 910/2014.

2. Le informazioni fornite conformemente al paragrafo 1 comprendono almeno:

a) il nome del fornitore della soluzione di portafoglio la cui fornitura e il cui uso sono stati sospesi;

b) il nome e l'identificativo di riferimento di tale soluzione di portafoglio, come indicato nell'elenco dei portafogli certificati redatto a norma dell'articolo 5 *quinquies* del regolamento (UE) n. 910/2014 e, se del caso, le versioni interessate;

c) la data e l'ora in cui è stata rilevata la violazione della sicurezza o la compromissione;

d) se note, la data e l'ora in cui si è concretizzata la violazione della sicurezza o la compromissione, sulla base di registri di rete o di sistema o di altre fonti di dati;

e) la data e l'ora della sospensione della soluzione di portafoglio;

f) i dati di contatto, compresi almeno un indirizzo e-mail e un numero di telefono, dello Stato membro notificante e, se diversi, i dati di contatto del fornitore del portafoglio di cui alla lettera a);

g) una descrizione della violazione della sicurezza o della compromissione;

h) una descrizione dei dati compromessi, comprese, se del caso, le categorie di dati personali di cui all'articolo 9, paragrafo 1, e all'articolo 10 del regolamento (UE) 2016/679;

i) ove possibile, una stima del numero approssimativo di utenti del portafoglio interessati e di altre persone fisiche interessate;

j) una descrizione dei potenziali impatti sulle parti facenti affidamento sul portafoglio o sugli utenti del portafoglio e, in quest'ultimo caso, se opportuno, l'indicazione delle eventuali misure che gli utenti del portafoglio possono adottare per attenuare tali potenziali impatti;

k) una descrizione delle misure adottate o programmate per porre rimedio alla violazione della sicurezza o alla compromissione, unitamente alla programmazione e ai termini per l'applicazione di tali misure di rimedio;

l) laddove applicabile e opportuno, una descrizione delle misure adottate o programmate per il passaggio degli utenti del portafoglio interessati a soluzioni o servizi di portafoglio alternativi.

Articolo 6

Ripristino della fornitura e dell'uso dei portafogli

Ove necessario per garantire il ripristino della fornitura, dell'attivazione e dell'uso di una soluzione di portafoglio, gli Stati membri provvedono senza indebito ritardo:

1) a ripristinare la fornitura e l'uso delle unità di portafoglio fornite nell'ambito di tale soluzione di portafoglio rilasciando un'unità di portafoglio fornita nell'ambito di una nuova versione della soluzione di portafoglio a tutti gli utenti interessati;

2) a rilasciare nuovi attestati di unità di portafoglio a nuove unità di portafoglio o, se del caso, a unità di portafoglio precedentemente rilasciate, a condizione che tali unità di portafoglio soddisfino i requisiti di sicurezza in vigore dopo che è stato posto rimedio alla violazione della sicurezza o alla compromissione;

3) ad abrogare qualsiasi misura attuata a norma dell'articolo 4 che ostacoli la fornitura di nuove unità di portafoglio nell'ambito della soluzione di portafoglio interessata, qualora tale misura fosse collegata unicamente alla violazione della sicurezza o alla compromissione cui è stato posto rimedio.

Articolo 7

Informazioni sul ripristino

Quando ripristina una soluzione di portafoglio, lo Stato membro provvede affinché:

1) tutte le parti che sono state informate della sospensione della fornitura e dell'uso della soluzione di portafoglio conformemente all'articolo 5, paragrafo 1, siano informate del ripristino senza indebito ritardo;

2) le informazioni fornite a norma del punto 1 comprendano almeno gli elementi di cui all'articolo 5, paragrafo 2, lettere a), b) e da f) a h), e i seguenti elementi:

   a) la data e l'ora in cui è stato posto rimedio alla violazione della sicurezza o alla compromissione;

   b) la data e l'ora del ripristino della soluzione di portafoglio interessata e, se del caso, delle unità di portafoglio interessate fornite nell'ambito di tale soluzione di portafoglio;

   c) una descrizione delle misure adottate per porre rimedio alla violazione della sicurezza o alla compromissione;

   d) una descrizione dei potenziali impatti residui sulle parti facenti affidamento sul portafoglio o sugli utenti del portafoglio e, in quest'ultimo caso, se opportuno, l'indicazione delle eventuali misure che gli utenti del portafoglio possono adottare per attenuare tali potenziali impatti residui.

Articolo 8

Ritiro dei portafogli

1. Qualora non sia posto rimedio a una violazione della sicurezza o a una compromissione che ha portato alla sospensione della fornitura e dell'uso di una soluzione di portafoglio entro tre mesi dalla data di sospensione della fornitura e dell'uso di tale soluzione di portafoglio, lo Stato membro che la fornisce provvede affinché essa sia ritirata e ne sia revocata la validità, senza indebito ritardo e in ogni caso entro 72 ore dalla scadenza del periodo di tre mesi.

2. Quando ritira una soluzione di portafoglio, lo Stato membro provvede affinché:

a) gli attestati di unità di portafoglio dell'unità di portafoglio della soluzione di portafoglio interessata siano revocati;

b) gli attestati di unità di portafoglio non possano ritornare in stato di validità;

c) non sia possibile rilasciare un nuovo attestato di unità di portafoglio a unità di portafoglio esistenti fornite nell'ambito della soluzione di portafoglio interessata;

d) non sia possibile fornire una nuova unità di portafoglio nell'ambito della soluzione di portafoglio interessata.

3. Le misure di cui ai paragrafi 1 e 2 non impediscono agli utenti del portafoglio interessati di esercitare il diritto alla portabilità dei dati di cui all'articolo 5 *bis*, paragrafo 4, lettera g), del regolamento (UE) n. 910/2014. Ciò è subordinato alla condizione che gli utenti del portafoglio possano esercitare tale diritto senza pregiudicare la sicurezza delle risorse critiche delle unità di portafoglio interessate, in particolare tenendo conto dei motivi del ritiro e della necessità di garantire che tali risorse siano efficacemente protette da un uso improprio.

Articolo 9

Informazioni sul ritiro

1. Senza indebito ritardo, e in ogni caso entro 24 ore dal ritiro della soluzione di portafoglio, sono fornite informazioni chiare, complete e facilmente accessibili in merito al ritiro della soluzione di portafoglio:

a) ai punti di contatto unici designati a norma dell'articolo 46 *quater*, paragrafo 1, del regolamento (UE) n. 910/2014;

b) alla Commissione;

c) agli utenti del portafoglio interessati;

d) alle parti facenti affidamento sul portafoglio registrate a norma dell'articolo 5 *ter* del regolamento (UE) n. 910/2014.

2. Le informazioni fornite conformemente al paragrafo 1 comprendono almeno:

a) il nome del fornitore della soluzione di portafoglio che è stata ritirata;

b) il nome e l'identificativo di riferimento di tale soluzione di portafoglio, come indicato nell'elenco dei portafogli certificati redatto a norma dell'articolo 5 *quinquies* del regolamento (UE) n. 910/2014 e, se del caso, le versioni interessate;

c) la data e l'ora del rilevamento della violazione della sicurezza o della compromissione che ha portato al ritiro della soluzione di portafoglio interessata a causa della sua gravità o perché non vi è stato posto rimedio entro tre mesi;

d) se note, la data e l'ora in cui si è concretizzata la violazione della sicurezza o la compromissione, sulla base di registri di rete o di sistema o di altre fonti di dati;

e) la data e l'ora del ritiro della soluzione di portafoglio e della revoca effettiva degli attestati di unità di portafoglio delle unità di portafoglio fornite nell'ambito della soluzione di portafoglio;

f) un'indicazione che precisi se il ritiro è dovuto alla gravità della violazione della sicurezza o della compromissione o al fatto che non è stato posto rimedio alla violazione della sicurezza o alla compromissione;

g) i dati di contatto, compresi almeno un indirizzo e-mail e un numero di telefono, dello Stato membro notificante e, se diversi, i dati di contatto del fornitore del portafoglio di cui alla lettera a);

h) una descrizione della violazione della sicurezza o della compromissione;

i) una descrizione dei dati compromessi, comprese, se del caso, le categorie di dati personali di cui all'articolo 9, paragrafo 1, e all'articolo 10 del regolamento (UE) 2016/679;

j) ove possibile, una stima del numero approssimativo di utenti del portafoglio interessati e di altre persone fisiche interessate;

k) una descrizione dei potenziali impatti sulle parti facenti affidamento sul portafoglio o sugli utenti del portafoglio e, in quest'ultimo caso, se opportuno, l'indicazione delle eventuali misure che gli utenti del portafoglio possono adottare per attenuare tali potenziali impatti;

l) una descrizione delle misure adottate o programmate per il passaggio degli utenti del portafoglio interessati a soluzioni di portafoglio alternative o, laddove applicabile e opportuno, a servizi alternativi.

Articolo 10

Sistema di informazione

Gli Stati membri inviano le informazioni di cui agli articoli 3, 5, 7 e 9 alla Commissione e ai punti di contatto unici degli Stati membri designati a norma dell'articolo 46 *quater*, paragrafo 1, del regolamento (UE) n. 910/2014 tramite il sistema CIRAS gestito dall'ENISA o un sistema equivalente concordato dagli Stati membri e dalla Commissione.

Articolo 11

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, ad eccezione dell'articolo 10, che si applica a decorrere dal 7 maggio 2026.

Fatto a Bruxelles, il 6 maggio 2025

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO

Criteri per la valutazione di una violazione della sicurezza o di una compromissione

1. Gli Stati membri basano la loro valutazione di una violazione della sicurezza o di una compromissione sui criteri seguenti:

   a) la violazione o la compromissione ha causato o è in grado di causare il decesso di una persona fisica o danni considerevoli alla salute di quest'ultima;

   b) si è verificato o potrebbe verificarsi un accesso non autorizzato o che si sospetta essere malevolo ai sistemi informativi e di rete di un fornitore del portafoglio, di un fornitore dei meccanismi di convalida di cui all'articolo 5 *bis*, paragrafo 8, del regolamento (UE) n. 910/2014 o di un fornitore del regime di identificazione elettronica nell'ambito del quale è fornita una soluzione di portafoglio («soggetti interessati»), in grado di causare gravi perturbazioni operative, e detti sistemi sono componenti critici della soluzione di portafoglio interessata, dei meccanismi di convalida interessati di cui all'articolo 5 *bis*, paragrafo 8, del regolamento (UE) n. 910/2014 o del regime di identificazione elettronica interessato nell'ambito del quale è fornita una soluzione di portafoglio;

   c) una soluzione di portafoglio, un meccanismo di convalida di cui all'articolo 5 *bis*, paragrafo 8, del regolamento (UE) n. 910/2014, o un regime di identificazione elettronica nell'ambito del quale è fornita una soluzione di portafoglio, oppure una loro parte:

      — è completamente indisponibile o si prevede che sarà completamente indisponibile per gli utenti del portafoglio o per le parti facenti affidamento sul portafoglio per più di 12 ore consecutive;

      — è indisponibile o si prevede che sarà indisponibile per gli utenti del portafoglio o per le parti facenti affidamento sul portafoglio per più di 16 ore calcolate sulla base di una settimana di calendario;

   d) si sospetta che oltre l'1 % degli utenti del portafoglio o delle parti facenti affidamento sul portafoglio risenta, o dovrebbe risentire, della disponibilità limitata della soluzione di portafoglio o dei servizi forniti dai soggetti interessati per quanto riguarda la soluzione di portafoglio;

   e) vi è la possibilità che si verifichi, o si è verificata, una compromissione dell'accesso fisico limitato al personale di fiducia dei soggetti interessati, o della protezione di tale accesso fisico, a uno o più luoghi in cui sono ubicati sistemi informativi e di rete a sostegno della soluzione di portafoglio, della fornitura dei meccanismi di convalida di cui all'articolo 5 *bis*, paragrafo 8, del regolamento (UE) n. 910/2014 associati a una soluzione di portafoglio o del regime di identificazione elettronica nell'ambito del quale è fornita una soluzione di portafoglio;

   f) una compromissione dell'integrità, della riservatezza, anche sotto il profilo della tutela della vita privata, o dell'autenticità dei dati conservati, trasmessi o elaborati nell'ambito della soluzione di portafoglio si configura, o può configurarsi, in uno o più dei modi seguenti:

      — ha un impatto su oltre l'1 % degli utenti del portafoglio della soluzione di portafoglio interessata o su oltre 100 000 di tali utenti del portafoglio, a seconda di quale valore sia inferiore;

      — deriva dal verificarsi di un'attività che si sospetta essere malevola;

      — deriva o potrebbe derivare da una o più vulnerabilità note, comprese quelle trattate conformemente al regolamento di esecuzione (UE) 2024/2981 della Commissione ([1]);

      — è probabile che incida sui dati personali in modo tale da poter comportare un rischio per i diritti e le libertà delle persone fisiche interessate, in particolare in caso di violazione dei dati personali di cui all'articolo 9, paragrafo 1, e all'articolo 10 del regolamento (UE) 2016/679;

([1]) Regolamento di esecuzione (UE) 2024/2981 della Commissione, del 28 novembre 2024, recante modalità di applicazione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio per quanto riguarda la certificazione dei portafogli europei di identità digitale (GU L, 2024/2981, 4.12.2024, ELI: http://data.europa.eu/eli/reg_impl/2024/2981/oj).

— è probabile che incida sulle comunicazioni elettroniche personali;

— è probabile che presenti un rischio elevato per i diritti e le libertà delle persone fisiche;

— è probabile che abbia ripercussioni sulle persone fisiche vulnerabili;

g) la certificazione della soluzione di portafoglio è stata annullata o si prevede che sarà annullata;

h) la violazione o la compromissione ha causato o è in grado di causare a un soggetto interessato una perdita finanziaria diretta superiore a 500 000 EUR o, se del caso, se tale importo è inferiore, al 5 % del suo fatturato totale annuo dell'esercizio precedente.

2. Gli Stati membri non prendono in considerazione le conseguenze previste di un'operazione di manutenzione effettuata dai soggetti interessati o per loro conto, a condizione che tale operazione:

a) sia stata notificata in anticipo agli utenti del portafoglio potenzialmente interessati, alle parti facenti affidamento sul portafoglio e ai pertinenti organismi di vigilanza competenti;

b) non risponda ad alcuno dei criteri di cui al punto 1 del presente allegato.

3. Per quanto riguarda il punto 1, lettera c), la durata di un incidente che incide sulla disponibilità è misurata a partire dal momento in cui avviene la perturbazione della corretta fornitura del servizio interessato fino al momento in cui il servizio è ripristinato e torna operativo. Qualora un soggetto interessato non sia in grado di determinare il momento in cui ha avuto inizio la perturbazione, la durata dell'incidente è misurata a partire dal momento in cui l'incidente è stato rilevato o dal momento in cui l'incidente è stato registrato nei registri di rete o di sistema o in altre fonti di dati, a seconda dell'evento che si verifica per primo. L'indisponibilità totale di un servizio è misurata dal momento in cui il servizio è completamente indisponibile per gli utenti fino al momento in cui le attività o le operazioni regolari sono state ripristinate al livello del servizio fornito prima dell'incidente. Se un soggetto interessato non è in grado di stabilire quando è iniziata la completa indisponibilità di un servizio, l'indisponibilità è misurata dal momento in cui è stata rilevata da tale soggetto.

4. Per quanto riguarda il punto 1, lettera d), si ritiene che la disponibilità di un servizio sia limitata in particolare quando esso è notevolmente più lento rispetto al tempo di risposta medio o quando non sono disponibili tutte le relative funzionalità. Ove possibile, per valutare i ritardi nei tempi di risposta sono utilizzati criteri oggettivi basati sui tempi di risposta medi dei servizi.

5. Ai fini della determinazione delle perdite finanziarie dirette derivanti da una violazione o da una compromissione di cui al punto 1, lettera h), i soggetti interessati tengono conto di tutte le perdite finanziarie da essi subite a seguito dell'incidente, quali i costi per la sostituzione o il trasferimento di software, hardware o infrastrutture, i costi del personale, compresi i costi associati alla sostituzione o al trasferimento del personale, all'assunzione di personale supplementare, alla remunerazione di straordinari e al recupero di competenze perdute o compromesse, le spese dovute all'inosservanza degli obblighi contrattuali, i costi per risarcimenti e indennizzi ai clienti, le perdite dovute a mancate entrate, i costi associati alla comunicazione interna ed esterna e i costi di consulenza, compresi quelli relativi alla consulenza legale, ai servizi forensi e ai servizi per rimediare all'incidente. I costi necessari per il funzionamento quotidiano dell'attività, quali i costi per la manutenzione generale di infrastrutture, attrezzature, hardware e software, i miglioramenti e le iniziative di valutazione dei rischi e i premi assicurativi non sono considerati perdite finanziarie derivanti da un incidente. I soggetti interessati calcolano gli importi delle perdite finanziarie sulla base dei dati disponibili e, laddove non sia possibile determinare gli importi effettivi, ne effettuano la stima.