►B 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

(GU L 257 del 28.8.2014, pag. 73)

Modificato da:

		Gazzetta ufficiale		
		n.	pag.	data
►M1	Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio del 14 dicembre 2022	L 333	80	27.12.2022
►M2	Regolamento (UE) 2024/1183 del Parlamento europeo e del Consiglio dell'11 aprile 2024	L 1183	1	30.4.2024

Rettificato da:

►C1 Rettifica, GU L 272 del 7.10.2016, pag. 96 (910/2014)

►C2 Rettifica, GU L 90317 del 9.4.2025, pag. 1 (2024/1183)

▼B

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

CAPO I

DISPOSIZIONI GENERALI

▼M2

Articolo 1

Oggetto

Il presente regolamento mira a garantire il buon funzionamento del mercato interno e a fornire un adeguato livello di sicurezza dei mezzi di identificazione elettronica e dei servizi fiduciari utilizzati in tutta l'Unione, al fine di consentire e facilitare l'esercizio, da parte delle persone fisiche e giuridiche, del diritto di partecipare in modo sicuro alla società digitale e di accedere ai servizi pubblici e privati online in tutta l'Unione. A tal fine, il presente regolamento:

a) fissa le condizioni alle quali gli Stati membri riconoscono i mezzi di identificazione elettronica delle persone fisiche e giuridiche, che rientrano in un regime notificato di identificazione elettronica di un altro Stato membro e forniscono e riconoscono i portafogli europei di identità digitale;

b) stabilisce le norme relative ai servizi fiduciari, in particolare per le transazioni elettroniche;

c) istituisce un quadro giuridico per le firme elettroniche, i sigilli elettronici, le validazioni temporali elettroniche, i documenti elettronici, i servizi elettronici di recapito certificato, i servizi relativi ai certificati di autenticazione di siti web, l'archiviazione elettronica, gli attestati elettronici di attributi, i dispositivi per la creazione di una firma elettronica, i dispositivi per la creazione di sigilli elettronici e i registri elettronici.

▼B

Articolo 2

Ambito di applicazione

▼M2

1. Il presente regolamento si applica ai regimi di identificazione elettronica notificati da uno Stato membro, ai portafogli europei di identità digitale forniti da uno Stato membro e ai prestatori di servizi fiduciari stabiliti nell'Unione.

▼B

2. Il presente regolamento non si applica alla prestazione di servizi fiduciari che sono utilizzati esclusivamente nell'ambito di sistemi chiusi contemplati dal diritto nazionale o da accordi conclusi tra un insieme definito di partecipanti.

▼M2

3. Il presente regolamento non pregiudica il diritto nazionale o dell'Unione legato alla conclusione e alla validità di contratti, altri vincoli giuridici o procedurali relativi alla forma, o requisiti settoriali relativi alla forma.

▼M2

4. Il presente regolamento non pregiudica il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([1]).

▼B

Articolo 3

Definizioni

Ai fini del presente regolamento si intende per:

▼M2

1) «identificazione elettronica», il processo per cui si fa uso di dati di identificazione personale in forma elettronica che rappresentano un'unica persona fisica o giuridica, o un'unica persona fisica che rappresenta un'altra persona fisica o una persona giuridica;

2) «mezzi di identificazione elettronica», un'unità materiale e/o immateriale contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online o, se del caso, per un servizio offline;

3) «dati di identificazione personale», un insieme di dati che è rilasciato conformemente al diritto dell'Unione o nazionale e che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta un'altra persona fisica o una persona giuridica;

4) «regime di identificazione elettronica», un sistema di identificazione elettronica per mezzo del quale si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano altre persone fisiche o persone giuridiche;

5) «autenticazione», un processo elettronico che consente di confermare l'identificazione elettronica di una persona fisica o giuridica, oppure di confermare l'origine e l'integrità di dati in forma elettronica;

5 *bis*) «utente», una persona fisica o giuridica, o una persona fisica che rappresenta un'altra persona fisica o una persona giuridica, che utilizza servizi fiduciari o mezzi di identificazione elettronica, forniti a norma del presente regolamento;

6) «parte facente affidamento sulla certificazione», una persona fisica o giuridica che fa affidamento sull'identificazione elettronica, sui portafogli europei di identità digitale o su altri mezzi di identificazione elettronica, oppure su un servizio fiduciario;

▼B

7) «organismo del settore pubblico», un'autorità statale, regionale o locale, un organismo di diritto pubblico o un'associazione formata da una o più di tali autorità o da uno o più di tali organismi di diritto pubblico, oppure un soggetto privato incaricato da almeno un'autorità, un organismo o un'associazione di cui sopra di fornire servizi pubblici, quando agisce in base a tale mandato;

([1]) 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).

▼B

8) «organismo di diritto pubblico», un organismo definito all'articolo 2, paragrafo 1, punto 4, della direttiva 2014/24/UE del Parlamento europeo e del Consiglio ([1]);

9) «firmatario», una persona fisica che crea una firma elettronica;

10) «firma elettronica», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati elettronici e utilizzati dal firmatario per firmare;

11) «firma elettronica avanzata», una firma elettronica che soddisfi i requisiti di cui all'articolo 26;

12) «firma elettronica qualificata», una firma elettronica avanzata creata da un dispositivo per la creazione di una firma elettronica qualificata e basata su un certificato qualificato per firme elettroniche;

13) «dati per la creazione di una firma elettronica», i dati unici utilizzati dal firmatario per creare una firma elettronica;

14) «certificato di firma elettronica», un attestato elettronico che collega i dati di convalida di una firma elettronica a una persona fisica e conferma almeno il nome o lo pseudonimo di tale persona;

15) «certificato qualificato di firma elettronica», un certificato di firma elettronica che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato I;

▼M2

16) «servizio fiduciario», un servizio elettronico prestato normalmente dietro remunerazione e consistente in uno qualsiasi degli elementi seguenti:

   a) il rilascio di certificati di firma elettronica, certificati di sigilli elettronici, certificati di autenticazione di siti web o certificati di prestazione di altri servizi fiduciari;

   b) la convalida di certificati di firma elettronica, certificati di sigilli elettronici, certificati di autenticazione di siti web o certificati di prestazione di altri servizi fiduciari;

   c) la creazione di firme elettroniche o sigilli elettronici;

   d) la convalida di firme elettroniche o sigilli elettronici;

   e) la conservazione di firme elettroniche, sigilli elettronici, certificati di firme elettroniche o certificati di sigilli elettronici;

   f) la gestione di dispositivi per la creazione di una firma elettronica a distanza o di dispositivi per la creazione di un sigillo elettronico a distanza;

   g) il rilascio di attestati elettronici di attributi;

   h) la convalida di attestati elettronici di attributi;

([1]) Direttiva 2014/24/UE del Parlamento europeo e del Consiglio, del 26 febbraio 2014, sugli appalti pubblici e che abroga la direttiva 2004/18/CE (GU L 94 del 28.3.2014, pag. 65).

▼M2

i) la creazione di validazioni temporali elettroniche;

j) la convalida di validazioni temporali elettroniche;

k) la prestazione di servizi elettronici di recapito certificato;

l) la convalida dei dati trasmessi tramite servizi elettronici di recapito certificato e relative prove;

m) l'archiviazione elettronica di dati elettronici e di documenti elettronici;

n) la registrazione di dati elettronici in un registro elettronico;

▼B

17) «servizio fiduciario qualificato», un servizio fiduciario che soddisfa i requisiti pertinenti stabiliti nel presente regolamento;

▼M2

18) «organismo di valutazione della conformità», un organismo di valutazione della conformità ai sensi dell'articolo 2, punto 13, del regolamento (CE) n. 765/2008, che è accreditato a norma di tale regolamento come competente a effettuare la valutazione della conformità del prestatore di servizi fiduciari qualificato e dei servizi fiduciari qualificati da esso prestati o come competente a effettuare la certificazione dei portafogli europei di identità digitale o dei mezzi di identificazione elettronica;

▼B

19) «prestatore di servizi fiduciari», una persona fisica o giuridica che presta uno o più servizi fiduciari, o come prestatore di servizi fiduciari qualificato o come prestatore di servizi fiduciari non qualificato;

20) «prestatore di servizi fiduciari qualificato», un prestatore di servizi fiduciari che presta uno o più servizi fiduciari qualificati e cui l'organismo di vigilanza assegna la qualifica di prestatore di servizi fiduciari qualificato;

▼M2

21) «prodotto», un hardware o software o i pertinenti componenti di hardware o software destinati a essere utilizzati per la prestazione di servizi di identificazione elettronica e servizi fiduciari;

▼B

22) «dispositivo per la creazione di una firma elettronica», un software o hardware configurato utilizzato per creare una firma elettronica;

23) «dispositivo per la creazione di una firma elettronica qualificata», un dispositivo per la creazione di una firma elettronica che soddisfa i requisiti di cui all'allegato II;

▼M2

23 *bis*) «dispositivo qualificato per la creazione di una firma elettronica a distanza», un dispositivo qualificato per la creazione di una firma elettronica, che è gestito da un prestatore di servizi fiduciari qualificato conformemente all'articolo 29 bis per conto di un firmatario;

▼M2

23 *ter*) «dispositivo qualificato per la creazione di un sigillo elettronico a distanza», un dispositivo qualificato per la creazione di un sigillo elettronico, che è gestito da un prestatore di servizi fiduciari qualificato conformemente all'articolo 39 bis per conto di un creatore di un sigillo;

▼B

24) «creatore di un sigillo», una persona giuridica che crea un sigillo elettronico;

25) «sigillo elettronico», dati in forma elettronica, acclusi oppure connessi tramite associazione logica ad altri dati in forma elettronica per garantire l'origine e l'integrità di questi ultimi;

26) «sigillo elettronico avanzato», un sigillo elettronico che soddisfi i requisiti sanciti all'articolo 36;

27) «sigillo elettronico qualificato», un sigillo elettronico avanzato creato da un dispositivo per la creazione di un sigillo elettronico qualificato e basato su un certificato qualificato per sigilli elettronici;

28) «dati per la creazione di un sigillo elettronico», i dati unici utilizzati dal creatore del sigillo elettronico per creare un sigillo elettronico;

29) «certificato di sigillo elettronico», un attestato elettronico che collega i dati di convalida di un sigillo elettronico a una persona giuridica e conferma il nome di tale persona;

30) «certificato qualificato di sigillo elettronico», un certificato di sigillo elettronico che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato III;

31) «dispositivo per la creazione di un sigillo elettronico», un software o hardware configurato utilizzato per creare un sigillo elettronico;

32) «dispositivo per la creazione di un sigillo elettronico qualificato», un dispositivo per la creazione di un sigillo elettronico che soddisfa mutatis mutandis i requisiti di cui all'allegato II;

33) «validazione temporale elettronica», dati in forma elettronica che collegano altri dati in forma elettronica a una particolare ora e data, così da provare che questi ultimi esistevano in quel momento;

34) «validazione temporale elettronica qualificata», una validazione temporale elettronica che soddisfa i requisiti di cui all'articolo 42;

35) «documento elettronico», qualsiasi contenuto conservato in forma elettronica, in particolare testo o registrazione sonora, visiva o audiovisiva;

36) «servizio elettronico di recapito certificato», un servizio che consente la trasmissione di dati fra terzi per via elettronica e fornisce prove relative al trattamento dei dati trasmessi, fra cui prove dell'avvenuto invio e dell'avvenuta ricezione dei dati, e protegge i dati trasmessi dal rischio di perdita, furto, danni o di modifiche non autorizzate;

▼C1

37) «servizio elettronico di recapito certificato qualificato», un servizio elettronico di recapito certificato che soddisfa i requisiti di cui all'articolo 44;

▼M2

38) «certificato di autenticazione di sito web», un attestato elettronico che consente di autenticare un sito web e collega il sito alla persona fisica o giuridica a cui il certificato è rilasciato;

▼B

39) «certificato qualificato di autenticazione di sito web», un certificato di autenticazione di sito web che è rilasciato da un prestatore di servizi fiduciari qualificato ed è conforme ai requisiti di cui all'allegato IV;

40) «dati di convalida», dati utilizzati per convalidare una firma elettronica o un sigillo elettronico;

▼M2

41) «convalida», il processo di verifica e conferma della validità dei dati in forma elettronica conformemente al presente regolamento;

42) «Portafoglio europeo di identità digitale», un mezzo di identificazione elettronica che consente all'utente di conservare, gestire e convalidare in modo sicuro dati di identità personale e attestati elettronici di attributi al fine di fornirli alle parti facenti affidamento sulla certificazione e agli altri utenti dei portafogli europei di identità digitale, e di firmare mediante firme elettroniche qualificate o apporre sigilli mediante sigilli elettronici qualificati;

43) «attributo», la caratteristica, la qualità, il diritto o l'autorizzazione di una persona fisica o giuridica o di un oggetto;

44) «attestato elettronico di attributi», un attestato in forma elettronica che consente l'autenticazione di attributi;

45) «attestato elettronico di attributi qualificato», un attestato elettronico di attributi che è rilasciato da un prestatore di servizi fiduciari qualificato e soddisfa i requisiti di cui all'allegato V;

46) «attestato elettronico di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto», un attestato elettronico di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o da un organismo del settore pubblico designato dallo Stato membro per rilasciare tali attestati di attributi per conto di organismi del settore pubblico responsabili di fonti autentiche in conformità dell'articolo 45 septies e che soddisfa i requisiti di cui all'allegato VII;

47) «fonte autentica», un archivio o un sistema, tenuto sotto la responsabilità di un organismo del settore pubblico o di un soggetto privato, che contiene e fornisce gli attributi relativi a una persona fisica o giuridica o a un oggetto e che è considerato una fonte primaria di tali informazioni o la cui autenticità è riconosciuta conformemente al diritto dell'Unione o nazionale, inclusa la prassi amministrativa;

▼M2

48) «archiviazione elettronica», 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;

49) «servizio di archiviazione elettronica qualificato», un servizio di archiviazione elettronica fornito da un prestatore di servizi fiduciari qualificato e che soddisfa i requisiti di cui all'articolo 45 undecies;

50) «marchio di fiducia UE per i portafogli di identità digitale», un'indicazione verificabile, semplice e riconoscibile, comunicata in modo chiaro, del fatto che un portafoglio europeo di identità digitale è stato fornito conformemente al presente regolamento;

51) «autenticazione forte dell'utente», un'autenticazione basata sull'uso di almeno due fattori di autenticazione appartenenti a diverse categorie, della conoscenza qualcosa che solo l'utente conosce, del possesso, qualcosa che solo l'utente possiede, o dell'inerenza, qualcosa che caratterizza l'utente, che sono indipendenti, in modo tale che la violazione di uno degli elementi non comprometta l'affidabilità degli altri, e progettata in maniera tale da proteggere la riservatezza dei dati di autenticazione;

52) «registro elettronico», una sequenza di registrazioni di dati elettronici che garantisce l'integrità di tali registrazioni e l'accuratezza dell'ordine cronologico di tali registrazioni;

53) «registro elettronico qualificato», un registro elettronico fornito da un prestatore di servizi fiduciari qualificato e che soddisfa i requisiti di cui all'articolo 45 terdecies;

54) «dati personali», qualsiasi informazione quale definita all'articolo 4, punto 1, del regolamento (UE) 2016/679;

55) «corrispondenza dell'identità», un processo in cui i dati di identificazione personale o i mezzi di identificazione elettronica sono abbinati o collegati a un account esistente appartenente alla stessa persona;

56) «registrazione di dati», dati elettronici registrati con i metadati connessi che supportano il trattamento dei dati;

57) «modalità offline», per quanto riguarda l'uso dei portafogli europei di identità digitale, un'interazione tra un utente e un terzo in un luogo fisico per mezzo di tecnologie di prossimità, laddove il portafoglio europeo di identità digitale non è tenuto ad accedere a sistemi a distanza tramite reti di comunicazione elettronica ai fini dell'interazione.

▼B

Articolo 4

Principio del mercato interno

1. Non sono imposte restrizioni alla prestazione di servizi fiduciari nel territorio di uno Stato membro da parte di un prestatore di servizi fiduciari stabilito in un altro Stato membro per motivi che rientrano negli ambiti di applicazione del presente regolamento.

▼B

2. I prodotti e i servizi fiduciari conformi al presente regolamento godono della libera circolazione nel mercato interno.

▼M2

Articolo 5

Pseudonimi nelle transazioni elettroniche

Fatti salvi le norme specifiche del diritto dell'Unione o nazionale che impongono agli utenti di identificarsi o gli effetti giuridici che il diritto nazionale attribuisce agli pseudonimi, l'uso di pseudonimi scelti dall'utente non è vietato.

▼B

CAPO II

IDENTIFICAZIONE ELETTRONICA

▼M2

SEZIONE 1

Portafoglio europeo di identità digitale

Articolo 5 bis

Portafogli europei di identità digitale

1. Al fine di garantire che tutte le persone fisiche e giuridiche nell'Unione abbiano un accesso transfrontaliero sicuro, affidabile e senza soluzione di continuità a servizi pubblici e privati, mantenendo nel contempo il pieno controllo dei loro dati, ciascuno Stato membro fornisce almeno un portafoglio europeo di identità digitale entro 24 mesi dalla data di entrata in vigore degli atti di esecuzione di cui al paragrafo 23 del presente articolo e all'articolo 5 quater, paragrafo 6.

2. I portafogli europei di identità digitale sono forniti in almeno uno dei modi seguenti:

a) direttamente da uno Stato membro;

b) su incarico di uno Stato membro;

c) indipendentemente da uno Stato membro pur essendo riconosciuti da quest'ultimo.

3. Il codice sorgente dei componenti software dell'applicazione dei portafogli europei di identità digitale è caratterizzato da una licenza open source. Gli Stati membri possono prevedere che, per motivi debitamente giustificati, il codice sorgente di componenti specifici diversi da quelli installati sui dispositivi degli utenti non sia divulgato.

4. I portafogli europei di identità digitale consentono all'utente, in modo intuitivo, trasparente e tracciabile da quest'ultimo, di:

a) richiedere, ottenere, selezionare, combinare, conservare, cancellare, condividere e presentare in modo sicuro, con il controllo esclusivo dell'utente, dati di identificazione personale e, se del caso, in combinazione con attestati elettronici di attributi, necessari per l'autenticazione delle parti facenti affidamento sulla certificazione online e, se del caso, in modalità offline, al fine di accedere ai servizi pubblici e privati, garantendo nel contempo che sia possibile la divulgazione selettiva dei dati;

▼M2

b) generare pseudonimi e conservarli in modo cifrato e locale all'interno del portafoglio europeo di identità digitale;

c) autenticare in modo sicuro il portafoglio europeo di identità digitale di un'altra persona e ricevere e condividere dati di identificazione personale e attestati elettronici di attributi in modo sicuro tra i due portafogli europei di identità digitale;

d) accedere a un registro di tutte le transazioni effettuate mediante il portafoglio europeo di identità digitale attraverso un pannello di gestione comune che consente all'utente di:

i) visualizzare un elenco aggiornato delle parti facenti affidamento sulla certificazione con le quali l'utente ha stabilito una connessione e, se del caso, tutti i dati scambiati;

ii) chiedere facilmente che una parte facente affidamento sulla certificazione cancelli i dati personali a norma dell'articolo 17 del regolamento (UE) 2016/679;

iii) segnalare facilmente la parte facente affidamento sulla certificazione all'autorità nazionale di protezione dei dati competente qualora sia ricevuta una richiesta di dati personali presumibilmente illecita o sospetta;

e) firmare mediante firme elettroniche qualificate o apporre sigilli mediante sigilli elettronici qualificati;

f) scaricare, nella misura in cui ciò sia tecnicamente possibile, i dati dell'utente, gli attestati elettronici di attributi e le configurazioni;

g) esercitare il diritto dell'utente alla portabilità dei dati.

5. In particolare, i portafogli europei di identità digitale:

a) sostengono protocolli e interfacce comuni:

i) per il rilascio di dati di identificazione personale, attestati elettronici qualificati e non qualificati di attributi o certificati qualificati e non qualificati al portafoglio europeo di identità digitale;

ii) per le parti facenti affidamento sulla certificazione ai fini della richiesta e della convalida dei dati di identificazione personale e degli attestati elettronici di attributi;

iii) per la condivisione e la presentazione alle parti facenti affidamento sulla certificazione di dati di identificazione personale, attestati elettronici di attributi o dati correlati divulgati selettivamente online e, se del caso, in modalità offline;

iv) affinché l'utente possa consentire l'interazione con il portafoglio europeo di identità digitale e visualizzare un marchio di fiducia UE per i portafogli di identità digitale;

v) per garantire in modo sicuro l'onboarding dell'utente utilizzando mezzi di identificazione elettronica a norma dell'articolo 5 bis, paragrafo 24;

vi) per l'interazione tra i portafogli europei di identità digitale di due persone, al fine di ricevere, convalidare e condividere dati di identificazione personale e attestati elettronici di attributi in modo sicuro;

▼M2

vii) per l'autenticazione e l'identificazione delle parti facenti affidamento sulla certificazione mediante l'attuazione di meccanismi di autenticazione a norma dell'articolo 5 ter;

viii) affinché le parti facenti affidamento sulla certificazione verifichino l'autenticità e la validità dei portafogli europei di identità digitale;

ix) per chiedere a una parte facente affidamento sulla certificazione la cancellazione dei dati personali a norma dell'articolo 17 del regolamento (UE) 2016/679;

x) per segnalare una parte facente affidamento sulla certificazione all'autorità nazionale di protezione dei dati competente in caso di ricezione di una richiesta di dati presumibilmente illecita o sospetta;

xi) per la creazione, mediante dispositivi per la creazione di firme elettroniche qualificate o sigilli elettronici qualificati, di sigilli elettronici qualificati o firme elettroniche qualificate;

b) non forniscono ai prestatori di servizi fiduciari che forniscono attestati elettronici di attributi alcuna informazione sull'uso di tali attestati elettronici;

c) garantiscono che l'identità delle parti facenti affidamento sulla certificazione possa essere autenticata e identificata mediante l'attuazione di meccanismi di autenticazione a norma dell'articolo 5 ter;

d) soddisfano i requisiti di cui all'articolo 8 per quanto riguarda il livello di garanzia elevato, in particolare in relazione ai requisiti per il controllo e la verifica dell'identità e alla gestione e autenticazione dei mezzi di identificazione elettronica;

e) nel caso di attestato elettronico di attributi con politiche di divulgazione incorporate, attuano il meccanismo appropriato per informare l'utente che la parte facente affidamento sulla certificazione o l'utente del portafoglio europeo di identità digitale che richiede tale attestato elettronico di attributi ha il permesso di accedervi;

f) garantiscono che i dati di identificazione personale, disponibili dal regime di identificazione elettronica nell'ambito del quale è fornito il portafoglio europeo di identità digitale, rappresentino in modo univoco la persona fisica, la persona giuridica o la persona fisica che le rappresenta e siano associati a tale portafoglio europeo di identità digitale;

g) offrono a tutte le persone fisiche la possibilità di firmare mediante firme elettroniche qualificate per impostazione predefinita e gratuitamente.

Fatto salvo il primo comma, lettera g), gli Stati membri possono prevedere misure proporzionate per garantire che l'uso gratuito di firme elettroniche qualificate da parte di persone fisiche sia limitato a scopi non professionali.

6. Gli Stati membri informano gli utenti, senza indebito ritardo, di eventuali violazioni della sicurezza che potrebbero aver compromesso in tutto o in parte il loro portafoglio europeo di identità digitale o i relativi contenuti e, in particolare, se il loro portafoglio europei di identità digitale è stato sospeso o revocato a norma dell'articolo 5 sexies.

▼M2

7. Fatto salvo l'articolo 5 septies, gli Stati membri possono prevedere, conformemente al diritto nazionale, funzionalità aggiuntive dei portafogli europei di identità digitale, compresa l'interoperabilità con i mezzi nazionali di identificazione elettronica esistenti. Tali funzionalità aggiuntive sono conformi al presente articolo.

8. Gli Stati membri prevedono meccanismi di convalida gratuiti per:

a) garantire che sia possibile verificare l'autenticità e la validità dei portafogli europei di identità digitale;

b) consentire agli utenti di verificare l'autenticità e la validità dell'identità delle parti facenti affidamento sulla certificazione registrate a norma dell'articolo 5 ter.

9. Gli Stati membri provvedono affinché la validità del portafoglio europeo di identità digitale possa essere revocata nelle circostanze seguenti:

a) su esplicita richiesta dell'utente;

b) qualora la sicurezza del portafoglio europeo di identità digitale sia stata compromessa;

c) alla morte dell'utente o alla cessazione dell'attività della persona giuridica.

10. I fornitori dei portafogli europei di identità digitale garantiscono che gli utenti possano facilmente richiedere assistenza tecnica e segnalare problemi tecnici o qualsiasi altro incidente che abbia un impatto negativo sull'uso del portafoglio europeo di identità digitale.

11. I portafogli europei di identità digitale sono forniti nell'ambito di un regime di identificazione elettronica il cui livello di garanzia è elevato.

12. I portafogli europei di identità digitale garantiscono la sicurezza fin dalla progettazione.

13. I portafogli europei di identità digitale sono emessi, utilizzati e revocati gratuitamente a tutte le persone fisiche.

14. Gli utenti hanno il pieno controllo dell'uso del loro portafoglio europeo di identità digitale e dei dati in esso contenuti. Il fornitore del portafoglio europeo di identità digitale non raccoglie informazioni relative all'uso del portafoglio europeo di identità digitale che non sono necessarie per la prestazione dei servizi del portafoglio europeo di identità digitale, né combina i dati di identificazione personale o gli altri dati personali conservati nel portafoglio europeo di identità digitale o relativi al suo uso con i dati personali provenienti da altri servizi offerti da tale fornitore o da servizi di terzi che non sono necessari per la prestazione dei servizi del portafoglio europeo di identità digitale, a meno che l'utente non l'abbia richiesto espressamente. I dati personali relativi alla fornitura del portafoglio europeo di identità digitale sono tenuti logicamente separati dagli altri dati detenuti dal fornitore del portafoglio europeo di identità digitale. Se il portafoglio europeo di identità digitale è fornito da soggetti privati conformemente al paragrafo 2, lettere b) e c), del presente articolo, si applicano, *mutatis mutandis*, le disposizioni di cui all'articolo 45 nonies, paragrafo 3.

▼M2

15. L'uso dei portafogli europei di identità digitale è facoltativo. L'accesso ai servizi pubblici e privati e al mercato del lavoro nonché la libertà d'impresa non sono in alcun modo limitati o resi svantaggiosi per le persone fisiche o giuridiche che non utilizzano i portafogli europei di identità digitale. Resta possibile accedere ai servizi pubblici e privati con altri mezzi di identificazione e autenticazione esistenti.

16. Il quadro tecnico del portafoglio europeo di identità digitale:

a) non consente ai fornitori di attestati elettronici di attributi o a qualsiasi altra parte, dopo il rilascio dell'attestato di attributi, di ottenere dati che consentano di tracciare, collegare o correlare le transazioni o il comportamento dell'utente o di venirne in altro modo a conoscenza, salvo esplicita autorizzazione dell'utente;

b) rende possibili tecniche di tutela della vita privata che impediscono i collegamenti, laddove l'attestato di attributi non richieda l'identificazione dell'utente.

17. Il trattamento di dati personali effettuato dagli Stati membri o per loro conto da organismi o parti responsabili della fornitura dei portafogli europei di identità digitale come mezzo di identificazione elettronica è effettuato nel rispetto di misure di protezione dei dati adeguate ed efficaci. Si deve dimostrare la conformità al regolamento (UE) 2016/679 di tale trattamento. Gli Stati membri possono introdurre disposizioni nazionali per specificare ulteriormente l'applicazione di tali misure.

18. Gli Stati membri notificano alla Commissione, senza indebito ritardo, informazioni riguardanti:

a) l'organismo responsabile dell'elaborazione e del mantenimento dell'elenco delle parti facenti affidamento sulla certificazione registrate che si avvalgono dei portafogli europei di identità digitale a norma dell'articolo 5 ter, paragrafo 5, e l'ubicazione di tale elenco;

b) gli organismi responsabili della fornitura dei portafogli europei di identità digitale a norma dell'articolo 5 bis, paragrafo 1;

c) gli organismi responsabili di garantire che i dati di identificazione personale siano associati al portafoglio europeo di identità digitale a norma dell'articolo 5 bis, paragrafo 5, lettera f);

d) il meccanismo che consente la convalida dei dati di identificazione personale di cui all'articolo 5 bis, paragrafo 5, lettera f), e dell'identità delle parti facenti affidamento sulla certificazione;

e) il meccanismo di convalida dell'autenticità e della validità dei portafogli europei di identità digitale.

La Commissione mette a disposizione del pubblico le informazioni notificate a norma del presente comma attraverso un canale sicuro, in forma firmata o sigillata elettronicamente e adatta al trattamento automatizzato.

▼M2

19. Fatto salvo il paragrafo 22 del presente articolo, l'articolo 11 si applica, *mutatis mutandis*, al portafoglio europeo di identità digitale.

20. L'articolo 24, paragrafo 2, lettera b) e lettere da d) a h), si applica, *mutatis mutandis*, ai fornitori dei portafogli europei di identità digitale.

21. I portafogli europei di identità digitale sono resi accessibili per l'uso da parte delle persone con disabilità, in condizioni di parità con gli altri utenti, conformemente alla direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio ([1]).

22. Ai fini della fornitura dei portafogli europei di identità digitale, i portafogli europei di identità digitale e i regimi di identificazione elettronica nell'ambito dei quali sono forniti non sono soggetti ai requisiti di cui agli articoli 7, 9, 10, 12 e 12 bis.

23. Entro il 21 novembre 2024 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai requisiti di cui ai paragrafi 4, 5, 8 e 18 del presente articolo relativamente all'attuazione del portafoglio europeo di identità digitale. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

24. La Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, 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 elevato o 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. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 5 ter

Parti facenti affidamento sulla certificazione dei portafogli europei di identità digitale

1. Qualora intenda avvalersi dei portafogli europei di identità digitale per la fornitura di servizi pubblici o privati mediante interazione digitale, la parte facente affidamento sulla certificazione si registra nello Stato membro in cui è stabilita .

2. La procedura di registrazione è efficace sotto il profilo dei costi e proporzionata al rischio. La parte facente affidamento sulla certificazione fornisce almeno:

a) le informazioni necessarie per autenticarsi nei portafogli europei di identità digitale, che comprendono almeno:

   i) lo Stato membro in cui la parte facente affidamento sulla certificazione è stabilita; e

([1]) Direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio, del 17 aprile 2019, sui requisiti di accessibilità dei prodotti e dei servizi (GU L 151 del 7.6.2019, pag. 70).

▼M2

ii) il nome della parte facente affidamento sulla certificazione e, se del caso, il suo numero di registrazione quale appare in un documento ufficiale, unitamente ai dati di identificazione di tale documento ufficiale;

b) i dati di contatto della parte facente affidamento sulla certificazione;

c) l'uso previsto dei portafogli europei di identità digitale, compresa una indicazione dei dati che la parte facente affidamento sulla certificazione deve richiedere agli utenti.

3. Le parti facenti affidamento sulla certificazione non chiedono agli utenti di fornire dati diversi da quelli di cui all'indicazione fornita a norma del paragrafo 2, lettera c).

4. I paragrafi 1 e 2 lasciano impregiudicato il diritto dell'Unione o nazionale applicabile alla prestazione di servizi specifici.

5. Gli Stati membri rendono pubbliche online le informazioni di cui al paragrafo 2, in forma firmata o sigillata elettronicamente e adatta al trattamento automatizzato.

6. Le parti facenti affidamento sulla certificazione registrate a norma del presente articolo informano senza indugio gli Stati membri in merito alle modifiche delle informazioni fornite nella registrazione a norma del paragrafo 2.

7. Gli Stati membri prevedono un meccanismo comune che consente l'identificazione e l'autenticazione delle parti facenti affidamento sulla certificazione, secondo quanto previsto all'articolo 5 bis, paragrafo 5, lettera c).

8. Qualora intendano avvalersi dei portafogli europei di identità digitale, le parti facenti affidamento sulla certificazione si identificano nei confronti dell'utente.

9. Le parti facenti affidamento sulla certificazione sono responsabili dell'esecuzione della procedura di autenticazione e di convalida dei dati di identificazione personale e degli attestati elettronici di attributi richiesti dai portafogli europei di identità digitale. Le parti facenti affidamento sulla certificazione non rifiutano l'uso di pseudonimi se l'identificazione dell'utente non è richiesta dal diritto dell'Unione o nazionale.

10. Gli intermediari che agiscono per conto delle parti facenti affidamento sulla certificazione sono considerati parti facenti affidamento sulla certificazione e non conservano dati sul contenuto della transazione.

11. Entro 21 novembre 2024 la Commissione, mediante atti di esecuzione relativi all'attuazione dei portafogli europei di identità digitale di cui all'articolo 6 bis, paragrafo 23, stabilisce specifiche e procedure tecniche per i requisiti di cui ai paragrafi 2, 5 e da 6a 9 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 5 quater

Certificazione dei portafogli europei di identità digitale

1. La conformità dei portafogli europei di identità digitale e dei regimi di identificazione elettronica nell'ambito dei quali sono forniti ai requisiti di cui all'articolo 5 bis, paragrafi 4, 5 e 8, al requisito della separazione logica di cui all'articolo 5 bis, paragrafo 14, e, se del caso, alle norme e alle specifiche tecniche di cui all'articolo 5 bis, paragrafo 24, è certificata da organismi di valutazione della conformità designati dagli Stati membri.

▼M2

2. La certificazione della conformità dei portafogli europei di identità digitale ai requisiti di cui al paragrafo 1 del presente articolo, o di parti di essi, che sono pertinenti in materia di cibersicurezza, è effettuata in conformità dei sistemi europei di certificazione della cibersicurezza adottati a norma del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio ([1]) e menzionati negli atti di esecuzione di cui al paragrafo 6 del presente articolo.

3. Gli Stati membri istituiscono sistemi nazionali di certificazione secondo i requisiti stabiliti negli atti di esecuzione di cui al paragrafo 6 del presente articolo per i requisiti di cui al paragrafo 1 del presente articolo che non sono pertinenti in materia di cibersicurezza e per i requisiti di cui al paragrafo 1 del presente articolo che sono pertinenti in materia di cibersicurezza nella misura in cui i sistemi di certificazione della cibersicurezza di cui al paragrafo 2 del presente articolo non contemplino, o contemplino solo parzialmente, tali requisiti di cibersicurezza, anche per tali requisiti. Gli Stati membri trasmettono i loro progetti di sistemi nazionali di certificazione al gruppo di cooperazione per l'identità digitale europea istituito a norma dell'articolo 46 sexies, paragrafo 1 ("gruppo di cooperazione"). Il gruppo di cooperazione può formulare pareri e raccomandazioni.

4. La certificazione a norma del paragrafo 1 è valida fino a cinque anni, a condizione che sia effettuata una valutazione di vulnerabilità ogni due anni. Qualora sia individuata una vulnerabilità a cui non è posto rimedio 'in modo tempestivo, la certificazione è annullata.

5. La conformità ai requisiti di cui all'articolo 5 bis relativi ai trattamenti dei dati personali può essere certificata a norma del regolamento (UE) 2016/679.

6. Entro il 21 novembre 2024 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili alla certificazione dei portafogli europei di identità digitale di cui ai paragrafi 1, 2 e 3 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

7. Gli Stati membri comunicano alla Commissione i nomi e gli indirizzi degli organismi di valutazione della conformità di cui al paragrafo 1. La Commissione mette tali informazioni a disposizione di tutti gli Stati membri.

8. Alla Commissione è conferito il potere di adottare atti delegati, conformemente all'articolo 47, che fissano criteri specifici che gli organismi di valutazione della conformità designati di cui al paragrafo 1 del presente articolo devono soddisfare.

([1]) 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).

▼M2

Articolo 5 quinquies

Pubblicazione di un elenco dei portafogli europei di identità digitale certificati

1. Gli Stati membri informano senza indebito ritardo la Commissione e il gruppo di cooperazione istituito a norma dell'articolo 46 sexies, paragrafo 1, in merito ai portafogli europei di identità digitale che sono stati forniti a norma dell'articolo 5 bis e certificati dagli organismi di valutazione della conformità di cui all'articolo 5 quater, paragrafo 1. Essi informano senza indebito ritardo la Commissione e il gruppo di cooperazione istituito a norma dell'articolo 46 sexies, paragrafo 1, dell'eventuale annullamento di una certificazione e ne indicano i motivi.

2. Fatto salvo l'articolo 5 bis, paragrafo 18, le informazioni fornite dagli Stati membri di cui al paragrafo 1 del presente articolo comprendono almeno:

a) il certificato e la relazione di valutazione della certificazione del portafoglio europeo di identità digitale certificato;

b) una descrizione del regime di identificazione elettronica nell'ambito del quale è fornito il portafoglio europeo di identità digitale;

c) il regime di vigilanza applicabile e informazioni sul regime di responsabilità per quanto riguarda la parte che fornisce il portafoglio europeo di identità digitale;

d) l'autorità o le autorità responsabili del regime di identificazione elettronica;

e) disposizioni per la sospensione o la revoca del regime di identificazione elettronica o dell'autenticazione oppure di parti compromesse dell'uno o dell'altra.

3. Sulla base delle informazioni pervenutele a norma del paragrafo 1, la Commissione redige, pubblica nella *Gazzetta ufficiale dell'Unione europea* e mantiene, in un formato leggibile meccanicamente, un elenco dei portafogli europei di identità digitale certificati.

4. Uno Stato membro può presentare alla Commissione una richiesta di eliminazione, dall'elenco di cui al paragrafo 3, di un portafoglio europeo di identità digitale e del regime di identificazione elettronica nell'ambito del quale è fornito.

5. Qualora le informazioni fornite a norma del paragrafo 1 subiscano modifiche, lo Stato membro fornisce alla Commissione informazioni aggiornate.

6. La Commissione tiene aggiornato l'elenco di cui al paragrafo 3 pubblicando nella *Gazzetta ufficiale dell'Unione europea* le corrispondenti modifiche dell'elenco entro un mese dalla ricezione di una richiesta a norma del paragrafo 4 o di informazioni aggiornate a norma del paragrafo 5.

7. Entro il 21 novembre 2024 la Commissione, mediante atti di esecuzione relativo all'attuazione dei portafogli europei di identità digitale di cui all'articolo 5 bis, paragrafo 23, stabilisce i formati e le procedure applicabili ai fini dei paragrafi 1, 4 e 5 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼M2

Articolo 5 sexies

Violazione della sicurezza dei portafogli europei di identità digitale

1. In caso di violazione o parziale compromissione dei portafogli europei di identità digitale forniti a norma dell'articolo 5 bis, dei meccanismi di convalida di cui all'articolo 5 bis, paragrafo 8, o del regime di identificazione elettronica nell'ambito del quale sono forniti i portafogli europei di identità digitale, tale da pregiudicare la loro affidabilità o l'affidabilità di altri portafogli europei di identità digitale, lo Stato membro che ha fornito i portafogli europei di identità digitale sospende senza indebito ritardo la fornitura e l'uso di portafogli europei di identità digitale.

Se giustificato dalla gravità della violazione della sicurezza o della compromissione di cui al primo comma, lo Stato membro ritira i portafogli europei di identità digitale senza indebito ritardo.

Lo Stato membro informa di conseguenza gli utenti interessati, i punti di contatto unici designati a norma dell'articolo 46 quater, paragrafo 1, le parti facenti affidamento sulla certificazione e la Commissione.

2. Qualora non sia posto rimedio alla violazione della sicurezza o alla compromissione di cui al paragrafo 1, primo comma, del presente articolo entro tre mesi dalla sospensione, lo Stato membro che ha fornito i portafogli europei di identità digitale ritira i portafogli europei di identità digitale e ne revoca la validità. Lo Stato membro informa di conseguenza gli utenti interessati, i punti di contatto unici designati a norma dell'articolo 46 quater, paragrafo 1, le parti facenti affidamento sulla certificazione e la Commissione in merito alla revoca.

3. Una volta posto rimedio alla violazione della sicurezza o alla compromissione di cui al paragrafo 1, primo comma, del presente articolo, lo Stato membro fornitore ripristina la fornitura e l'utilizzo dei portafogli europei di identità digitale e informa senza indebito ritardo gli utenti interessati e le parti facenti affidamento sulla certificazione, i punti di contatto unici designati a norma dell'articolo 46 quater, paragrafo 1, e la Commissione.

4. La Commissione pubblica senza indebito ritardo le corrispondenti modifiche dell'elenco di cui all'articolo 5 quinquies nella *Gazzetta ufficiale dell'Unione europea*.

5. Entro il 21 novembre 2024 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili alle misure di cui ai paragrafi 1, 2 e 3 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 5 septies

Ricorso transfrontaliero ai portafogli europei di identità digitale

1. Qualora gli Stati membri richiedano l'identificazione e l'autenticazione elettroniche per accedere a servizi online prestati da un organismo del settore pubblico, essi accettano anche i portafogli europei di identità digitale forniti conformemente al presente regolamento.

▼M2

2. Qualora a norma del diritto dell'Unione o nazionale le parti private facenti affidamento sulla certificazione che forniscono servizi, ad eccezione delle microimprese e delle piccole imprese quali definite all'articolo 2 dell'allegato della raccomandazione 2003/361/CE della Commissione ([1]), siano tenute a utilizzare l'autenticazione forte dell'utente per l'identificazione online, o qualora l'identificazione forte dell'utente per l'identificazione online sia richiesta per obbligo contrattuale, anche nei settori dei trasporti, dell'energia, delle banche, dei servizi finanziari, della sicurezza sociale, della sanità, dell'acqua potabile, dei servizi postali, dell'infrastruttura digitale, dell'istruzione o delle telecomunicazioni, tali parti private facenti affidamento sulla certificazione accettano, entro 36 mesi dalla data di entrata in vigore degli atti di esecuzione di cui all'articolo 5 bis, paragrafo 23, e all'articolo 5 quater, paragrafo 6, e solo su richiesta volontaria dell'utente, anche i portafogli europei di identità digitale forniti conformemente al presente regolamento.

3. Qualora i fornitori delle piattaforme online di dimensioni molto grandi di cui all'articolo 33 del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio ([2]) richiedano l'autenticazione degli utenti per l'accesso ai servizi online, essi accettano e agevolano anche l'uso dei portafogli europei di identità digitale forniti conformemente al presente regolamento per l'autenticazione degli utenti, esclusivamente su richiesta volontaria dell'utente e nel rispetto dei dati minimi necessari per lo specifico servizio online per il quale è richiesta l'autenticazione.

4. In collaborazione con gli Stati membri, la Commissione facilita l'elaborazione di codici di condotta in stretta cooperazione con tutti i pertinenti portatori di interessi, compresa la società civile, per contribuire all'ampia disponibilità e utilizzabilità dei portafogli europei di identità digitale che rientrano nell'ambito di applicazione del presente regolamento nonché per incoraggiare i prestatori di servizi a ultimare l'elaborazione dei codici di condotta.

5. Entro 24 mesi dall'introduzione dei portafogli europei di identità digitale la Commissione valuta la domanda di portafogli europei di identità digitale, nonché la loro disponibilità e utilizzabilità, tenendo conto di criteri quali l'adozione da parte degli utenti, la presenza transfrontaliera dei prestatori di servizi, gli sviluppi tecnologici, l'evoluzione dei modelli di utilizzo e la domanda dei consumatori.

▼M2

SEZIONE 2

Regimi di identificazione elettronica

▼B

Articolo 6

Riconoscimento reciproco

1. Ove il diritto o la prassi amministrativa nazionale richiedano l'impiego di un'identificazione elettronica mediante mezzi di identificazione e autenticazione elettroniche per accedere a un servizio prestato da un organismo del settore pubblico online in uno Stato membro, i

([1]) Raccomandazione 2003/361/CE della Commissione, del 6 maggio 2003, relativa alla definizione delle microimprese, piccole e medie imprese (GU L 124 del 20.5.2003, pag. 36).

([2]) Regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio, del 19 ottobre 2022, relativo a un mercato unico dei servizi digitali e che modifica la direttiva 2000/31/CE (regolamento sui servizi digitali) (GU L 277 del 27.10.2022, pag. 1).

▼B

mezzi di identificazione elettronica rilasciati in un altro Stato membro sono riconosciuti nel primo Stato membro ai fini dell'autenticazione transfrontaliera di tale servizio online, purché soddisfino le seguenti condizioni:

a) i mezzi di identificazione elettronica sono rilasciati nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione a norma dell'articolo 9;

b) il livello di garanzia dei mezzi di identificazione elettronica corrisponde a un livello di garanzia pari o superiore al livello di garanzia richiesto dall'organismo del settore pubblico competente per accedere al servizio online in questione nel primo Stato membro, sempre che il livello di garanzia di tali mezzi di identificazione elettronica corrisponda al livello di garanzia significativo o elevato;

c) l'organismo del settore pubblico competente usa il livello di garanzia significativo o elevato in relazione all'accesso a tale servizio online.

Tale riconoscimento ha luogo non oltre 12 mesi dalla data in cui la Commissione pubblica l'elenco i di cui alla lettera a), primo comma.

2. Un mezzo di identificazione elettronica rilasciato nell'ambito di un regime di identificazione elettronica compreso nell'elenco pubblicato dalla Commissione a norma dell'articolo 9 e che corrisponde al livello di garanzia basso può essere riconosciuto dagli organismi del settore pubblico ai fini dell'autenticazione transfrontaliera del servizio prestato online da tali organismi.

Articolo 7

Ammissibilità alla notifica dei regimi di identificazione elettronica

Un regime di identificazione elettronica è ammesso alla notifica ai sensi dell'articolo 9, paragrafo 1, purché soddisfi tutte le seguenti condizioni:

a) i mezzi di identificazione elettronica nell'ambito del regime di identificazione elettronica sono rilasciati:

   i) dallo Stato membro notificante;

   ii) su incarico dello Stato membro notificante; o

   iii) a titolo indipendente dallo Stato membro notificante e sono riconosciuti da tale Stato membro;

b) i mezzi di identificazione elettronica nell'ambito del regime di identificazione elettronica possono essere utilizzati per accedere almeno a un servizio che è fornito da un organismo del settore pubblico e che richiede l'identificazione elettronica nello Stato membro notificante;

c) il regime di identificazione elettronica e i mezzi di identificazione elettronica rilasciati conformemente alle sue disposizioni soddisfano i requisiti di almeno uno dei livelli di garanzia stabiliti nell'atto di esecuzione di cui all'articolo 8, paragrafo 3;

▼B

d) lo Stato membro notificante garantisce che i dati di identificazione personale che rappresentano unicamente la persona in questione siano attribuiti, conformemente alle specifiche tecniche, norme e procedure relative al pertinente livello di garanzia definito nell'atto di esecuzione di cui all'articolo 8, paragrafo 3, alla persona fisica o giuridica di cui all'articolo 3, punto 1, al momento in cui è rilasciata l'identificazione elettronica nell'ambito di detto regime;

e) la parte che rilascia i mezzi di identificazione elettronica nell'ambito di detto regime assicura che i mezzi di identificazione elettronica siano attribuiti alla persona di cui alla lettera d) del presente articolo conformemente alle specifiche, norme e procedure tecniche relative al pertinente livello di garanzia definito nnell'atto di esecuzione di cui all'articolo 8, paragrafo 3;

f) lo Stato membro notificante garantisce la disponibilità dell'autenticazione online, per consentire alle parti facenti affidamento sulla certificazione stabilite nel territorio di un altro Stato membro di confermare i dati di identificazione personale che hanno ricevuto in forma elettronica.

Per le parti facenti affidamento sulla certificazione diverse dagli organismi del settore pubblico, lo Stato membro notificante può definire i termini di accesso a tale autenticazione. Quando l'autenticazione transfrontaliera è effettuata in relazione a un servizio online prestato da un organismo del settore pubblico, essa è fornita a titolo gratuito.

Gli Stati membri non impongono alcun requisito tecnico specifico sproporzionato alle parti facenti affidamento sulla certificazione che intendono effettuare tale autenticazione, qualora tali requisiti impediscano o ostacolino notevolmente l'interoperabilità dei regimi di identificazione elettronica notificati;

▼M2

g) almeno sei mesi prima della notifica di cui all'articolo 9, paragrafo 1, lo Stato membro notificante fornisce agli altri Stati membri, ai fini dell'articolo 12, paragrafo 5, una descrizione di tale regime conformemente alle modalità procedurali stabilite dagli atti di esecuzione adottati a norma dell'articolo 12, paragrafo 6;

▼B

h) il regime di identificazione elettronica soddisfa i requisiti definiti nell'atto di esecuzione di cui all'articolo 12, paragrafo 8.

Articolo 8

Livelli di garanzia dei regimi di identificazione elettronica

1. Un regime di identificazione elettronica notificato a norma dell'articolo 9, paragrafo 1, specifica livelli di garanzia basso, significativo e/o elevato per i mezzi di identificazione elettronica rilasciati nell'ambito di detto regime.

2. I livelli di garanzia basso, significativo e elevato soddisfano rispettivamente i seguenti criteri:

▼B

a) il livello di garanzia basso si riferisce a mezzi di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce un grado di sicurezza limitato riguardo all'identità pretesa o dichiarata di una persona ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, il cui scopo è quello di ridurre il rischio di uso abusivo o alterazione dell'identità;

b) il livello di garanzia significativo si riferisce a mezzi di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce un grado di sicurezza significativo riguardo all'identità pretesa o dichiarata di una persona ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, il cui scopo è quello di ridurre significativamente il rischio di uso abusivo o alterazione dell'identità;

c) il livello di garanzia elevato si riferisce a un mezzo di identificazione elettronica nel contesto di un regime di identificazione elettronica che fornisce riguardo all'identità pretesa o dichiarata di una persona un grado di sicurezza più elevato dei mezzi di identificazione elettronica aventi un livello di garanzia significativo ed è caratterizzato in riferimento a specifiche, norme e procedure tecniche a esso pertinenti, compresi controlli tecnici, il cui scopo è quello di impedire l'uso abusivo o l'alterazione dell'identità.

▼M2

3. Entro il 18 settembre 2015, tenendo conto delle norme internazionali pertinenti e fatto salvo il paragrafo 2, la Commissione, mediante atti di esecuzione, definisce le specifiche, norme e procedure tecniche minime in riferimento alle quali sono specificati i livelli di garanzia basso, significativo e elevato dei mezzi di identificazione elettronica.;

▼B

Le suddette specifiche, norme e procedure tecniche minime sono fissate facendo riferimento all'affidabilità e alla qualità dei seguenti elementi:

a) della procedura di controllo e verifica dell'identità delle persone fisiche o giuridiche che chiedono il rilascio dei mezzi di identificazione elettronica;

b) della procedura di rilascio dei mezzi di identificazione elettronica richiesti;

c) del meccanismo di autenticazione mediante il quale la persona fisica o giuridica usa i mezzi di identificazione elettronica per confermare la propria identità a una parte facente affidamento sulla certificazione;

d) dell'entità che rilascia i mezzi di identificazione elettronica;

e) di qualsiasi altro organismo implicato nella domanda di rilascio dei mezzi di identificazione elettronica; e

f) delle specifiche tecniche e di sicurezza dei mezzi di identificazione elettronica rilasciati.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

Articolo 9

Notifica

1. Lo Stato membro notificante rende note alla Commissione le informazioni seguenti e, senza indugio, qualsiasi loro successiva modifica:

a) una descrizione del regime di identificazione elettronica, con indicazione dei suoi livelli di garanzia e della o delle entità che rilasciano i mezzi di identificazione elettronica nell'ambito del regime;

b) il regime di vigilanza e il regime di informazioni sulla responsabilità applicabili per quanto riguarda:

i) la parte che rilascia i mezzi di identificazione elettronica; e

ii) la parte che gestisce la procedura di autenticazione;

c) l'autorità o le autorità responsabili del regime di identificazione elettronica;

d) informazioni sull'entità o sulle entità che gestiscono la registrazione dei dati unici di identificazione personale;

e) una descrizione di come sono soddisfatti i requisiti definiti negli atti di esecuzione di cui all'articolo 12, paragrafo 8;

f) una descrizione dell'autenticazione di cui all'articolo 7, lettera f);

g) disposizioni per la sospensione o la revoca del regime di identificazione elettronica notificato o dell'autenticazione oppure di parti compromesse dell'uno o dell'altra.

▼M2

2. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea*, senza indebito ritardo, un elenco dei regimi di identificazione elettronica notificati a norma del paragrafo 1 congiuntamente alle informazioni fondamentali su tali regimi.

3. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* le modifiche dell'elenco di cui al paragrafo 2 entro un mese dalla ricezione delle notifiche.

▼B

4. Uno Stato membro può presentare alla Commissione una richiesta di eliminazione del regime di identificazione elettronica da esso notificato dall'elenco di cui al paragrafo 2. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* le corrispondenti modifiche dell'elenco entro un mese dalla data di ricezione della richiesta dello Stato membro.

▼B

5. La Commissione può, mediante atti di esecuzione, definire le circostanze, i formati e le procedure delle notifiche a norma del paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 10

▼M2

Violazione della sicurezza dei regimi di identificazione elettronica

▼B

1. In caso di violazione o parziale compromissione del regime di identificazione elettronica notificato ai sensi dell'articolo 9, paragrafo 1, o dell'autenticazione di cui all'articolo 7, lettera f), con limitazione dell'affidabilità dell'autenticazione transfrontaliera di tale regime, lo Stato membro notificante senza indugio sospende o revoca tale autenticazione transfrontaliera o le sue parti compromesse e ne informa gli altri Stati membri e la Commissione.

2. Una volta posto rimedio alla violazione o alla compromissione di cui al paragrafo 1, lo Stato membro notificante ristabilisce l'autenticazione transfrontaliera e informa senza indugio gli altri Stati membri e la Commissione.

3. Qualora non sia posto rimedio alla violazione o alla compromissione di cui al paragrafo 1 entro tre mesi dalla sospensione o dalla revoca, lo Stato membro notificante notifica agli altri Stati membri e alla Commissione il ritiro del regime di identificazione elettronica.

La Commissione pubblica senza indebito ritardo le corrispondenti modifiche dell'elenco di cui all'articolo 9, paragrafo 2, nella *Gazzetta ufficiale dell'Unione europea*.

Articolo 11

Responsabilità

1. Lo Stato membro notificante è responsabile per i danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito al mancato adempimento dei suoi obblighi di cui all'articolo 7, lettere d) e f), in una transazione transfrontaliera.

2. La parte che rilascia i mezzi di identificazione elettronica è responsabile di danni causati con dolo o per negligenza a qualsiasi persona fisica o giuridica in seguito al mancato adempimento dell'obbligo di cui all'articolo 7, lettera e), in una transazione transfrontaliera.

3. La parte che gestisce la procedura di autenticazione è responsabile di danni causati con dolo o per negligenza a qualsiasi persona fisica o giuridica per non avere garantito la corretta gestione dell'autenticazione di cui all'articolo 7, lettera f), in una transazione transfrontaliera.

4. I paragrafi 1, 2 e 3 si applicano conformemente alle norme nazionali in materia di responsabilità.

▼B

5. I paragrafi 1, 2 e 3 lasciano impregiudicata la responsabilità conformemente al diritto nazionale delle parti di una transazione in cui sono utilizzati mezzi di identificazione elettronica che rientrano nel regime di identificazione elettronica notificato a norma dell'articolo 9, paragrafo 1.

▼M2

Articolo 11 bis

Corrispondenza dell'identità a livello transfrontaliero

1. Quando fungono da parti facenti affidamento sulla certificazione per i servizi transfrontalieri, gli Stati membri garantiscono una corrispondenza univoca dell'identità delle persone fisiche che utilizzano mezzi di identificazione elettronica notificati o i portafogli europei di identità digitale.

2. Gli Stati membri prevedono misure tecniche e organizzative per garantire un livello elevato di protezione dei dati personali utilizzati per la corrispondenza dell'identità e per prevenire la profilazione degli utenti.

3. Entro il 21 novembre 2024 la Commissione stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai requisiti di cui al paragrafo 1 del presente articolo mediante atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

Articolo 12

▼M2

Interoperabilità

▼B

1. I regimi nazionali di identificazione elettronica notificati a norma dell'articolo 9, paragrafo 1, sono interoperabili.

2. È istituito un quadro di interoperabilità ai fini del paragrafo 1.

3. Il quadro di interoperabilità risponde ai seguenti criteri:

a) mira a essere neutrale dal punto di vista tecnologico e non comporta discriminazioni tra specifiche soluzioni tecniche nazionali per l'identificazione elettronica all'interno di uno Stato membro;

b) segue, ove possibile, le norme europee e internazionali;

▼M2

c) facilita l'applicazione della tutela della vita privata e della sicurezza fin dalla progettazione;

———————

▼B

4. Il quadro di interoperabilità è composto da:

a) un riferimento ai requisiti tecnici minimi connessi ai livelli di garanzia di cui all'articolo 8;

▼B

b) una mappatura dei livelli di garanzia nazionali dei regimi di identificazione elettronica notificati in base ai livelli di garanzia di cui all'articolo 8;

c) un riferimento ai requisiti tecnici minimi di interoperabilità;

▼M2

d) un riferimento a un insieme minimo di dati di identificazione personale necessari a rappresentare in modo univoco una persona fisica o giuridica, una persona fisica che rappresenta un'altra persona fisica o una persona giuridica disponibile nell'ambito dei regimi di identificazione elettronica;

▼B

e) norme di procedura;

f) disposizioni per la risoluzione delle controversie; e

g) norme di sicurezza operativa comuni.

▼M2

5. Gli Stati membri effettuano valutazioni tra pari dei regimi di identificazione elettronica che rientrano nell'ambito di applicazione del presente regolamento e che devono essere notificati a norma dell'articolo 9, paragrafo 1, lettera a).

6. Entro il 18 marzo 2025 la Commissione, mediante atti di esecuzione, fissa le modalità procedurali necessarie per le valutazioni tra pari di cui al paragrafo 5 del presente articolo, al fine di promuovere un elevato livello di fiducia e di sicurezza, commisurato al grado di rischio esistente. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

———————

8. Entro il 18 settembre 2025, al fine di garantire condizioni uniformi di esecuzione del requisito di cui al paragrafo 1 del presente articolo, la Commissione, fatti salvi i criteri di cui al paragrafo 3 del presente articolo e tenendo conto dei risultati della cooperazione fra gli Stati membri, adotta atti di esecuzione sul quadro di interoperabilità quale definito al paragrafo 4 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

9. Gli atti di esecuzione di cui a paragrafi 7 e 8 sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼M2

Articolo 12 bis

Certificazione dei regimi di identificazione elettronica

1. La conformità ai requisiti di cibersicurezza di cui al presente regolamento dei regimi di identificazione elettronica da notificare, compresa la conformità ai pertinenti requisiti di cibersicurezza di cui all'articolo 8, paragrafo 2, per quanto riguarda i livelli di garanzia dei regimi di identificazione elettronica, è certificata dagli organismi di valutazione della conformità designati dagli Stati membri.

▼M2

2. La certificazione ai sensi del paragrafo 1 del presente articolo è effettuata nell'ambito di un pertinente sistema di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881, o di parti di esso, nella misura in cui il certificato di cibersicurezza o parti di esso contemplino tali requisiti di cibersicurezza.

3. La certificazione di cui al paragrafo 1 è valida per un periodo massimo di cinque anni, a condizione che sia effettuata una valutazione delle vulnerabilità ogni due anni. Qualora sia individuata una vulnerabilità a cui non è posto rimedio entro tre mesi dall'individuazione, la certificazione è annullata.

4. Fatto salvo il paragrafo 2, gli Stati membri possono, conformemente a tale paragrafo, chiedere a uno Stato membro notificante informazioni supplementari sui regimi di identificazione elettronica, o su parti di essi, certificati.

5. La valutazione tra pari dei regimi di identificazione elettronica di cui all'articolo 12, paragrafo 5, non si applica ai regimi di identificazione elettronica, o a parti di essi, certificati conformemente al paragrafo 1 del presente articolo. Gli Stati membri possono utilizzare un certificato o una dichiarazione di conformità, rilasciati conformemente a un pertinente sistema di certificazione o a parti di esso, ai requisiti non relativi alla cibersicurezza di cui all'articolo 8, paragrafo 2, per quanto riguarda il livello di garanzia dei regimi di identificazione elettronica.

6. Gli Stati membri comunicano alla Commissione i nomi e gli indirizzi degli organismi di valutazione della conformità di cui al paragrafo 1. La Commissione mette tali informazioni a disposizione di tutti gli Stati membri.

Articolo 12 ter

Accesso a componenti hardware e software

Se i fornitori di portafogli europei di identità digitale e gli emittenti di mezzi di identificazione elettronica notificati che agiscono a titolo commerciale o professionale e utilizzano i servizi di piattaforma di base definiti all'articolo 2, punto 2, del regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio ([1]) ai fini della fornitura, agli utenti finali, di servizi del portafoglio europeo di identità digitale e di mezzi di identificazione elettronica, o nello svolgimento di tale attività, sono utenti commerciali ai sensi dell'articolo 2, punto 21, di tale regolamento, i gatekeeper consentono loro, in particolare, l'effettiva interoperabilità, nonché l'accesso, ai fini dell'interoperabilità, allo stesso sistema operativo e alle stesse componenti hardware o software. Tale interoperabilità effettiva e tale accesso sono consentiti a titolo gratuito e indipendentemente dal fatto che le componenti hardware o software che sono disponibili per il gatekeeper, o da esso utilizzati, al momento della fornitura di tali servizi, siano parte del sistema operativo, ai sensi dell'articolo 6, paragrafo 7, del regolamento (UE) 2022/1925. Il presente articolo non pregiudica l'articolo 5 bis, paragrafo 14, del presente regolamento.

([1]) Regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio, del 14 settembre 2022, relativo a mercati equi e contendibili nel settore digitale e che modifica le direttive (UE) 2019/1937 e (UE) 2020/1828 (regolamento sui mercati digitali) (GU L 265 del 12.10.2022, pag. 1).

▼B

CAPO III

SERVIZI FIDUCIARI

SEZIONE 1

Disposizioni generali

Articolo 13

Responsabilità e onere della prova

▼M2

1. Fatti salvi il paragrafo 2 del presente articolo e il regolamento (UE) 2016/679, i prestatori di servizi fiduciari sono responsabili dei danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito a un mancato adempimento degli obblighi ai sensi del presente regolamento. Qualsiasi persona fisica o giuridica che abbia subito un danno materiale o immateriale a seguito di una violazione del presente regolamento da parte di un prestatore di servizi fiduciari ha il diritto di chiedere un risarcimento conformemente al diritto dell'Unione e nazionale.

L'onere di dimostrare il dolo o la negligenza di un prestatore di servizi fiduciari non qualificato ricade sulla persona fisica o giuridica che denuncia il danno di cui al primo comma.

Si presume il dolo o la negligenza da parte di un prestatore di servizi fiduciari qualificato, salvo che questi dimostri che il danno di cui al primo comma si è verificato senza suo dolo o sua negligenza.

▼B

2. Se i prestatori di servizi fiduciari informano debitamente e preventivamente i loro clienti delle limitazioni d'uso dei servizi da essi forniti e se tali limitazioni sono riconoscibili da parte di terzi, non sono responsabili dei danni che derivano dall'utilizzo di servizi oltre i limiti indicati.

3. I paragrafi 1 e 2 si applicano conformemente alle norme nazionali in materia di responsabilità.

▼M2

Articolo 14

Aspetti internazionali

1. I servizi fiduciari prestati da prestatori di servizi fiduciari stabiliti in un paese terzo o da un'organizzazione internazionale sono riconosciuti giuridicamente equivalenti ai servizi fiduciari qualificati prestati da prestatori di servizi fiduciari qualificati stabiliti nell'Unione qualora i servizi fiduciari aventi origine nel paese terzo o dall' organizzazione internazionale siano riconosciuti mediante atti di esecuzione o un accordo concluso fra l'Unione e il paese terzo o l'organizzazione internazionale a norma dell'articolo 218 TFUE.

Gli atti di esecuzione di cui al primo comma sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼M2

2. Gli atti di esecuzione e l'accordo di cui al paragrafo 1 garantiscono che i requisiti che si applicano ai prestatori di servizi fiduciari qualificati stabiliti nell'Unione e ai servizi fiduciari qualificati da essi forniti siano soddisfatti dai prestatori di servizi fiduciari nel paese terzo interessato o dall'organizzazione internazionale, nonché dai servizi fiduciari da essi forniti. In particolare, i paesi terzi e le organizzazioni internazionali istituiscono, mantengono e pubblicano un elenco di fiducia dei prestatori di servizi fiduciari riconosciuti.

3. L'accordo di cui al paragrafo 1 garantiscono che i servizi fiduciari qualificati forniti da prestatori di servizi fiduciari qualificati stabiliti nell'Unione siano riconosciuti come giuridicamente equivalenti ai servizi fiduciari forniti da prestatori di servizi fiduciari nel paese terzo o dall'organizzazione internazionale con cui è concluso l'accordo.

Articolo 15

Accessibilità per le persone con disabilità ed esigenze particolari

La fornitura di mezzi di identificazione elettronica, di servizi fiduciari e di prodotti destinati all'utente finale impiegati per la prestazione di tali servizi è resa disponibile in un linguaggio semplice e comprensibile, conformemente alla Convenzione delle Nazioni Unite sui diritti delle persone con disabilità e ai requisiti di accessibilità di cui alla direttiva (UE) 2019/882, recando in tal modo beneficio anche alle persone con limitazioni funzionali, come le persone anziane, e alle persone con un accesso limitato alle tecnologie digitali.

Articolo 16

Sanzioni

1. Fatto salvo l'articolo 31 della direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio ([1]), gli Stati membri stabiliscono le norme relative alle sanzioni applicabili in caso di violazioni del presente regolamento. Tali sanzioni sono effettive, proporzionate e dissuasive.

2. Gli Stati membri provvedono affinché tali violazioni del presente regolamento da parte di prestatori di servizi fiduciari qualificati e non qualificati siano soggette a sanzioni amministrative pari a un importo massimo di almeno:

a) EUR 5 000 000 se il prestatore di servizi fiduciari è una persona fisica; oppure

b) se il prestatore di servizi fiduciari è una persona giuridica, EUR 5 000 000 o pari all'1 % del fatturato mondiale totale annuo dell'impresa a cui apparteneva il prestatore di servizi fiduciari nell'esercizio precedente l'anno in cui si è verificata la violazione, se superiore.

([1]) 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).

▼M2

3. A seconda dell'ordinamento giuridico degli Stati membri, le regole in materia di sanzioni amministrative possono essere applicate in modo tale ch' l'azione sanzionatoria sia avviata dall'organismo di vigilanza competente e la sanzione pecuniaria sia irrogata dai tribunali nazionali competenti' L'applicazione di tali regole in tali Stati membri garantisce che tali mezzi di ricorso siano efficaci e abbiano un effetto equivalente alle sanzioni amministrative imposte direttamente dalle autorità di controllo.

▼B

SEZIONE 2

▼M2

Servizi fiduciari non qualificati

_____

▼M1

_____

▼M2

Articolo 19 bis

Requisiti per i prestatori di servizi fiduciari non qualificati

1. Un prestatore di servizi fiduciari non qualificato che presta servizi fiduciari non qualificati:

a) dispone di politiche adeguate e adotta misure corrispondenti per la gestione dei rischi giuridici, commerciali, operativi e di altro tipo, sia diretti che indiretti, per la prestazione del servizio fiduciario non qualificato, le quali, fatto salvo l'articolo 21 della direttiva (UE) 2022/2555, comprendono almeno misure relative:

   i) alla registrazione a un servizio fiduciario e alle relative procedure di onboarding;

   ii) ai controlli procedurali o amministrativi necessari per prestare servizi fiduciari;

   iii) alla gestione e all'attuazione dei servizi fiduciari;

b) alla notifica, senza indebito ritardo ma in ogni caso entro 24 ore dall'essere venuto a conoscenza di violazioni della sicurezza o perturbazioni, all'organismo di vigilanza, alle persone interessate identificabili, al pubblico se è di pubblico interesse e, ove applicabile, ad altre autorità competenti interessate, di tutte le eventuali violazioni della sicurezza o perturbazioni connesse alla prestazione del servizio o all'attuazione delle misure di cui alla lettera a), punti i), ii) o iii), aventi un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi.

2. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili al paragrafo 1, lettera a), del presente articolo. Si presume che i requisiti di cui al presente articolo siano stati rispettati, ove siano rispettate tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

SEZIONE 3

Servizi fiduciari qualificati

Articolo 20

Vigilanza dei prestatori di servizi fiduciari qualificati

▼M2

1. I prestatori di servizi fiduciari qualificati sono sottoposti, a proprie spese e almeno ogni 24 mesi, a una verifica da parte di un organismo di valutazione della conformità. Lo scopo della verifica è confermare che i prestatori di servizi fiduciari qualificati e i servizi fiduciari qualificati da essi prestati rispettano i requisiti di cui al presente regolamento e all'articolo 21 della direttiva (UE) 2022/2555. I prestatori di servizi fiduciari qualificati presentano la risultante relazione di valutazione della conformità all'organismo di vigilanza entro tre giorni lavorativi dalla sua ricezione.

1 *bis*. I prestatori di servizi fiduciari qualificati informano l'organismo di vigilanza al più tardi un mese prima di qualsiasi verifica programmata e consentono all'organismo di vigilanza di partecipare, su richiesta, in qualità di osservatore.

1 *ter*. Gli Stati membri notificano senza indebito ritardo alla Commissione i nomi, gli indirizzi e i dettagli relativi all'accreditamento degli organismi di valutazione della conformità di cui al paragrafo 1 e qualsiasi successiva modifica degli stessi. La Commissione mette tali informazioni a disposizione di tutti gli Stati membri.

2. Fatto salvo il paragrafo 1, l'organismo di vigilanza può, in qualsiasi momento, condurre una verifica o chiedere a un organismo di valutazione della conformità di eseguire una valutazione di conformità dei prestatori di servizi fiduciari qualificati, a spese di tali prestatori di servizi fiduciari, per confermare che essi e i servizi fiduciari qualificati da essi prestati rispondono ai requisiti di cui al presente regolamento. Qualora siano state rilevate violazioni delle norme in materia di protezione dei dati personali' l'organismo di vigilanza informa senza indebito ritardo le autorità di controllo competenti a norma del regolamento (UE) 2016/679.

3. Qualora il prestatore di servizi fiduciari qualificato non soddisfi uno qualsiasi dei requisiti di cui al presente regolamento l'organismo di vigilanza gli impone di rimediare entro un termine stabilito, ove applicabile.

Qualora tale prestatore non rimedi e, ove applicabile, non rispetti il termine fissato dall'organismo di vigilanza, quest'ultimo, se ciò è giustificato in particolare dalla portata, dalla durata e dalle conseguenze di tale inadempienza, revoca la qualifica di tale prestatore o del servizio interessato da esso prestato.

3 *bis*. Qualora le autorità competenti designate o istituite a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555 informino l'organismo di vigilanza del fatto che il fornitore di servizi fiduciari qualificati non soddisfa uno qualsiasi dei requisiti di cui all'articolo 21 di tale direttiva, l'organismo di vigilanza, se ciò è giustificato in particolare dalla portata, dalla durata e dalle conseguenze di tale inadempienza, revoca la qualifica di tale prestatore o del servizio interessato da esso prestato.

▼M2

3 *ter.* Qualora le autorità di vigilanza istituite a norma dell'articolo 51 del regolamento (UE) 2016/679 informino l'organismo di vigilanza del fatto che il fornitore di servizi fiduciari qualificati non soddisfa uno qualsiasi dei requisiti di cui a tale regolamento, l'organismo di vigilanza, se ciò è giustificato in particolare dalla portata, dalla durata e dalle conseguenze di tale inadempienza, revoca la qualifica di tale prestatore o del servizio interessato da esso prestato.

3 *quater.* L'organismo di vigilanza comunica al prestatore di servizi fiduciari qualificato la revoca della sua qualifica o della qualifica del servizio interessato L'organismo di vigilanza informa l'organismo notificato a norma dell'articolo 22, paragrafo 3, del presente regolamento ai fini dell'aggiornamento degli elenchi di fiducia di cui al paragrafo 1 di tale articolo e l'autorità competente designata o istituita a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555.

4. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure riguardo a quanto segue:

a) l'accreditamento degli organismi di valutazione della conformità e la relazione di valutazione della conformità di cui al paragrafo 1;

b) i requisiti di verifica in base ai quali gli organismi di valutazione della conformità effettueranno le loro valutazioni della conformità, comprese valutazioni composite, dei prestatori di servizi fiduciari qualificati di cui al paragrafo 1;

c) i regimi di valutazione della conformità per l'esecuzione della valutazione della conformità dei prestatori di servizi fiduciari qualificati da parte degli organismi di valutazione della conformità e per la presentazione della relazione di cui al paragrafo 1.

Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

Articolo 21

Avviamento di un servizio fiduciario qualificato

▼M2

1. Qualora i prestatori di servizi fiduciari intendano avviare la prestazione di un servizio fiduciario qualificato, notificano all'organismo di vigilanza la loro intenzione insieme a una relazione di valutazione della conformità rilasciata da un organismo di valutazione della conformità che conferma il rispetto dei requisiti di cui al presente regolamento e all'articolo 21 della direttiva (UE) 2022/2555.

2. L'organismo di vigilanza verifica se il prestatore di servizi fiduciari e i servizi fiduciari da esso prestati rispettano i requisiti di cui al presente regolamento e, in particolare, i requisiti per i prestatori di servizi fiduciari qualificati e per i servizi fiduciari qualificati da essi prestati.

▼M2

Al fine di verificare il rispetto dei requisiti di cui all'articolo 21 della direttiva (UE) 2022/2555 da parte del prestatore di servizi fiduciari, l'organismo di vigilanza chiede alle autorità competenti designate o stabilite a norma dell'articolo 8, paragrafo 1, di tale direttiva di svolgere azioni di vigilanza in tal senso e di fornire informazioni sui risultati senza indebito ritardo e in ogni caso entro due mesi dal ricevimento della richiesta. Se la verifica non si è conclusa entro due mesi dalla notifica, tali autorità competenti ne informano l'organismo di vigilanza specificando i motivi del ritardo e il periodo necessario per concludere la verifica.

Se conclude che il prestatore di servizi fiduciari e i servizi fiduciari da esso prestati rispettano i requisiti di cui al presente regolamento, l'organismo di vigilanza concede la qualifica al prestatore di servizi fiduciari e ai servizi fiduciari da esso prestati e informa l'organismo di cui all'articolo 22, paragrafo 3, affinché aggiorni gli elenchi di fiducia di cui all'articolo 22, paragrafo 1, entro tre mesi dalla notifica conformemente al paragrafo 1 del presente articolo.

Se la verifica non si è conclusa entro tre mesi dalla notifica, l'organismo di vigilanza ne informa il prestatore di servizi fiduciari specificando i motivi del ritardo e il periodo necessario per concludere la verifica.

▼B

3. I prestatori di servizi fiduciari qualificati possono iniziare a prestare il servizio fiduciario qualificato dopo che la qualifica è stata registrata negli elenchi di fiducia di cui all'articolo 22, paragrafo 1.

▼M2

4. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce i formati e le procedure relativi alla notifica e alla verifica ai fini dei paragrafi 1 e 2 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

Articolo 22

Elenchi di fiducia

1. Tutti gli Stati membri istituiscono, mantengono e pubblicano elenchi di fiducia, che includono le informazioni relative ai prestatori di servizi fiduciari qualificati per i quali sono responsabili, unitamente a informazioni relative ai servizi fiduciari qualificati da essi prestati.

2. Gli Stati membri istituiscono, mantengono e pubblicano, in modo sicuro, gli elenchi di fiducia di cui al paragrafo 1, firmati o sigillati elettronicamente in una forma adatta al trattamento automatizzato.

3. Gli Stati membri notificano alla Commissione, senza indugio, informazioni sull'organismo responsabile dell'istituzione, del mantenimento e della pubblicazione degli elenchi nazionali di fiducia, precisando dove gli elenchi sono pubblicati, e sui certificati utilizzati per firmare o sigillare tali elenchi di fiducia e le eventuali modifiche apportate.

▼B

4. La Commissione rende pubbliche, attraverso un canale sicuro, le informazioni di cui al paragrafo 3 in forma firmata o sigillata elettronicamente e adatta al trattamento automatizzato.

5. Entro il 18 settembre 2015, la Commissione, mediante atti di esecuzione, specifica le informazioni di cui al paragrafo 1 e definisce le specifiche tecniche e i formati per gli elenchi di fiducia applicabili ai fini dei paragrafi da 1 a 4. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 23

Marchio di fiducia UE per i servizi fiduciari qualificati

1. Dopo la registrazione della qualifica di cui all'articolo 21, paragrafo 2, secondo comma, nell'elenco di fiducia di cui all'articolo 22, paragrafo 1, i prestatori di servizi fiduciari qualificati possono utilizzare il marchio di fiducia UE per presentare in modo semplice, riconoscibile e chiaro i servizi fiduciari qualificati da essi prestati.

2. Quando utilizzano il marchio di fiducia UE per i servizi fiduciari qualificati di cui al paragrafo 1, i prestatori di servizi fiduciari qualificati garantiscono che sul loro sito web sia disponibile un link all'elenco di fiducia pertinente.

3. Entro il 1º luglio 2015 la Commissione, mediante atti di esecuzione, fornisce criteri specifici relativi alla forma e, in particolare, alla presentazione, alla composizione, alla dimensione e al disegno del marchio di fiducia UE per i servizi fiduciari qualificati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 24

Requisiti per i prestatori di servizi fiduciari qualificati

▼M2

1. Allorché rilascia un certificato qualificato o un attestato elettronico di attributi qualificato, un prestatore di servizi fiduciari qualificato verifica l'identità e, se opportuno, eventuali attributi specifici della persona fisica o giuridica a cui deve essere rilasciato il certificato qualificato o l'attestato elettronico di attributi qualificato.

1 *bis.* La verifica dell'identità di cui al paragrafo 1 è effettuata, con mezzi adeguati, dal prestatore di servizi fiduciari qualificato, direttamente o tramite un terzo, sulla base di uno dei metodi seguenti o, ove necessario, di una combinazione degli stessi, conformemente agli atti di esecuzione di cui al paragrafo 1 quater:

a) mediante il portafoglio europeo di identità digitale o un mezzo di identificazione elettronica notificato che rispetta i requisiti di cui all'articolo 8 per quanto riguarda il livello di garanzia elevato;

b) mediante un certificato di una firma elettronica qualificata o di un sigillo elettronico qualificato rilasciato conformemente alla lettera a), c) o d);

▼M2

c) mediante altri metodi di identificazione che garantiscono l'identificazione della persona con un elevato livello di sicurezza, la conformità dei quali è confermata da un organismo di valutazione della conformità;

d) mediante la presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica, sulla base di adeguate prove e procedure, conformemente al diritto nazionale.

1 *ter*. La verifica degli attributi di cui al paragrafo 1 è effettuata, con mezzi adeguati, dal prestatore di servizi fiduciari qualificato, direttamente o tramite un terzo, sulla base di uno dei metodi seguenti o una combinazione degli stessi, ove necessario, conformemente agli atti di esecuzione di cui al paragrafo 1 quater:

a) mediante il portafoglio europeo di identità digitale o un mezzo di identificazione elettronica notificato che rispetta i requisiti di cui all'articolo 8 per quanto riguarda il livello di garanzia elevato;

b) mediante un certificato di una firma elettronica qualificata o di un sigillo elettronico qualificato rilasciato in conformità del paragrafo 1 bis, lettera a), c) o d);

c) mediante un attestato elettronico di attributi qualificato;

d) mediante altri metodi che garantiscono la verifica degli attributi con un elevato livello di sicurezza, la conformità dei quali è confermata da un organismo di valutazione della conformità;

e) mediante la presenza concreta della persona fisica o di un rappresentante autorizzato della persona giuridica, sulla base di adeguate prove e procedure, conformemente al diritto nazionale.

1 *quater*. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure per la verifica dell'identità e degli attributi conformemente ai paragrafi 1, 1 bis e 1 ter. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2

▼B

2. Un prestatore di servizi fiduciari qualificato che presta servizi fiduciari qualificati:

▼M2

a) informa l'organismo di vigilanza almeno un mese prima dell'attuazione di qualsiasi modifica nella prestazione dei suoi servizi fiduciari qualificati o con almeno tre mesi di anticipo qualora intenda cessare tali attività.

▼B

b) impiega personale e, ove applicabile, subcontraenti dotati delle competenze, dell'affidabilità, dell'esperienza e delle qualifiche necessarie e che hanno ricevuto una formazione adeguata in materia di norme di sicurezza e di protezione dei dati personali e applica procedure amministrative e gestionali, che corrispondono a norme europee o internazionali;

c) riguardo alla responsabilità civile per danni a norma dell'articolo 13, mantiene risorse finanziarie adeguate e/o si procura un'assicurazione di responsabilità civile appropriata, conformemente al diritto nazionale;

▼M2

d) prima di avviare una relazione contrattuale informa, in modo chiaro, completo e facilmente accessibile, in uno spazio accessibile al pubblico e individualmente, chiunque intenda utilizzare un servizio fiduciario qualificato in merito ai termini e alle condizioni precisi per l'utilizzo di tale servizio, comprese eventuali limitazioni del suo utilizzo;

e) utilizza sistemi affidabili e prodotti protetti da alterazioni e che garantiscono la sicurezza tecnica e l'affidabilità dei processi che assicurano, anche ricorrendo a tecniche crittografiche adeguate;

▼B

f) utilizza sistemi affidabili per memorizzare i dati a esso forniti, in modo verificabile, affinché:

i) siano accessibili alla consultazione del pubblico soltanto con il consenso della persona a cui i dati fanno riferimento;

ii) soltanto le persone autorizzate possano effettuare inserimenti e modifiche ai dati memorizzati;

iii) l'autenticità dei dati sia verificabile;

▼M2

f *bis*) fatto salvo l'articolo 21 della direttiva (UE) 2022/2555, dispone di politiche adeguate e adotta misure corrispondenti per la gestione dei rischi giuridici, commerciali, operativi e di altro tipo, sia diretti che indiretti, per la prestazione del servizio fiduciario qualificato, comprese almeno misure connesse ai seguenti aspetti:

i) registrazione a un servizio e relative procedure di onboarding;

ii) controlli procedurali o amministrativi;

iii) gestione e attuazione dei servizi;

f *ter*) senza indebito ritardo ma in ogni caso entro 24 ore dall'incidente, notifica all'organismo di vigilanza, alle persone interessate identificabili, agli altri organismi competenti interessati se applicabile e, su richiesta dell'organismo di vigilanza, al pubblico se è di pubblico interesse tutte le violazioni della sicurezza o perturbazioni connesse alla prestazione del servizio o all'attuazione delle misure di cui alla lettera f bis), punti i), ii) o iii), aventi un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi;

g) adotta misure adeguate contro la falsificazione, il furto o l'appropriazione indebita di dati o contro l'atto, compiuto senza diritto, di cancellarli, alterarli o renderli inaccessibili;

h) registra e mantiene accessibili per tutto il tempo necessario dopo la cessazione delle attività del prestatore di servizi fiduciari qualificato tutte le informazioni pertinenti relative a dati rilasciati e ricevuti dal prestatore di servizi fiduciari qualificato, a fini di produzione di prove nell'ambito di procedimenti giudiziari e per assicurare la continuità del servizio. Tali registrazioni possono essere elettroniche;

▼M2

i) dispone di un piano di cessazione delle attività aggiornato per garantire la continuità del servizio conformemente alle disposizioni verificate dall'organismo di vigilanza a norma dell'articolo 46 ter, paragrafo 4, lettera i);

_____

▼B

k) se i prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati, istituiscono una banca dati dei certificati aggiornata.

▼M2

L'organismo di vigilanza può chiedere informazioni in aggiunta alle informazioni notificate a norma del primo comma, lettera a), o il risultato di una valutazione della conformità e può subordinare a condizioni la concessione dell'autorizzazione ad attuare le modifiche previste ai servizi fiduciari qualificati. Se la verifica non si è conclusa entro tre mesi dalla notifica, l'organismo di vigilanza ne informa il prestatore di servizi fiduciari specificando i motivi del ritardo e il periodo necessario per concludere la verifica.

▼B

3. Se un prestatore di servizi fiduciari qualificato che rilascia certificati qualificati decide di revocare un certificato, registra tale revoca nella propria banca dati dei certificati e pubblica la situazione di revoca del certificato tempestivamente e, in ogni caso, entro 24 ore dal ricevimento della richiesta. La revoca diventa immediatamente effettiva all'atto della pubblicazione.

4. In considerazione del paragrafo 3, i prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati trasmettono alle parti facenti affidamento sulla certificazione informazioni sulla situazione di validità o revoca dei certificati qualificati da essi rilasciati. Queste informazioni sono rese disponibili almeno per ogni certificato rilasciato in qualsiasi momento e oltre il periodo di validità del certificato, in modo automatizzato, affidabile, gratuito ed efficiente.

▼M2

4 *bis.* I paragrafi 3 e 4 si applicano in maniera analoga alla revoca di attestati elettronici qualificati di attributi.

4 *ter.* Alla Commissione è conferito il potere di adottare atti delegati, conformemente all'articolo 47, che stabiliscono le misure supplementari di cui al paragrafo 2, lettera f bis), del presente articolo.

5. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure riguardo ai requisiti di cui al paragrafo 2, del presente articolo. Si presume che i requisiti di cui al presente paragrafo siano stati rispettati ove siano rispettate tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 24 bis

Riconoscimento dei servizi fiduciari qualificati

1. Le firme elettroniche qualificate basate su un certificato qualificato rilasciato in uno Stato membro e i sigilli elettronici qualificati basati su un certificato qualificato rilasciato in uno Stato membro

▼M2

sono riconosciuti rispettivamente quali firme elettroniche qualificate e sigilli elettronici qualificati in tutti gli altri Stati membri.

2. I dispositivi qualificati per la creazione di una firma elettronica e i dispositivi qualificati per la creazione di un sigillo elettronico certificati in uno Stato membro sono riconosciuti rispettivamente quali dispositivi qualificati per la creazione di una firma elettronica e dispositivi qualificati per la creazione di un sigillo elettronico in tutti gli altri Stati membri.

3. Un certificato qualificato di firme elettroniche, un certificato qualificato di sigilli elettronici, un servizio fiduciario qualificato per la gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza e un servizio fiduciario qualificato per la gestione di dispositivi qualificati per la creazione di un sigillo elettronico a distanza forniti in uno Stato membro sono riconosciuti rispettivamente quali certificato qualificato di firme elettroniche, certificato qualificato di sigilli elettronici, servizio fiduciario qualificato per la gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza e servizio fiduciario qualificato per la gestione di dispositivi qualificati per la creazione di un sigillo elettronico a distanza in tutti gli altri Stati membri.

4. Un servizio di convalida qualificato delle firme elettroniche qualificate e un servizio di convalida qualificato dei sigilli elettronici qualificati forniti in uno Stato membro sono riconosciuti rispettivamente quali servizio di convalida qualificato delle firme elettroniche qualificate e servizio di convalida qualificato dei sigilli elettronici qualificati in tutti gli altri Stati membri.

5. Un servizio di conservazione qualificato delle firme elettroniche qualificate e un servizio di conservazione qualificato dei sigilli elettronici qualificati forniti in uno Stato membro sono riconosciuti rispettivamente quali servizio di conservazione qualificato delle firme elettroniche qualificate e servizio di conservazione qualificato dei sigilli elettronici qualificati in tutti gli altri Stati membri.

6. Una validazione temporale elettronica qualificata fornita in uno Stato membro è riconosciuta quale validazione temporale elettronica qualificata in tutti gli altri Stati membri.

7. Un certificato qualificato di autenticazione dei siti web rilasciato in uno Stato membro è riconosciuto quale certificato qualificato di autenticazione dei siti web in tutti gli altri Stati membri.

8. Un servizio elettronico di recapito certificato qualificato fornito in uno Stato membro è riconosciuto quale servizio elettronico di recapito certificato qualificato in tutti gli altri Stati membri.

9. Un attestato elettronico di attributi qualificato rilasciato in uno Stato membro è riconosciuto quale attestato elettronico di attributi qualificato in tutti gli altri Stati membri.

10. Un servizio di archiviazione elettronica qualificato fornito in uno Stato membro è riconosciuto quale servizio di archiviazione elettronica qualificato in tutti gli altri Stati membri.

▼M2

11. Un registro elettronico qualificato fornito in uno Stato membro è riconosciuto quale registro elettronico qualificato in tutti gli altri Stati membri.

▼B

SEZIONE 4

Firme elettroniche

Articolo 25

Effetti giuridici delle firme elettroniche

1. A una firma elettronica non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per firme elettroniche qualificate.

2. Una firma elettronica qualificata ha effetti giuridici equivalenti a quelli di una firma autografa.

▼M2

_____

▼B

Articolo 26

Requisiti di una firma elettronica avanzata

►M2 1. ◄ Una firma elettronica avanzata soddisfa i seguenti requisiti:

a) è connessa unicamente al firmatario;

b) è idonea a identificare il firmatario;

c) è creata mediante dati per la creazione di una firma elettronica che il firmatario può, con un elevato livello di sicurezza, utilizzare sotto il proprio esclusivo controllo; e

d) è collegata ai dati sottoscritti in modo da consentire l'identificazione di ogni successiva modifica di tali dati.

▼M2

2. Entro il 21 maggio 2026 la Commissione valuta la necessità di adottare atti di esecuzione per stabilire un elenco di norme di riferimento e, se necessario, stabilire specifiche e procedure applicabili alle firme elettroniche avanzate. Sulla base di tale valutazione, la Commissione può adottare tali atti di esecuzione. Si presume che i requisiti delle firme elettroniche avanzate siano stati rispettati ove una firma elettronica avanzata sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

Articolo 27

Firme elettroniche nei servizi pubblici

1. Se uno Stato membro richiede una firma elettronica avanzata per utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce le firme elettroniche avanzate, le firme elettroniche avanzate basate su un certificato qualificato

▼B

di firma elettronica e le firme elettroniche qualificate che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

2. Se uno Stato membro richiede una firma elettronica avanzata basata su un certificato qualificato per utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce le firme elettroniche avanzate basate su un certificato qualificato e le firme elettroniche qualificate che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

3. Gli Stati membri non richiedono, per un utilizzo transfrontaliero in un servizio online offerto da un organismo del settore pubblico, una firma elettronica dotata di un livello di garanzia di sicurezza più elevato di quello della firma elettronica qualificata.

▼M2

_____

▼B

5. Entro il 18 settembre 2015, e tenendo conto delle prassi, delle norme e degli atti giuridici dell'Unione vigenti, la Commissione, mediante atti di esecuzione, definisce i formati di riferimento delle firme elettroniche avanzate o i metodi di riferimento nel caso in cui siano utilizzati formati alternativi. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 28

Certificati qualificati di firme elettroniche

1. I certificati qualificati di firme elettroniche soddisfano i requisiti di cui all'allegato I.

2. I certificati qualificati di firme elettroniche non sono soggetti a requisiti obbligatori oltre ai requisiti di cui all'allegato I.

3. I certificati qualificati di firme elettroniche possono includere attributi specifici aggiuntivi non obbligatori. Tali attributi non pregiudicano l'interoperabilità e il riconoscimento delle firme elettroniche qualificate.

4. Qualora un certificato qualificato di firme elettroniche sia stato revocato dopo l'iniziale attivazione, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata in nessuna circostanza.

5. Fatte salve le condizioni seguenti, gli Stati membri possono fissare norme nazionali in merito alla sospensione temporanea di un certificato qualificato di firma elettronica:

a) in caso di temporanea sospensione di un certificato qualificato di firma elettronica, il certificato perde la sua validità per il periodo della sospensione;

b) il periodo di sospensione è indicato chiaramente nella banca dati dei certificati e la situazione di sospensione è visibile, durante il periodo di sospensione, dal servizio che fornisce le informazioni sulla situazione del certificato.

▼M2

6. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai certificati qualificati di firma elettronica. Si presume che i requisiti di cui all'allegato I siano stati rispettati ove un certificato qualificato di firma elettronica sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo2.

▼B

Articolo 29

Requisiti relativi ai dispositivi per la creazione di una firma elettronica qualificata

1. I dispositivi per la creazione di una firma elettronica qualificata soddisfano i requisiti di cui all'allegato II.

▼M2

1 *bis.* La generazione o la gestione dei dati per la creazione di una firma elettronica o la duplicazione dei dati per la creazione di tale firma a fini di back-up è effettuata solo per conto del firmatario, su richiesta del firmatario e da un prestatore di servizi fiduciari qualificato che presta un servizio fiduciario qualificato per la gestione di un dispositivo qualificato per la creazione di una firma elettronica a distanza.

▼B

2. La Commissione può, mediante atti di esecuzione, stabilire i numeri di riferimento delle norme applicabili ai dispositivi per la creazione di una firma elettronica qualificata. Si presume che i requisiti di cui all'allegato II siano stati rispettati ove un dispositivo per la creazione di una firma elettronica qualificata risponda a dette norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼M2

Articolo 29 bis

Requisiti relativi ai servizi qualificati per la gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza

1. La gestione di dispositivi qualificati per la creazione di una firma elettronica a distanza come servizio qualificato è effettuata solo da un prestatore di servizi fiduciari qualificato che:

a) genera o gestisce dati per la creazione di una firma elettronica per conto del firmatario;

b) fatto salvo l'allegato II, punto 1, lettera d), duplica i dati per la creazione di una firma elettronica solo a fini di back-up, a condizione che siano soddisfatti i requisiti seguenti:

   i) la sicurezza degli insiemi di dati duplicati deve essere dello stesso livello della sicurezza degli insiemi di dati originali;

   ii) il numero di insiemi di dati duplicati non deve eccedere il minimo necessario per garantire la continuità del servizio;

▼M2

c) soddisfa i requisiti indicati nella relazione di certificazione dello specifico dispositivo qualificato per la creazione di una firma elettronica a distanza, rilasciata a norma dell'articolo 30.

2. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, specifiche e procedure ai fini del paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

Articolo 30

Certificazione dei dispositivi per la creazione di una firma elettronica qualificata

1. La conformità dei dispositivi per la creazione di una firma elettronica qualificata con i requisiti stabiliti all'allegato II è certificata da appropriati organismi pubblici o privati designati dagli Stati membri.

2. Gli Stati membri notificano alla Commissione i nomi e gli indirizzi dell'organismo pubblico o privato di cui al paragrafo 1. La Commissione mette tali informazioni a disposizione degli Stati membri.

3. La certificazione di cui al paragrafo 1 si basa su uno dei seguenti elementi:

a) un processo di valutazione di sicurezza condotto conformemente a una delle norme per la valutazione di sicurezza dei prodotti informatici incluse nell'elenco redatto conformemente al secondo comma; o

b) un processo diverso da quello di cui alla lettera a), a condizione che utilizzi livelli di sicurezza comparabili e che l'organismo pubblico o privato di cui al paragrafo 1 notifichi tale processo alla Commissione. Detto processo può essere utilizzato solo in assenza delle norme di cui alla lettera a) ovvero quando è in corso un processo di valutazione di sicurezza di cui alla lettera a).

La Commissione adotta, mediante atti di esecuzione, un elenco di norme per la valutazione di sicurezza dei prodotti delle tecnologie dell'informazione di cui alla lettera a). Tali atti di esecuzione sono adottati secondo la procedura di esame di cui all'articolo 48, paragrafo 2.

▼M2

3*bis*. La validità di una certificazione di cui al paragrafo 1 non supera i cinque anni, a condizione che ogni due anni siano effettuate valutazioni delle vulnerabilità. Qualora siano individuate vulnerabilità a cui non è posto rimedio, la certificazione è annullata.

▼B

4. Alla Commissione è conferito il potere di adottare atti delegati conformemente all'articolo 47 riguardo alla fissazione di criteri specifici che gli organismi designati di cui al paragrafo 1 del presente articolo devono soddisfare.

▼B

Articolo 31

Pubblicazione di un elenco di dispositivi per la creazione di una firma elettronica qualificata certificati

1. Gli Stati membri notificano alla Commissione, senza indugio e in ogni caso non oltre un mese dopo la conclusione della certificazione, informazioni sui dispositivi per la creazione di una firma elettronica qualificata certificati dagli organismi di cui all'articolo 30, paragrafo 1. Essi notificano inoltre alla Commissione, senza indugio e in ogni caso non oltre un mese dopo la cancellazione della certificazione, informazioni sui dispositivi per la creazione di una firma elettronica che non sono più certificati.

2. Sulla base delle informazioni pervenutele, la Commissione redige, pubblica e mantiene un elenco di dispositivi per la creazione di una firma elettronica qualificata certificati.

▼M2

3. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce i formati e le procedure applicabili ai fini del paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

Articolo 32

Requisiti per la convalida delle firme elettroniche qualificate

1. Il processo di convalida di una firma elettronica qualificata conferma la validità di una firma elettronica qualificata purché:

a) il certificato associato alla firma fosse, al momento della firma, un certificato qualificato di firma elettronica conforme all'allegato I;

b) il certificato qualificato sia stato rilasciato da un prestatore di servizi fiduciari qualificato e fosse valido al momento della firma;

c) i dati di convalida della firma corrispondano ai dati trasmessi alla parte facente affidamento sulla certificazione;

d) l'insieme unico di dati che rappresenta il firmatario nel certificato sia correttamente trasmesso alla parte facente affidamento sulla certificazione;

e) l'impiego di un eventuale pseudonimo sia chiaramente indicato alla parte facente affidamento sulla certificazione, se uno pseudonimo era utilizzato al momento della firma;

f) la firma elettronica sia stata creata da un dispositivo per la creazione di una firma elettronica qualificata;

g) l'integrità dei dati firmati non sia stata compromessa;

h) i requisiti di cui all'articolo 26 fossero soddisfatti al momento della firma;

▼M2

Si presume che i requisiti di cui al primo comma del presente paragrafo siano stati rispettati ove la convalida delle firme elettroniche qualificate sia conforme alle norme, alle specifiche e alle procedure di cui al paragrafo 3

▼B

2. Il sistema utilizzato per convalidare la firma elettronica qualificata fornisce alla parte facente affidamento sulla certificazione il risultato corretto del processo di convalida e le consente di rilevare eventuali questioni attinenti alla sicurezza.

▼M2

3. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili alla convalida delle firme elettroniche qualificate. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 32 bis

Requisiti per la convalida delle firme elettroniche avanzate basate su certificati qualificati

1. Il processo di convalida di una firma elettronica avanzata basata su un certificato qualificato conferma la validità di una firma elettronica avanzata basata su un certificato qualificato a condizione che:

a) il certificato associato alla firma fosse, al momento della firma, un certificato qualificato di firma elettronica conforme all'allegato I;

b) il certificato qualificato sia stato rilasciato da un prestatore di servizi fiduciari qualificato e fosse valido al momento della firma;

c) i dati di convalida della firma corrispondano ai dati trasmessi alla parte facente affidamento sulla certificazione;

d) l'insieme unico di dati che rappresenta il firmatario nel certificato sia correttamente trasmesso alla parte facente affidamento sulla certificazione;

e) l'impiego di un eventuale pseudonimo sia chiaramente indicato alla parte facente affidamento sulla certificazione, se uno pseudonimo era stato utilizzato al momento della firma;

f) l'integrità dei dati firmati non sia stata compromessa;

g) i requisiti di cui all'articolo 26 fossero soddisfatti al momento della firma.

2. Il sistema utilizzato per convalidare la firma elettronica avanzata basata su un certificato qualificato fornisce alla parte facente affidamento sulla certificazione il risultato corretto del processo di convalida e le consente di rilevare eventuali problemi attinenti alla sicurezza.

3. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili alla convalida delle firme elettroniche avanzate basate su certificati qualificati. Si presume che i requisiti di cui al paragrafo 1 del presente articolo siano stati rispettati ove la convalida di una firma elettronica avanzata su certificati qualificati sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

Articolo 33

Servizio di convalida qualificato delle firme elettroniche qualificate

1. Un servizio di convalida qualificato delle firme elettroniche qualificate può essere prestato soltanto da un prestatore di servizi fiduciari qualificato che:

a) fornisce la convalida a norma dell'articolo 32, paragrafo 1; e

b) consente alle parti facenti affidamento sulla certificazione di ricevere il risultato del processo di convalida in un modo automatizzato che sia affidabile ed efficiente e rechi la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore del servizio di convalida qualificato.

▼M2

2. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili al servizio di convalida qualificato di cui al paragrafo 1 del presente articolo. Si presume che i requisiti di cui al paragrafo 1 del presente articolo siano stati rispettati ove il servizio di convalida qualificato delle firme elettroniche qualificate sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

Articolo 34

Servizio di conservazione qualificato delle firme elettroniche qualificate

1. Un servizio di conservazione qualificato delle firme elettroniche qualificate può essere prestato soltanto da un prestatore di servizi fiduciari qualificato che utilizza procedure e tecnologie in grado di estendere l'affidabilità della firma elettronica qualificata oltre il periodo di validità tecnologica.

▼M2

1 *bis.* Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove le modalità del servizio di conservazione qualificato delle firme elettroniche qualificate siano conformi alle norme, alle specifiche e alle procedure di cui al paragrafo 2.

2. Entro 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili al servizio di conservazione qualificato delle firme elettroniche qualificate. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

SEZIONE 5

Sigilli elettronici

Articolo 35

Effetti giuridici dei sigilli elettronici

1. A un sigillo elettronico non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i sigilli elettronici qualificati.

2. Un sigillo elettronico qualificato gode della presunzione di integrità dei dati e di correttezza dell'origine di quei dati a cui il sigillo elettronico qualificato è associato.

▼M2

_____

▼B

Articolo 36

Requisiti dei sigilli elettronici avanzati

►M2 1. ◄ Un sigillo elettronico avanzato soddisfa i seguenti requisiti:

a) è connesso unicamente al creatore del sigillo;

b) è idoneo a identificare il creatore del sigillo;

c) è creato mediante dati per la creazione di un sigillo elettronico che il creatore del sigillo elettronico può, con un elevato livello di sicurezza, usare sotto il proprio controllo per creare sigilli elettronici; e

d) è collegato ai dati cui si riferisce in modo da consentire l'identificazione di ogni successiva modifica di detti dati.

▼M2

2. Entro 21 maggio 2026 la Commissione valuta la necessità di adottare atti di esecuzione per stabilire un elenco di norme di riferimento e, se necessario, stabilire specifiche e procedure applicabili ai sigilli elettronici avanzati. Sulla base di tale valutazione, la Commissione può adottare tali atti di esecuzione. Si presume che i requisiti dei sigilli elettronici avanzati siano stati rispettati ove un sigillo elettronico avanzato sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

Articolo 37

Sigilli elettronici nei servizi pubblici

1. Se uno Stato membro richiede un sigillo elettronico avanzato per poter utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce i sigilli elettronici avanzati, i sigilli elettronici avanzati basati su un certificato qualificato di sigillo elettronico e i sigilli elettronici qualificati che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

▼B

2. Se uno Stato membro richiede un sigillo elettronico avanzato basato su un certificato qualificato per poter utilizzare i servizi online offerti da un organismo del settore pubblico, o per suo conto, tale Stato membro riconosce i sigilli elettronici avanzati basati su un certificato qualificato e i sigilli elettronici qualificati che almeno siano nei formati o utilizzino i metodi definiti negli atti di esecuzione di cui al paragrafo 5.

3. Gli Stati membri non richiedono, per l'utilizzo transfrontaliero in un servizio online offerto da un organismo del settore pubblico, un sigillo elettronico dotato di un livello di garanzia di sicurezza più elevato di quello del sigillo elettronico qualificato.

▼M2

_____

▼B

5. Entro il 18 settembre 2015, e tenendo conto delle prassi, delle norme e degli atti giuridici dell'Unione vigenti, la Commissione, mediante atti di esecuzione, definisce i formati di riferimento dei sigilli elettronici avanzati o i metodi di riferimento nel caso in cui siano utilizzati formati alternativi. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 38

Certificati qualificati di sigilli elettronici

1. I certificati qualificati di sigilli elettronici soddisfano i requisiti di cui all'allegato III.

2. I certificati qualificati di sigilli elettronici non sono soggetti a requisiti obbligatori oltre ai requisiti di cui all'allegato III.

3. I certificati qualificati di sigilli elettronici possono includere attributi specifici aggiuntivi non obbligatori. Tali attributi non pregiudicano l'interoperabilità e il riconoscimento dei sigilli elettronici qualificati.

4. Qualora un certificato qualificato di un sigillo elettronico sia stato revocato dopo l'iniziale attivazione, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata in nessuna circostanza.

5. Fatte salve le condizioni seguenti, gli Stati membri possono fissare norme nazionali in merito alla sospensione temporanea dei certificati qualificati di sigilli elettronici:

a) in caso di temporanea sospensione di un certificato qualificato di sigillo elettronico, il certificato perde la sua validità per il periodo della sospensione;

b) il periodo di sospensione è indicato chiaramente nella banca dati dei certificati e la situazione di sospensione è visibile, durante il periodo di sospensione, dal servizio che fornisce le informazioni sulla situazione del certificato.

▼M2

6. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai certificati qualificati dei sigilli elettronici. Si presume che i requisiti di cui all'allegato III siano stati rispettati ove un certificato qualificato di sigillo elettronico sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

Articolo 39

Dispositivi per la creazione di un sigillo elettronico qualificato

1. L'articolo 29 si applica mutatis mutandis ai requisiti per i dispositivi per la creazione di un sigillo elettronico qualificato.

2. L'articolo 30 si applica mutatis mutandis alla certificazione dei dispositivi per la creazione di un sigillo elettronico qualificato.

3. L'articolo 31 si applica mutatis mutandis alla pubblicazione di un elenco di dispositivi per la creazione di un sigillo elettronico qualificato certificati.

▼M2

Articolo 39 bis

Requisiti relativi ai servizi qualificati per la gestione di dispositivi qualificati per la creazione di un sigillo elettronico a distanza

L'articolo 29 bis si applica *mutatis mutandis* ai servizi qualificati per la gestione di dispositivi qualificati per la creazione di un sigillo elettronico a distanza.

▼B

Articolo 40

Convalida e conservazione dei sigilli elettronici qualificati

Gli articoli 32, 33 e 34 si applicano mutatis mutandis alla convalida e alla conservazione dei sigilli elettronici qualificati.

▼M2

Articolo 40 bis

Requisiti per la convalida dei sigilli elettronici avanzati basati su certificati qualificati

L'articolo 32 bis si applica *mutatis mutandis* alla convalida dei sigilli elettronici avanzati basati su certificati qualificati.

▼B

SEZIONE 6

Validazione temporale elettronica

Articolo 41

Effetti giuridici della validazione temporale elettronica

▼C1

1. Alla validazione temporale elettronica qualificata non possono essere negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti della validazione temporale elettronica qualificata.

2. Una validazione temporale elettronica qualificata gode della presunzione di accuratezza della data e dell'ora che indica e di integrità dei dati ai quali tale data e ora sono associate.

▼M2

———————

▼B

Articolo 42

Requisiti per la validazione temporale elettronica qualificata

1. Una validazione temporale elettronica qualificata soddisfa i requisiti seguenti:

a) collega la data e l'ora ai dati in modo da escludere ragionevolmente la possibilità di modifiche non rilevabili dei dati;

b) si basa su una fonte accurata di misurazione del tempo collegata al tempo universale coordinato; e

c) è apposta mediante una firma elettronica avanzata o sigillata con un sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato o mediante un metodo equivalente.

▼M2

1 *bis*. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il collegamento della data e dell'ora ai dati e l'accuratezza della fonte di misurazione del tempo siano conformi alle norme, alle specifiche e alle procedure di cui al paragrafo 2.

2. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili sia al collegamento della data e dell'ora ai dati sia alla determinazione dell'accuratezza delle fonti di misurazione del tempo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

SEZIONE 7

Servizi elettronici di recapito certificato

Articolo 43

Effetti giuridici di un servizio elettronico di recapito certificato

1. Ai dati inviati e ricevuti mediante un servizio elettronico di recapito certificato non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della loro forma elettronica o perché non soddisfano i requisiti del servizio elettronico di recapito certificato qualificato.

2. I dati inviati e ricevuti mediante servizio elettronico di recapito certificato qualificato godono della presunzione di integrità dei dati, dell'invio di tali dati da parte del mittente identificato, della loro ricezione da parte del destinatario identificato e di accuratezza della data e dell'ora dell'invio e della ricezione indicate dal servizio elettronico di recapito certificato qualificato.

Articolo 44

Requisiti per i servizi elettronici di recapito certificato qualificati

1. I servizi elettronici di recapito certificato qualificati soddisfano i requisiti seguenti:

▼B

a) sono forniti da uno o più prestatori di servizi fiduciari qualificati;

b) garantiscono con un elevato livello di sicurezza l'identificazione del mittente;

c) garantiscono l'identificazione del destinatario prima della trasmissione dei dati;

d) l'invio e la ricezione dei dati sono garantiti da una firma elettronica avanzata o da un sigillo elettronico avanzato di un prestatore di servizi fiduciari qualificato in modo da escludere la possibilità di modifiche non rilevabili dei dati;

e) qualsiasi modifica ai dati necessaria al fine di inviarli o riceverli è chiaramente indicata al mittente e al destinatario dei dati stessi;

f) la data e l'ora di invio e di ricezione e qualsiasi modifica dei dati sono indicate da una validazione temporale elettronica qualificata.

Qualora i dati siano trasferiti fra due o più prestatori di servizi fiduciari qualificati, i requisiti di cui alle lettere da a) a f) si applicano a tutti i prestatori di servizi fiduciari qualificati.

▼M2

1 *bis.* Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il processo di invio e ricezione dei dati sia conforme alle norme, alle specifiche e alle procedure di cui al paragrafo 2.

2. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai processi di invio e ricezione dei dati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

2 *bis.* I fornitori di servizi elettronici di recapito certificato qualificati possono concordare l'interoperabilità tra i servizi elettronici di recapito certificato qualificati che forniscono. Tale quadro di interoperabilità rispetta i requisiti di cui al paragrafo 1 e tale rispetto dei requisiti è confermato da un organismo di valutazione della conformità.

2 *ter.* La Commissione, mediante atti di esecuzione, può stabilire un elenco di norme di riferimento e, se necessario, può stabilire specifiche e procedure applicabili al quadro di interoperabilità di cui al paragrafo 2 bis del presente articolo. Le specifiche tecniche e il contenuto delle norme sono efficaci sotto il profilo dei costi e proporzionati. Gli atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

SEZIONE 8

Autenticazione dei siti web

▼M2

Articolo 45

Requisiti per i certificati qualificati di autenticazione di siti web

1. I certificati qualificati di autenticazione di siti web rispettano i requisiti di cui all'allegato IV. La valutazione del rispetto di tali requisiti è effettuata conformemente alle norme, alle specifiche e alle procedure di cui al paragrafo 2 del presente articolo.

1 *bis.* I certificati qualificati di autenticazione di siti web rilasciati conformemente al paragrafo 1 del presente articolo sono riconosciuti dai fornitori di browser web. I fornitori di browser web garantiscono che i dati di identità attestati nel certificato e gli attributi aggiuntivi attestati siano visualizzati in maniera tale da risultare facilmente consultabili. I fornitori di browser web garantiscono il supporto dei certificati qualificati di autenticazione di siti web di cui al paragrafo 1 del presente articolo e l'interoperabilità con gli stessi, a eccezione delle microimprese o piccole imprese quali definite all'articolo 2 dell'allegato alla raccomandazione 2003/361/CE della Commissione nel corso dei loro primi cinque anni di attività come prestatori di servizi di navigazione in rete.

1 *ter.* I certificati qualificati di autenticazione di siti web non sono soggetti a requisiti obbligatori diversi dai requisiti di cui al paragrafo 1.

2. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai certificati qualificati di autenticazione di siti web, di cui al paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 45 bis

Misure precauzionali in materia di cibersicurezza

1. I fornitori di browser web non adottano alcuna misura che sia in contrasto con i loro obblighi di cui all'articolo 45, in particolare con gli obblighi di riconoscere i certificati qualificati di autenticazione di siti web e di garantire che i dati di identità forniti siano visualizzati in maniera tale da risultare facilmente consultabili.

2. In deroga al paragrafo 1 e solo in caso di preoccupazioni fondate riguardanti violazioni della sicurezza o la perdita di integrità di un certificato o un insieme di certificati identificati, i fornitori di browser web possono adottare misure precauzionali in relazione a tale certificato o insieme di certificati.

3. Qualora adotti misure precauzionali a norma del paragrafo 2, il fornitore di browser web notifica per iscritto, senza indebito ritardo, le sue preoccupazioni, unitamente a una descrizione delle misure adottate per attenuare tali preoccupazioni, alla Commissione, all'organismo di vigilanza competente, al soggetto al quale è stato rilasciato il certificato

▼M2

e al prestatore di servizi fiduciari qualificato che ha rilasciato tale certificato o insieme di certificati. Al ricevimento di tale notifica, l'organismo di vigilanza competente rilascia un avviso di ricevimento al fornitore di browser web in questione.

4. L'organismo di vigilanza competente indaga sulle questioni sollevate nella notifica conformemente all'articolo 46 ter, paragrafo 4, lettera k). Se l'esito di tale esame non comporta la revoca della qualifica del certificato, l'organismo di vigilanza ne informa il fornitore di browser web e gli chiede di porre fine alle misure precauzionali di cui al paragrafo 2 del presente articolo.

SEZIONE 9

Attestati elettronici di attributi

Articolo 45 ter

Effetti giuridici degli attestati elettronici di attributi

1. A un attestato elettronico di attributi non vengono negati gli effetti giuridici né l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per gli attestati elettronici qualificati di attributi.

2. Un attestato elettronico di attributi qualificato e gli attestati di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto hanno gli stessi effetti giuridici degli attestati in formato cartaceo rilasciati legalmente.

3. Un attestato di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica in uno Stato membro, o per suo conto, è riconosciuto come un attestato di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto in tutti gli Stati membri.

Articolo 45 quater

Attestati elettronici di attributi nei servizi pubblici

Qualora il diritto nazionale richieda l'identificazione elettronica mediante un mezzo di identificazione e di autenticazione elettroniche per accedere a un servizio online prestato da un organismo del settore pubblico, i dati di identificazione personale contenuti nell'attestato elettronico di attributi non sostituiscono l'identificazione elettronica mediante mezzi di identificazione e autenticazione elettroniche finalizzati all'identificazione elettronica, a meno che ciò non sia specificamente consentito dallo Stato membro . In tal caso sono accettati anche gli attestati elettronici qualificati di attributi provenienti da altri Stati membri.

Articolo 45 quinquies

Requisiti per gli attestati elettronici qualificati di attributi

1. Gli attestati elettronici qualificati di attributi rispettano i requisiti di cui all'allegato V.

▼M2

2. La valutazione del rispetto dei requisiti di cui all'allegato V è effettuata conformemente alle norme, alle specifiche e alle procedure di cui al paragrafo 5 del presente articolo.

3. Gli attestati elettronici qualificati di attributi non sono soggetti a requisiti obbligatori oltre ai requisiti di cui all'allegato V.

4. Qualora un attestato elettronico di attributi qualificato sia stato revocato dopo l'iniziale rilascio, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata in nessuna circostanza.

5. Entro il 21 novembre 2024 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili agli attestati elettronici qualificati di attributi. Tali atti di esecuzione sono coerenti con gli atti di esecuzione di cui all'articolo 5 bis, paragrafo 23, relativi all'attuazione del portafoglio europeo di identità digitale. Essi sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 45 sexies

Verifica degli attributi rispetto a fonti autentiche

1. Entro 24 mesi dalla data di entrata in vigore degli atti di esecuzione di cui all'articolo 5 bis, paragrafo 23, e all'articolo 5 quater, paragrafo 6, gli Stati membri provvedono affinché, almeno per gli attributi elencati nell'allegato VI, qualora tali attributi facciano affidamento su fonti autentiche all'interno del settore pubblico, siano adottate misure volte a consentire ai prestatori di servizi fiduciari qualificati che forniscono attestati elettronici qualificati di attributi di verificare tali attributi mediante mezzi elettronici, su richiesta dell'utente, conformemente al diritto dell'Unione o nazionale.

2. Entro il 21 novembre 2024, tenendo conto delle pertinenti norme internazionali, la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili al catalogo di attributi, nonché i regimi per gli attestati di attributi e le procedure di verifica degli attestati elettronici qualificati di attributi ai fini del paragrafo 1 del presente articolo. Tali atti di esecuzione sono coerenti con gli atti di esecuzione di cui all'articolo 5 bis, paragrafo 23, relativi all'attuazione del portafoglio europeo di identità digitale. Sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 45 septies

Requisiti per gli attestati elettronici di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto

1. Un attestato elettronico di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto soddisfa i requisiti seguenti:

a) i requisiti di cui all'allegato VII;

▼M2

b) il certificato qualificato a supporto della firma elettronica qualificata o del sigillo elettronico qualificato dell'organismo del settore pubblico di cui all'articolo 3, punto 46, identificato come l'emittente di cui all'allegato VII, lettera b), contenente una serie specifica di attributi certificati in una forma adatta al trattamento automatizzato in cui:

i) si indica che l'organismo emittente è stabilito conformemente al diritto dell'Unione o nazionale come il responsabile della fonte autentica in base alla quale è rilasciato l'attestato elettronico di attributi oppure come l'organismo designato ad agire per suo conto;

ii) si fornisce un insieme di dati che rappresenta senza ambiguità la fonte autentica di cui al punto i); e

iii) si individua il diritto dell'Unione o nazionale di cui al punto i).

2. Lo Stato membro in cui sono stabiliti gli organismi del settore pubblico di cui all'articolo 3, punto 46, provvede affinché gli organismi del settore pubblico che rilasciano attestati elettronici di attributi soddisfino un livello di affidabilità e attendibilità equivalente a quello dei prestatori di servizi fiduciari qualificati conformemente all'articolo 24.

3. Gli Stati membri notificano alla Commissione gli organismi del settore pubblico di cui all'articolo 3, punto 46. Tale notifica comprende una relazione di valutazione della conformità rilasciata da un organismo di valutazione della conformità che conferma il rispetto dei requisiti di cui ai paragrafi 1, 2 e 6. La Commissione mette a disposizione del pubblico, attraverso un canale sicuro, l'elenco degli organismi del settore pubblico di cui all'articolo 3, punto 46, in forma firmata o sigillata elettronicamente e adatta al trattamento automatizzato.

4. Qualora un attestato elettronico di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto sia stato revocato dopo l'iniziale rilascio, esso decade della propria validità dal momento della revoca e la sua situazione non è ripristinata.

5. Un attestato elettronico di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto è considerato conforme ai requisiti di cui al paragrafo 1 se è conforme alle norme, alle specifiche e alle procedure di cui al paragrafo 6.

6. Entro 21 novembre 2024 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili agli attestati elettronici di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto. Tali atti di esecuzione sono coerenti con gli atti di esecuzione di cui all'articolo 5 bis, paragrafo 23, relativi all'attuazione del portafoglio europeo di identità digitale. Essi sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼M2

7. Entro il 21 novembre 2024 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai fini del paragrafo 3 del presente articolo. Tali atti di esecuzione sono coerenti con gli atti di esecuzione di cui all'articolo 5 bis, paragrafo 23, relativi all'attuazione del portafoglio europeo di identità digitale. Essi sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

8. Gli organismi del settore pubblico di cui all'articolo 3, punto 46, che rilasciano un attestato elettronico di attributi forniscono un'interfaccia con i portafogli europei di identità digitale forniti conformemente all'articolo 5 bis.

Articolo 45 octies

Rilascio di attestati elettronici di attributi ai portafogli europei di identità digitale

1. I fornitori di attestati elettronici di attributi offrono agli utenti dei portafogli europei di identità digitale la possibilità di richiedere, ottenere, conservare e gestire l'attestato elettronico di attributi indipendentemente dallo Stato membro in cui è fornito il portafoglio europeo di identità digitale.

2. I fornitori di attestati elettronici qualificati di attributi forniscono un'interfaccia con i portafogli europei di identità digitale forniti conformemente all'articolo 5 bis.

Articolo 45 nonies

Norme supplementari per la prestazione di servizi di attestazione elettronica di attributi

1. I prestatori di servizi di attestazione elettronica qualificata e non qualificata di attributi non combinano i dati personali relativi alla prestazione di tali servizi con i dati personali provenienti da qualsiasi altro servizio prestato da loro o dai loro partner commerciali.

2. I dati personali relativi alla prestazione di servizi di attestazione elettronica di attributi sono tenuti logicamente separati dagli altri dati detenuti dal fornitore di attestati elettronici di attributi.

3. I prestatori di servizi di attestazione elettronica qualificata di attributi attuano la prestazione di tali servizi fiduciari qualificati in modo funzionalmente separato dagli altri servizi da essi prestati.

SEZIONE 10

Servizi di archiviazione elettronica

Articolo 45 decies

Effetti giuridici dei servizi di archiviazione elettronica

1. Ai dati elettronici e ai documenti elettronici conservati mediante un servizio di archiviazione elettronica non vengono negati gli effetti

▼M2

giuridici né l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della loro forma elettronica o perché non sono conservati mediante un servizio di archiviazione elettronica qualificato.

2. I dati elettronici e i documenti elettronici conservati mediante un servizio di archiviazione elettronica qualificato godono della 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.

Articolo 45 undecies

Requisiti per i servizi di archiviazione elettronica qualificati

1. I servizi di archiviazione elettronica qualificati soddisfano i requisiti seguenti:

a) sono forniti da prestatori di servizi fiduciari qualificati;

b) utilizzano procedure e tecnologie in grado di garantire la durabilità e la leggibilità dei dati elettronici e dei documenti elettronici oltre il periodo di validità tecnologica e almeno per tutto il periodo di conservazione legale o contrattuale, preservandone nel contempo l'integrità e l'esattezza dell'origine;

c) assicurano che tali dati elettronici e tali documenti elettronici siano conservati in modo tale da essere protetti dal rischio di perdita e alterazione, ad eccezione delle modifiche riguardanti il loro supporto o il loro formato elettronico;

d) consentono alle parti autorizzate facenti affidamento sulla certificazione di ricevere una relazione in un modo automatizzato in cui si conferma che i dati elettronici e i documenti elettronici consultati da un archivio elettronico qualificato godono della presunzione di integrità dei dati dall'inizio del periodo di conservazione fino al momento della consultazione.

La relazione di cui alla lettera d) del primo comma è fornita in modo affidabile ed efficiente e reca la firma elettronica qualificata o il sigillo elettronico qualificato del prestatore del servizio di archiviazione elettronica qualificato.

2. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai servizi di archiviazione elettronica qualificati. Si presume che i requisiti dei servizi di archiviazione elettronica qualificati siano rispettati ove un servizio di archiviazione elettronica qualificato sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

SEZIONE 11

Registri elettronici

Articolo 45 duodecies

Effetti giuridici dei registri elettronici

1. A un registro elettronico non sono negati gli effetti giuridici né l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della sua forma elettronica o perché non soddisfa i requisiti per i registri elettronici qualificati.

▼M2

2. Le registrazioni di dati contenute in un registro elettronico qualificato godono della presunzione del loro ordine cronologico sequenziale univoco e accurato e della loro integrità.

Articolo 45 terdecies

Requisiti per i registri elettronici qualificati

1. I registri elettronici qualificati soddisfano i requisiti seguenti:

a) sono creati e gestiti da uno o più prestatori di servizi fiduciari qualificati;

b) stabiliscono l'origine delle registrazioni di dati nel registro;

c) garantiscono l'ordine cronologico sequenziale univoco delle registrazioni di dati nel registro;

d) registrano i dati in modo tale che sia possibile individuare immediatamente qualsiasi successiva modifica degli stessi, garantendone l'integrità nel tempo.

2. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove un registro elettronico sia conforme alle norme, alle specifiche e alle procedure di cui al paragrafo 3.

3. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai requisiti di cui al paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

CAPO IV

DOCUMENTI ELETTRONICI

Articolo 46

Effetti giuridici dei documenti elettronici

A un documento elettronico non sono negati gli effetti giuridici e l'ammissibilità come prova in procedimenti giudiziali per il solo motivo della sua forma elettronica.

▼M2

CAPO IV *bis*

QUADRO DI GOVERNANCE

Articolo 46 bis

Vigilanza sul quadro relativo al portafoglio europeo di identità digitale

1. Gli Stati membri designano uno o più organismi di vigilanza stabiliti nel loro territorio.

Agli organismi di vigilanza designati a norma del primo comma sono conferiti i poteri necessari e le risorse adeguate per l'esercizio dei loro compiti in modo efficace, efficiente e indipendente.

▼M2

2. Gli Stati membri notificano alla Commissione i nomi e gli indirizzi dei loro organismi di vigilanza designati a norma del paragrafo 1 e qualsiasi successiva modifica degli stessi. La Commissione pubblica un elenco degli organismi di vigilanza notificati.

3. Il ruolo degli organismi di vigilanza designati a norma del paragrafo 1 è il seguente:

a) vigilare sui fornitori di portafogli europei di identità digitale stabiliti nello Stato membro designante e assicurarsi, mediante attività di vigilanza ex ante e ex post, che tali fornitori e i portafogli europei di identità digitale da essi forniti rispondano ai requisiti di cui al presente regolamento;

b) intervenire, se necessario, in relazione ai fornitori di portafogli europei di identità digitale stabiliti nel territorio dello Stato membro designante, mediante attività di vigilanza ex post, qualora siano informati che i fornitori o i portafogli europei di identità digitale da essi forniti violano il presente regolamento.

4. I compiti degli organismi di vigilanza designati a norma del paragrafo 1 comprendono, in particolare, i seguenti:

a) cooperare con altri organismi di vigilanza e assisterli a norma degli articoli 46 quater e 46 sexies;

b) chiedere le informazioni necessarie per monitorare la conformità al presente regolamento;

c) informare le pertinenti autorità competenti degli Stati membri interessati, designate o istituite a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555, in merito a violazioni significative della sicurezza o a perdite di integrità di cui vengono a conoscenza nello svolgimento dei loro compiti e, in caso di violazione significativa della sicurezza o di perdita di integrità che riguarda altri Stati membri, informare il punto di contatto unico dello Stato membro interessato, designato o istituito a norma dell'articolo 8, paragrafo 3, della direttiva (UE) 2022/2555, e i punti di contatto unici degli altri Stati membri interessati, designati a norma dell'articolo 46 quater, paragrafo 1, del presente regolamento, nonché informare il pubblico o imporre al fornitore del portafoglio europeo di identità digitale di farlo, ove l'organismo di vigilanza accerti che la divulgazione della violazione della sicurezza o della perdita di integrità sia nell'interesse pubblico;

d) effettuare ispezioni in loco e supervisione a distanza;

e) imporre ai fornitori di portafogli europei di identità digitale di rimediare a qualsiasi mancato soddisfacimento dei requisiti di cui al presente regolamento;

f) sospendere o cancellare la registrazione e l'inclusione delle parti facenti affidamento sulla certificazione nel meccanismo di cui all'articolo 5 ter, paragrafo 7, in caso di uso illecito o fraudolento del portafoglio europeo di identità digitale;

g) cooperare con le competenti autorità di controllo istituite a norma dell'articolo 51 del regolamento (UE) 2016/679, in particolare informandole senza indebito ritardo laddove siano state rilevate violazioni delle norme in materia di protezione dei dati personali e in merito alle violazioni della sicurezza che sembrano costituire violazioni dei dati personali.

▼M2

5. Qualora chieda al fornitore di un portafoglio europeo di identità digitale di rimediare a qualsiasi mancato soddisfacimento dei requisiti ai sensi del presente regolamento a norma del paragrafo 4, lettera d), e tale fornitore non agisca di conseguenza e, se del caso, entro un termine stabilito dall'organismo di vigilanza designato a norma del paragrafo 1, quest'ultimo, tenendo conto in particolare della portata, della durata e delle conseguenze di tale inadempienza, può imporre al fornitore di sospendere o cessare la fornitura del portafoglio europeo di identità digitale. L'organismo di vigilanza informa senza indebito ritardo gli organismi di vigilanza di altri Stati membri, la Commissione, le parti facenti affidamento sulla certificazione e gli utenti del portafoglio europeo di identità digitale della decisione di richiedere la sospensione o la cessazione della fornitura del portafoglio europeo di identità digitale.

6. Entro il 31 marzo di ogni anno ciascun organismo di vigilanza designato a norma del paragrafo 1 presenta alla Commissione una relazione sulle sue principali attività del precedente anno civile. La Commissione mette tali relazioni annuali a disposizione del Parlamento europeo e del Consiglio.

7. Entro 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce i formati e le procedure applicabili alla relazione di cui al paragrafo 6 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 46 ter

Vigilanza dei servizi fiduciari

1. Gli Stati membri designano un organismo di vigilanza istituito nel loro territorio o designano, di comune accordo con un altro Stato membro, un organismo di vigilanza stabilito in tale altro Stato membro. Tale organismo di vigilanza è responsabile di compiti di vigilanza nello Stato membro designante per quanto riguarda i servizi fiduciari.

Agli organismi di vigilanza designati a norma del primo comma sono conferiti i poteri necessari e le risorse adeguate per l'esercizio dei loro compiti.

2. Gli Stati membri notificano alla Commissione i nomi e gli indirizzi degli organismi di vigilanza designati a norma del paragrafo 1 e qualsiasi successiva modifica degli stessi. La Commissione pubblica un elenco degli organismi di vigilanza notificati.

3. Il ruolo degli organismi di vigilanza designati a norma del paragrafo 1 è il seguente:

a) vigilare sui prestatori di servizi fiduciari qualificati stabiliti nel territorio dello Stato membro designante e assicurarsi, mediante attività di vigilanza *ex ante* e *ex post*, che essi e i servizi fiduciari qualificati da essi prestati rispondano ai requisiti di cui al presente regolamento;

b) adottare misure, ove necessario, in relazione a prestatori di servizi fiduciari non qualificati stabiliti nel territorio dello Stato membro designante, mediante attività di vigilanza ex post, qualora siano informati che tali prestatori di servizi fiduciari non qualificati o i servizi fiduciari da essi prestati presumibilmente non soddisfano i requisiti stabiliti dal presente regolamento.

▼M2

4. I compiti dell'organismo di vigilanza designato a norma del paragrafo 1 comprendono, in particolare, i seguenti:

a) informare le pertinenti autorità competenti degli Stati membri interessati, designate o istituite a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555, in merito a violazioni significative della sicurezza o a perdite di integrità di cui venga a conoscenza nello svolgimento dei suoi compiti e, in caso di violazione significativa della sicurezza o di perdita di integrità che riguarda altri Stati membri, informare il punto di contatto unico dello Stato membro interessato, designato o istituito a norma dell'articolo 8, paragrafo 3, della direttiva (UE) 2022/2555, e i punti di contatto unici degli altri Stati membri interessati, designati a norma dell'articolo 46 quater, paragrafo 1, del presente regolamento, nonché informare il pubblico o imporre al prestatore di servizi fiduciari di farlo, ove l'organismo di vigilanza accerti che la divulgazione della violazione della sicurezza o della perdita di integrità sia nell'interesse pubblico;

b) cooperare con altri organismi di vigilanza e assisterli a norma degli articoli 46 quater e 46 sexies;

c) analizzare le relazioni di valutazione della conformità di cui all'articolo 20, paragrafo 1, e all'articolo 21, paragrafo 1;

d) riferire alla Commissione in merito alle sue principali attività a norma del paragrafo 6 del presente articolo;

e) svolgere verifiche o chiedere a un organismo di valutazione della conformità di effettuare una valutazione di conformità dei prestatori di servizi fiduciari qualificati a norma dell'articolo 20, paragrafo 2;

f) cooperare con le competenti autorità di controllo istituite a norma dell'articolo 51 del regolamento (UE) 2016/679, in particolare informandole senza indebito ritardo laddove siano state rilevate violazioni delle norme in materia di protezione dei dati personali e in merito alle violazioni della sicurezza che sembrano costituire violazioni dei dati personali;

g) concedere la qualifica ai prestatori di servizi fiduciari e ai servizi da essi prestati e revocare tale qualifica a norma degli articoli 20 e 21;

h) informare l'organismo responsabile dell'elenco nazionale di fiducia di cui all'articolo 22, paragrafo 3, in merito alle proprie decisioni di concedere o revocare la qualifica, salvo se tale organismo è anche l'organismo di vigilanza designato a norma del paragrafo 1 del presente articolo;

i) verificare l'esistenza e la corretta applicazione delle disposizioni sui piani di cessazione qualora il prestatore di servizi fiduciari qualificato cessi le sue attività, inclusi i modi in cui le informazioni sono mantenute accessibili a norma dell'articolo 24, paragrafo 2, lettera h);

j) imporre ai prestatori di servizi fiduciari di rimediare a qualsiasi mancato soddisfacimento dei requisiti di cui al presente regolamento;

▼M2

k) indagare sulle dichiarazioni presentate dai fornitori di browser web a norma dell'articolo 45 bis e intervenire se necessario.

5. Gli Stati membri possono imporre che l'organismo di vigilanza designato a norma del paragrafo 1 istituisca, mantenga e aggiorni un'infrastruttura fiduciaria conformemente al diritto nazionale.

6. Entro il 31 marzo di ogni anno ciascun organismo di vigilanza designato a norma del paragrafo 1 presenta alla Commissione una relazione sulle sue principali attività del precedente anno civile. La Commissione mette tali relazioni annuali a disposizione del Parlamento europeo e del Consiglio.

7. Entro il 21 maggio 2025 la Commissione adotta orientamenti sull'esercizio, da parte degli organismi di vigilanza designati a norma del paragrafo 1 del presente articolo, dei compiti di cui al paragrafo 4 del presente articolo e, mediante atti di esecuzione, stabilisce i formati e le procedure applicabili alla relazione di cui al paragrafo 6 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 46 quater

Punti di contatto unici

1. Ciascuno Stato membro designa un punto di contatto unico per i servizi fiduciari, i portafogli europei di identità digitale e i regimi di identificazione elettronica notificati.

2. Ciascun punto di contatto unico svolge una funzione di collegamento per agevolare la cooperazione transfrontaliera tra gli organismi di vigilanza per i prestatori di servizi fiduciari e tra gli organismi di vigilanza per i fornitori dei portafogli europei di identità digitale e, se del caso, con la Commissione e l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) nonché con altre autorità competenti all'interno del rispettivo Stato membro.

3. Ciascuno Stato membro rende pubblici e, senza indebito ritardo, notifica alla Commissione i nomi e gli indirizzi del punto di contatto unico designato a norma del paragrafo 1 e qualsiasi successiva modifica degli stessi.

4. La Commissione pubblica un elenco dei punti di contatto unici notificati a norma del paragrafo 3.

Articolo 46 quinquies

Assistenza reciproca

1. Per agevolare la vigilanza e l'esecuzione degli obblighi ai sensi del presente regolamento, gli organismi di vigilanza designati a norma dell'articolo 46 bis, paragrafo 1, e dell'articolo 46 ter, paragrafo 1, possono chiedere, anche attraverso il gruppo di cooperazione istituito a norma dell'articolo 46 sexies, paragrafo 1, assistenza reciproca agli organismi di vigilanza di un altro Stato membro nel quale è stabilito il fornitore del portafoglio europeo di identità digitale o il prestatore di servizi fiduciari o nel quale sono ubicati i suoi sistemi informativi e di rete o sono prestati i suoi servizi.

2. L'assistenza reciproca implica almeno quanto segue:

▼M2

a) l'organismo di vigilanza che applica misure di vigilanza e di esecuzione in uno Stato membro informa e consulta l'organismo di vigilanza dell'altro Stato membro interessato;

b) un organismo di vigilanza può chiedere all'organismo di vigilanza di un altro Stato membro interessato di adottare misure di vigilanza o di esecuzione, anche, per esempio, mediante richieste di effettuare ispezioni connesse alle relazioni di valutazione della conformità di cui agli articoli 20 e 21 per quanto riguarda la prestazione di servizi fiduciari;

c) se del caso, gli organismi di vigilanza possono svolgere indagini congiunte con gli organismi di vigilanza di altri Stati membri.

Le disposizioni e le procedure per le indagini congiunte di cui al primo comma, sono convenute e stabilite dagli Stati membri interessati conformemente al rispettivo diritto nazionale.

3. L'organismo di vigilanza cui è presentata una richiesta di assistenza può rifiutare tale richiesta per uno dei seguenti motivi:

a) l'assistenza richiesta non è proporzionata alle attività di vigilanza dell'organismo di vigilanza svolte a norma degli articoli 46 bis e 46 ter;

b) l'organismo di vigilanza non è competente a fornire l'assistenza richiesta;

c) fornire l'assistenza richiesta sarebbe incompatibile con il presente regolamento.

4. Entro il 21 maggio 2025, e successivamente ogni due anni, il gruppo di cooperazione istituito a norma dell'articolo 46 sexies, paragrafo 1, emana orientamenti sugli aspetti organizzativi e sulle procedure relativi all'assistenza reciproca di cui ai paragrafi 1 e 2 del presente articolo.

Articolo 46 sexies

Gruppo di cooperazione per l'identità digitale europea

1. Per sostenere e agevolare la cooperazione transfrontaliera e lo scambio di informazioni tra gli Stati membri in materia di servizi fiduciari, portafogli europei di identità digitale e regimi di identificazione elettronica notificati, la Commissione istituisce un gruppo di cooperazione per l'identità digitale europea («gruppo di cooperazione»).

2. Il gruppo di cooperazione si compone di rappresentanti nominati dagli Stati membri e rappresentanti della Commissione. Il gruppo di cooperazione è presieduto dalla Commissione. La Commissione provvede alle funzioni di segretariato del gruppo di cooperazione.

3. Rappresentanti dei pertinenti portatori di interessi possono essere invitati, ad hoc, ad assistere alle riunioni del gruppo di cooperazione e a partecipare ai suoi lavori in qualità di osservatori.

4. L'ENISA è invitata a partecipare in qualità di osservatore ai lavori del gruppo di cooperazione quando esso procede a scambi di opinioni, migliori pratiche e informazioni su aspetti pertinenti in materia di cibersicurezza, quali la notifica delle violazioni di sicurezza, e quando si tratta dell'uso dei certificati o delle norme di cibersicurezza.

5. Il gruppo di cooperazione svolge i compiti seguenti:

▼M2

a) scambia consulenze e coopera con la Commissione in materia di iniziative strategiche emergenti nel settore dei portafogli di identità digitale, dei mezzi di identificazione elettronica e dei servizi fiduciari;

b) fornisce consulenza alla Commissione, se del caso, nella fase precoce dell'elaborazione di progetti di atti delegati e di atti esecuzione da adottare a norma del presente regolamento;

c) al fine di sostenere gli organismi di vigilanza nell'attuazione delle disposizioni del presente regolamento:

   i) scambia migliori pratiche e informazioni sull'attuazione delle disposizioni del presente regolamento;

   ii) valuta i pertinenti sviluppi nei settori del portafoglio di identità digitale, dell'identificazione elettronica e dei servizi fiduciari;

   iii) organizza riunioni congiunte con le pertinenti parti interessate di tutta l'Unione per discutere delle attività svolte dal gruppo di cooperazione e raccoglie contributi sulle sfide strategiche emergenti;

   iv) con il sostegno dell'ENISA, scambia opinioni, migliori pratiche e informazioni su questioni pertinenti in materia di cibersicurezza in relazioni ai portafogli europei di identità digitale, ai regimi di identificazione elettronica e ai servizi fiduciari;

   v) scambia migliori pratiche in relazione allo sviluppo e all'attuazione di politiche in materia di notifica delle violazioni della sicurezza e misure comuni di cui agli articoli 5 sexies e 10;

   vi) organizza riunioni congiunte con il gruppo di cooperazione NIS istituito a norma dell'articolo 14, paragrafo 1, della direttiva (UE) 2022/2555 per scambiare informazioni pertinenti in relazione a minacce informatiche, incidenti e vulnerabilità associati ai servizi fiduciari e all'identificazione elettronica, iniziative di sensibilizzazione, formazioni, esercitazioni e competenze, sviluppo delle capacità, capacità in materia di norme e specifiche tecniche, nonché norme e specifiche tecniche;

   vii) discute, su richiesta di un organismo di vigilanza, delle richieste specifiche di assistenza reciproca di cui all'articolo 46 quinquies;

   viii) facilita lo scambio di informazioni tra gli organismi di vigilanza fornendo orientamenti sugli aspetti organizzativi e sulle procedure per l'assistenza reciproca di cui all'articolo 46 quinquies;

d) organizza valutazioni tra pari dei regimi di identificazione elettronica da notificare ai sensi del presente regolamento.

6. Gli Stati membri garantiscono la collaborazione effettiva ed efficiente dei rispettivi rappresentanti designati nel gruppo di cooperazione.

▼M2

7. Entro il 21 maggio 2025 la Commissione, mediante atti di esecuzione, stabilisce le modalità procedurali necessarie per facilitare la cooperazione tra gli Stati membri di cui al paragrafo 5, lettera d), del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

▼B

CAPO V

DELEGA DI POTERE E DISPOSIZIONI DI ESECUZIONE

Articolo 47

Esercizio della delega

1. Il potere di adottare atti delegati è conferito alla Commissione alle condizioni stabilite nel presente articolo.

▼M2
▼C2

2. Il potere di adottare gli atti delegati di cui all'articolo 5 *quater*, paragrafo 8, all'articolo 24, paragrafo 4 *ter*, e all'articolo 30, paragrafo 4, è conferito alla Commissione per un periodo indeterminato a decorrere dal 17 settembre 2014.

3. La delega di potere di cui all'articolo 5 *quater*, paragrafo 8, all'articolo 24, paragrafo 4 *ter*, e all'articolo 30, paragrafo 4, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.

▼B

4. Non appena adotta un atto delegato, la Commissione ne dà contestualmente notifica al Parlamento europeo e al Consiglio.

▼M2
▼C2

5. L'atto delegato adottato ai sensi dell'articolo 5 *quater*, paragrafo 8, dell'articolo 24, paragrafo 4 ter, o dell'articolo 30, paragrafo 4, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.

▼B

Articolo 48

Procedura di comitato

1. La Commissione è assistita da un comitato. Esso è un comitato ai sensi del regolamento (UE) n. 182/2011.

2. Nei casi in cui è fatto riferimento al presente paragrafo, si applica l'articolo 5 del regolamento (UE) n. 182/2011.

▼B

CAPO VI

DISPOSIZIONI FINALI

▼M2

Articolo 48 bis

Obblighi di comunicazione

1. Gli Stati membri provvedono affinché siano raccolte statistiche relative al funzionamento dei portafogli europei di identità digitale e dei servizi fiduciari qualificati forniti nei rispettivi territori.

2. Le statistiche raccolte conformemente al paragrafo 1 comprendono:

a) il numero di persone fisiche e giuridiche in possesso di un portafoglio europeo di identità digitale valido;

b) il numero e il tipo di servizi che accettano l'uso dei portafogli europei di identità digitale;

c) il numero di reclami presentati dagli utenti e di incidenti relativi alla protezione dei consumatori o dei dati relativi alle parti facenti affidamento sulla certificazione e ai servizi fiduciari qualificati;

d) una relazione di sintesi che include dati riguardanti gli incidenti che impediscono l'uso dei portafogli europei di identità digitale;

e) una sintesi degli incidenti di sicurezza significativi, delle violazioni dei dati e degli utenti interessati dei portafogli europei di identità digitale o dei servizi fiduciari qualificati.

3. Le statistiche di cui al paragrafo 2 sono messe a disposizione del pubblico in un formato aperto, di uso comune e leggibile meccanicamente.

4. Entro il 31 marzo di ogni anno gli Stati membri presentano alla Commissione una relazione sulle statistiche raccolte conformemente al paragrafo 2.

Articolo 49

Riesame

1. La Commissione riesamina l'applicazione del presente regolamento e presenta, entro 21 maggio 2026, una relazione in proposito al Parlamento europeo e al Consiglio. In tale relazione, in particolare, la Commissione valuta se sia opportuno modificare l'ambito di applicazione del presente regolamento o sue disposizioni specifiche, comprese, segnatamente, le disposizioni di cui all'articolo 5 quater, paragrafo 5, tenendo conto dell'esperienza acquisita nell'applicazione del regolamento stesso e dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi giuridici. Se necessario, tale relazione è corredata di una proposta di modifica del presente regolamento.

2. La relazione di cui al paragrafo 1 comprende una valutazione della disponibilità, della sicurezza e dell'utilizzabilità dei mezzi di identificazione elettronica notificati e dei passaporti europei di identità digitale che rientrano nell'ambito di applicazione del presente regolamento, ed esamina se sia necessario imporre a tutti i prestatori di

▼M2

servizi privati online che fanno affidamento su servizi di identificazione elettronica di terzi per l'autenticazione degli utenti di accettare l'utilizzo di mezzi di identificazione elettronica notificati e del portafoglio europeo di identità digitale.

3. Entro 21 maggio 2030, e successivamente ogni quattro anni, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sui progressi compiuti nella realizzazione degli obiettivi del presente regolamento.

▼B

Articolo 50

Abrogazione

1. La direttiva 1999/93/CEE è abrogata con effetto dal 1º luglio 2016.

2. I riferimenti alla direttiva abrogata si intendono fatti al presente regolamento.

▼M2

Articolo 51

Misure transitorie

1. I dispositivi per la creazione di una firma sicura la cui conformità sia stata determinata conformemente all'articolo 3, paragrafo 4, della direttiva 1999/93/CE continuano a essere considerati dispositivi qualificati per la creazione di una firma elettronica a norma del presente regolamento fino al 21 maggio 2027.

2. I certificati qualificati rilasciati a persone fisiche a norma della direttiva 1999/93/CE continuano a essere considerati certificati qualificati di firme elettroniche a norma del presente regolamento fino al 21 maggio 2026.

3. La gestione di dispositivi qualificati per la creazione di una firma elettronica e di sigilli elettronici a distanza da parte di prestatori di servizi fiduciari qualificati diversi dai prestatori di servizi fiduciari qualificati che forniscono servizi fiduciari qualificati per la gestione di dispositivi qualificati per la creazione di una firma e di un sigillo elettronici a distanza conformemente agli articoli 29 bis e 39 bis può essere effettuata senza la necessità di ottenere la qualifica per la prestazione di tali servizi di gestione fino al 21 maggio 2026.

4. I prestatori di servizi fiduciari qualificati cui è stata assegnata la qualifica a norma del presente regolamento prima del 20 maggio 2024 presentano all'organismo di vigilanza una relazione di valutazione della conformità che attesti il rispetto dell'articolo 24, paragrafi 1, 1 bis e 1 ter, quanto prima e comunque entro il 21 maggio 2026.

▼B

Articolo 52

Entrata in vigore

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

2. Il presente regolamento si applica a decorrere dal 1º luglio 2016, a eccezione delle seguenti disposizioni:

▼B

a) articolo 8, paragrafo 3, articolo 9, paragrafo 5, articolo 12, paragrafi da 2 a 9, articolo 17, paragrafo 8, articolo 19, paragrafo 4, articolo 20, paragrafo 4, articolo 21, paragrafo 4, articolo 22, paragrafo 5, articolo 23, paragrafo 3, articolo 24, paragrafo 5, articolo 27, paragrafi 4 e 5, articolo 28, paragrafo 6, articolo 29, paragrafo 2, articolo 30, paragrafi 3 e 4, articolo 31, paragrafo 3, articolo 32, paragrafo 3, articolo 33, paragrafo 2, articolo 34, paragrafo 2, articolo 37, paragrafi 4 e 5, articolo 38, paragrafo 6, articolo 42, paragrafo 2, articolo 44, paragrafo 2, articolo 45, paragrafo 2, articolo 47 e articolo 48, che si applicano dal 17 settembre 2014;

b) l'articolo 7, l'articolo 8, paragrafi 1 e 2, gli articoli 9, 10, 11 e l'articolo 12, paragrafo 1, si applicano a decorrere dalla data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3, e all'articolo 12, paragrafo 8;

c) l'articolo 6 si applica a decorrere da tre anni dalla data di applicazione degli atti di esecuzione di cui all'articolo 8, paragrafo 3, e all'articolo 12, paragrafo 8.

3. Quando il regime di identificazione elettronica notificato è compreso nell'elenco pubblicato dalla Commissione ai sensi dell'articolo 9 prima della data di cui al paragrafo 2, lettera c), del presente articolo, il riconoscimento dei mezzi di identificazione elettronica in virtù di tale regime ai sensi dell'articolo 6 ha luogo non oltre 12 mesi dopo la pubblicazione di detto regime ma non prima della data di cui al paragrafo 2, lettera c), del presente articolo.

4. Nonostante il paragrafo 2, lettera c), del presente articolo, uno Stato membro può decidere che i mezzi di identificazione elettronica a norma del regime di identificazione elettronica notificato ai sensi dell'articolo 9, paragrafo 1, da un altro Stato membro, siano riconosciuti nel primo Stato membro a decorrere dalla data di pubblicazione degli atti di esecuzione di cui agli articoli 8, paragrafo 3, e 12, paragrafo 8. Gli Stati membri interessati ne informano la Commissione. La Commissione rende pubbliche tali informazioni.

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

▼B

ALLEGATO I

REQUISITI PER I CERTIFICATI QUALIFICATI DI FIRMA ELETTRONICA

I certificati qualificati di firma elettronica contengono:

a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di firma elettronica;

b) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e

   — per una persona giuridica: il nome e, se del caso, il numero di registrazione quali figurano nei documenti ufficiali,

   — per una persona fisica: il nome della persona;

c) è chiaramente indicato almeno il nome del firmatario, o uno pseudonimo, qualora sia usato uno pseudonimo;

d) i dati di convalida della firma elettronica che corrispondono ai dati per la creazione di una firma elettronica;

e) l'indicazione dell'inizio e della fine del periodo di validità del certificato;

f) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;

g) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;

h) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera g) è disponibile gratuitamente;

▼M2

i) le informazioni relative alla validità del certificato qualificato o l'ubicazione dei servizi cui è possibile rivolgersi per informarsi in merito;

▼B

j) qualora i dati per la creazione di una firma elettronica connessi ai dati di convalida della firma elettronica siano ubicati in un dispositivo per la creazione di una firma elettronica qualificata, un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento automatizzato.

▼B

ALLEGATO II

REQUISITI PER I DISPOSITIVI PER LA CREAZIONE DI UNA FIRMA ELETTRONICA QUALIFICATA

1. I dispositivi per la creazione di una firma elettronica qualificata garantiscono, mediante mezzi tecnici e procedurali appropriati, almeno quanto segue:

   a) è ragionevolmente assicurata la riservatezza dei dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica;

   b) i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica possono comparire in pratica una sola volta;

   c) i dati per la creazione di una firma elettronica utilizzati per creare una firma elettronica non possono, con un grado ragionevole di sicurezza, essere derivati e la firma elettronica è attendibilmente protetta da contraffazioni compiute con l'impiego di tecnologie attualmente disponibili;

   d) i dati per la creazione di una firma elettronica utilizzati nella creazione della stessa possono essere attendibilmente protetti dal firmatario legittimo contro l'uso da parte di terzi.

2. I dispositivi per la creazione di una firma elettronica qualificata non alterano i dati da firmare né impediscono che tali dati siano presentati al firmatario prima della firma.

▼M2

_____

▼B

ALLEGATO III

REQUISITI PER I CERTIFICATI QUALIFICATI DEI SIGILLI ELETTRONICI

I certificati qualificati dei sigilli elettronici contengono:

a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di sigillo elettronico;

b) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e

   — per una persona giuridica: il nome e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali,

   — per una persona fisica: il nome della persona;

c) almeno il nome del creatore del sigillo e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;

d) i dati di convalida del sigillo elettronico che corrispondono ai dati per la creazione di un sigillo elettronico;

e) l'indicazione dell'inizio e della fine del periodo di validità del certificato;

f) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;

g) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;

h) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera g) è disponibile gratuitamente;

▼M2

i) le informazioni relative alla validità del certificato qualificato o l'ubicazione dei servizi cui è possibile rivolgersi per informarsi in merito;

▼B

j) qualora i dati per la creazione di un sigillo elettronico connessi ai dati di convalida del sigillo elettronico siano ubicati in un dispositivo per la creazione di un sigillo elettronico qualificato, un'indicazione appropriata di questo fatto, almeno in una forma adatta al trattamento automatizzato.

▼B

ALLEGATO IV

REQUISITI PER I CERTIFICATI QUALIFICATI DI AUTENTICAZIONE DI SITI WEB

I certificati qualificati di autenticazione di siti web contengono:

a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che il certificato è stato rilasciato quale certificato qualificato di autenticazione di sito web;

b) un insieme di dati che rappresenta in modo univoco il prestatore di servizi fiduciari qualificato che rilascia i certificati qualificati e include almeno lo Stato membro in cui tale prestatore è stabilito e

— per una persona giuridica: il nome e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali,

— per una persona fisica: il nome della persona;

▼M2

c) per le persone fisiche: almeno il nome della persona a cui è stato rilasciato il certificato, o uno pseudonimo; qualora sia usato uno pseudonimo, ciò è chiaramente indicato;

c *bis*) per le persone giuridiche: un insieme unico di dati che rappresenta senza ambiguità la persona giuridica cui è stato rilasciato il certificato, con almeno il nome della persona giuridica cui è stato rilasciato il certificato e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;

▼B

d) elementi dell'indirizzo, fra cui almeno la città e lo Stato, della persona fisica o giuridica cui è rilasciato il certificato e, se del caso, quali appaiono nei documenti ufficiali;

e) il nome del dominio o dei domini gestiti dalla persona fisica o giuridica cui è rilasciato il certificato;

f) l'indicazione dell'inizio e della fine del periodo di validità del certificato;

g) il codice di identità del certificato che deve essere unico per il prestatore di servizi fiduciari qualificato;

h) la firma elettronica avanzata o il sigillo elettronico avanzato del prestatore di servizi fiduciari qualificato che rilascia il certificato;

i) il luogo in cui il certificato relativo alla firma elettronica avanzata o al sigillo elettronico avanzato di cui alla lettera h) è disponibile gratuitamente;

▼M2

j) le informazioni relative alla validità del certificato qualificato o l'ubicazione dei servizi cui è possibile rivolgersi per informarsi in merito.

▼M2

ALLEGATO V

REQUISITI PER GLI ATTESTATI ELETTRONICI QUALIFICATI DI ATTRIBUTI

Gli attestati elettronici qualificati di attributi contengono:

a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che l'attestato è stato rilasciato quale attestato elettronico di attributi qualificato;

b) un insieme di dati che rappresenta senza ambiguità il prestatore di servizi fiduciari qualificato che rilascia l'attestato elettronico di attributi qualificato e include almeno lo Stato membro in cui tale prestatore è stabilito e

   i) per una persona giuridica: il nome e, ove applicabile, il numero di registrazione quali appaiono nei documenti ufficiali,

   ii) per una persona fisica: il nome della persona;

c) un insieme di dati che rappresenta senza ambiguità il soggetto cui si riferiscono gli attributi attestati; qualora sia usato uno pseudonimo, ciò è chiaramente indicato;

d) l'attributo o gli attributi attestati, comprese, ove applicabile, le informazioni necessarie per individuare l'ambito di applicazione di tali attributi;

e) l'indicazione dell'inizio e della fine del periodo di validità dell'attestato;

f) il codice di identità dell'attestato, che deve essere unico per il prestatore di servizi fiduciari qualificato, e, se applicabile, l'indicazione del regime per gli attestati di cui fa parte l'attestato di attributi;

g) la firma elettronica qualificata o il sigillo elettronico qualificato del prestatore di servizi fiduciari qualificato che rilascia l'attestato;

h) il luogo in cui il certificato relativo alla firma elettronica qualificata o al sigillo elettronico qualificato di cui alla lettera g) è disponibile gratuitamente;

i) le informazioni relative alla validità dell'attestato qualificato o l'ubicazione dei servizi a cui è possibile rivolgersi per informarsi in merito.

▼**M2**

ALLEGATO VI

ELENCO MINIMO DI ATTRIBUTI

A norma dell'articolo 45 sexies, gli Stati membri garantiscono l'adozione di misure volte a consentire ai prestatori di servizi fiduciari qualificati di attestati elettronici di attributi di verificare mediante mezzi elettronici, su richiesta dell'utente, l'autenticità dei seguenti attributi rispetto alla pertinente fonte autentica a livello nazionale, direttamente o mediante intermediari designati riconosciuti a livello nazionale, conformemente al diritto dell'Unione o al diritto nazionale e qualora tali attributi facciano affidamento su fonti autentiche all'interno del settore pubblico:

1. indirizzo;
2. età;
3. genere;
4. stato civile;
5. composizione del nucleo familiare;
6. nazionalità o cittadinanza;
7. titoli e licenze di studio;
8. qualifiche e licenze professionali;
9. poteri e mandati di rappresentanza di persone fisiche o giuridiche
10. permessi e licenze pubblici;
11. per le persone giuridiche, i dati societari e finanziari.

▼M2

ALLEGATO VII

REQUISITI PER GLI ATTESTATI ELETTRONICI DI ATTRIBUTI RILASCIATI DA UN ORGANISMO DEL SETTORE PUBBLICO RESPONSABILE DI UNA FONTE AUTENTICA O PER SUO CONTO

Un attestato elettronico di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto contiene:

a) un'indicazione, almeno in una forma adatta al trattamento automatizzato, del fatto che l'attestato è stato rilasciato quale attestato elettronico di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto;

b) un insieme di dati che rappresenta senza ambiguità l'organismo del settore pubblico che rilascia l'attestato elettronico di attributi e include almeno lo Stato membro in cui tale organismo del settore pubblico è stabilito nonché il suo nome e, se del caso, il numero di registrazione quali appaiono nei documenti ufficiali;

c) un insieme di dati che rappresenta in modo senza ambiguità il soggetto cui si riferiscono gli attributi attestati; qualora sia usato uno pseudonimo, ciò è chiaramente indicato;

d) l'attributo o gli attributi attestati, comprese, ove applicabile, le informazioni necessarie per individuare l'ambito di applicazione di tali attributi;

e) l'indicazione dell'inizio e della fine del periodo di validità dell'attestato;

f) il codice di identità dell'attestato, che deve essere unico per l'organismo del settore pubblico che rilascia l'attestato, e, se applicabile, l'indicazione del regime per gli attestati di cui fa parte l'attestato di attributi;

g) la firma elettronica qualificata o il sigillo elettronico qualificato dell'organismo emittente;

h) il luogo in cui il certificato relativo alla firma elettronica qualificata o al sigillo elettronico qualificato di cui alla lettera g) è disponibile gratuitamente;

i) le informazioni relative alla validità dell'attestato o l'ubicazione dei servizi a cui è possibile rivolgersi per informarsi in merito.