Consiglio dell'Unione europea

Bruxelles, 25 novembre 2022
(OR. en)

14959/22

Fascicolo interistituzionale: 2021/0136(COD)

LIMITE

TELECOM 473
COMPET 919
MI 844
DATAPROTECT 321
JAI 1497
CODEC 1774

NOTA

Origine:	Comitato dei rappresentanti permanenti (parte prima)
Destinatario:	Consiglio
n. doc. prec.:	14344/22
n. doc. Comm.:	9471/21
Oggetto:	Proposta di regolamento del Parlamento europeo e del Consiglio che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea - Orientamento generale

I. INTRODUZIONE

1. La Commissione ha adottato la proposta di regolamento relativo a un'identità digitale europea (**e-ID europea**) il 3 giugno 2021[1]. L'iniziativa modifica il regolamento eIDAS del 2014[2], che aveva posto le basi necessarie per accedere ai servizi ed effettuare transazioni online e transfrontaliere nell'UE in sicurezza.

[1] Doc. 9471/21.
[2] Regolamento (UE) n. 910/2014.

2. La proposta, basata sull'articolo 114 TFUE, dispone che gli Stati membri emettano un portafoglio europeo di identità digitale nel quadro di un regime di identificazione elettronica notificato, fondato su norme tecniche comuni, a seguito di una certificazione obbligatoria. Al fine di definire l'architettura tecnica necessaria, accelerare l'attuazione del regolamento riveduto, fornire orientamenti agli Stati membri ed evitare la frammentazione, la proposta era accompagnata da una raccomandazione relativa allo sviluppo di un pacchetto di strumenti dell'Unione.

3. La proposta di regolamento è intesa a garantire alle persone e alle imprese l'accesso universale all'identificazione e all'autenticazione elettroniche sicure e affidabili mediante un portafoglio digitale personale sul telefono cellulare.

II. LAVORI NELLE ALTRE ISTITUZIONI

1. In seno al Parlamento europeo, la proposta è stata affidata alla commissione per l'industria, la ricerca e l'energia (ITRE) con tre commissioni associate per parere, ossia la commissione per il mercato interno e la protezione dei consumatori (IMCO), la commissione giuridica (JURI) e la commissione per le libertà civili, la giustizia e gli affari interni (LIBE). La relatrice del fascicolo è Romana Jerković (S&D, Croazia). La commissione ITRE non ha ancora adottato la sua relazione.

2. Il 15 luglio 2021 il Comitato economico e sociale europeo è stato invitato a formulare un parere sulla proposta, che è stato poi espresso il 20 ottobre 2021. Il Comitato europeo delle regioni ha formulato spontaneamente un parere sulla proposta il 12 ottobre 2021.

3. Il Garante europeo della protezione dei dati (GEPD) ha presentato osservazioni formali sulla proposta il 28 luglio 2021.

III. STATO DI AVANZAMENTO DEI LAVORI AL CONSIGLIO

1. In sede di Consiglio, la proposta è stata esaminata a livello di gruppo "Telecomunicazioni e società dell'informazione" ("gruppo TELECOM"), che ha avviato le discussioni nel corso della presidenza portoghese, nel giugno 2021. L'analisi della proposta è proseguita in sede di gruppo TELECOM sotto la presidenza slovena, con esito positivo della prima lettura il 15 novembre 2021.

2. La presidenza francese ha presentato la sua **prima proposta di compromesso** il 15 febbraio e il 5 aprile, mentre la **seconda** è stata discussa il 23 maggio e il 9 giugno. Nel quadro di un dibattito orientativo tenutosi in sede di gruppo TELECOM il 19 luglio 2022, la presidenza ceca, basandosi sui lavori della presidenza francese, ha individuato importanti questioni di alto livello rimaste in sospeso e ha chiesto alle delegazioni di esprimere le opzioni da loro prescelte, al fine di riformulare di conseguenza le parti pertinenti della seconda proposta di compromesso. La versione riveduta ha dato luogo a una **terza proposta di compromesso** che è stata presentata dalla presidenza ceca in occasione delle riunioni del gruppo TELECOM del 5 e 8 settembre. Ulteriori versioni e i relativi adeguamenti hanno favorito con successo un maggiore livello di convergenza sulla maggior parte delle questioni in sospeso.

3. Tuttavia, la **quarta proposta di compromesso**, presentata alle delegazioni alla riunione del gruppo TELECOM del 28 settembre, ha rivelato il persistere di divergenze tra gli Stati membri, in particolare su una questione di alto livello, ovvero il livello di garanzia scelto per il portafoglio europeo di identità digitale. Alcuni Stati membri che dispongono già di un sistema nazionale di identificazione elettronica, hanno inizialmente adottato un livello di garanzia "significativo", per poi investirvi successivamente, mentre nell'attuale proposta di identificazione elettronica è richiesto un livello di garanzia "elevato". Consapevole dell'elevato numero di mezzi di identificazione elettronica di livello di garanzia "significativo" rilasciati in alcuni Stati membri, la presidenza ceca ha quindi proposto un meccanismo per facilitare la procedura di *onboarding* degli utenti, contribuendo in tal modo all'adozione dei portafogli europei di identità digitale. La disposizione consente agli utenti di iscriversi al portafoglio europeo di identità digitale utilizzando i mezzi nazionali di identificazione elettronica esistenti di livello di garanzia "significativo" in combinazione con ulteriori procedure di *onboarding* a distanza che, insieme, soddisfano i requisiti del livello di garanzia "elevato". Le specifiche tecniche e operative sono soggette alla normativa di attuazione e la conformità ai requisiti è certificata.

4. La **quinta proposta di compromesso** è stata discussa nella riunione del gruppo TELECOM del 25 ottobre. Durante la riunione del gruppo TELECOM dell'8 novembre 2022, la presidenza ceca ha presentato le limitate modifiche apportate e, a seguito delle osservazioni supplementari e dei suggerimenti redazionali ricevuti dalle delegazioni, ha preparato la **versione finale del testo di compromesso** in vista della sua presentazione al Coreper.

5. Il 18 novembre il Coreper ha esaminato la proposta di compromesso e **ha convenuto all'unanimità di sottoporla al Consiglio TTE (Telecomunicazioni), senza modifiche, in vista di un orientamento generale** nella sessione del 6 dicembre 2022.

IV. PRINCIPALI ELEMENTI DELLA PROPOSTA DI COMPROMESSO

1. Portafoglio europeo di identità digitale

Uno dei principali obiettivi strategici della proposta della Commissione relativa a un portafoglio europeo di identità digitale ("portafoglio") è fornire ai cittadini e agli altri residenti, quali definiti dalle legislazioni nazionali, uno strumento europeo di identità digitale armonizzato, basato sul concetto di un portafoglio europeo di identità digitale. In quanto mezzo di identificazione elettronica emesso nell'ambito di regimi nazionali a un livello di garanzia "elevato", il portafoglio sarebbe un mezzo di identificazione elettronica a sé stante basato sul rilascio dei dati di identificazione personale e del portafoglio da parte degli Stati membri.

2. Livello di garanzia del portafoglio europeo di identità digitale

I livelli di garanzia dovrebbero caratterizzare il grado di sicurezza con cui i mezzi di identificazione elettronica stabiliscono l'identità di una persona, fornendo così la garanzia che la persona che pretende di avere una determinata identità è effettivamente la persona cui tale identità è stata assegnata. Sulla base dell'ampio sostegno registrato nelle riunioni del gruppo e nel dibattito in sede di Coreper del 14 ottobre, il portafoglio deve essere emesso nell'ambito di un sistema di identificazione elettronica che soddisfi i requisiti del livello di garanzia "elevato". Inoltre, all'articolo 6 bis è stata aggiunta una disposizione specifica sulle procedure di *onboarding* degli utenti. La modifica è intesa a rispondere alle preoccupazioni degli Stati membri che hanno già rilasciato un numero considerevole di mezzi nazionali di identificazione elettronica di livello di garanzia "significativo". La disposizione consente all'utente di utilizzare i propri mezzi nazionali di identificazione elettronica in combinazione con ulteriori procedure

di *onboarding* a distanza al fine di rendere possibile il controllo dell'identità a un livello di garanzia "elevato" e, in definitiva, ottenere un portafoglio. Poiché il progetto di regolamento sull'identificazione elettronica si basa su sistemi di certificazione della cibersicurezza che dovrebbero portare a un livello armonizzato di fiducia nella sicurezza dei portafogli europei di identità digitale, si prevede che anche la conservazione sicura del materiale crittografico sarà soggetta a certificazione della cibersicurezza. La presidenza ha pertanto proposto un nuovo **considerando (10 ter)** che affronti tali presupposti tecnici per conseguire un livello di garanzia "elevato" e consenta un processo di follow-up nell'ambito dell'implementazione dei portafogli europei di identità digitale.

3. Notifica delle parti facenti affidamento sulla certificazione

3.1 L'**articolo 6 ter** sulla notifica delle parti facenti affidamento sulla certificazione è stato riformulato. Come regola generale, il processo di notifica mediante il quale la parte facente affidamento sulla certificazione comunica la propria intenzione di avvalersi del portafoglio dovrebbe essere efficace sotto il profilo dei costi, proporzionato al rischio e garantire che la parte facente affidamento sulla certificazione fornisca almeno le informazioni necessarie per autenticarsi nel portafoglio. Per impostazione predefinita sono richieste solo informazioni minime e la notifica dovrebbe consentire l'uso di procedure di autodichiarazione automatizzate o semplici.

3.2 Può essere tuttavia necessario un regime specifico a causa di requisiti settoriali, come quelli applicabili al trattamento di categorie particolari di dati personali. È stata pertanto introdotta una disposizione corrispondente che mira a disciplinare i casi in cui è necessaria una procedura di registrazione o di autorizzazione più rigorosa. Per contro, qualora il diritto dell'Unione o nazionale non stabilisca requisiti specifici per accedere alle informazioni fornite mediante il portafoglio, gli Stati membri possono esonerare tali parti facenti affidamento sulla certificazione dall'obbligo di notificare la loro intenzione di avvalersi dei portafogli.

4. Certificazione

4.1 Il regolamento dovrebbe servirsi, avvalersi e imporre l'uso di sistemi di certificazione pertinenti ed esistenti nell'ambito del regolamento sulla cibersicurezza, o di parti di essi, per certificare la conformità dei portafogli, o di parti di essi, ai requisiti applicabili in materia di cibersicurezza. Di conseguenza, il quadro del regolamento sulla cibersicurezza si applica pienamente, compreso il meccanismo di valutazione tra pari tra le autorità nazionali di certificazione della cibersicurezza previsto da tale regolamento. Al fine di allineare il più possibile il regolamento sull'identificazione elettronica e il regolamento sulla cibersicurezza, gli Stati membri designeranno organismi pubblici e privati accreditati per certificare il portafoglio come previsto dal regolamento sulla cibersicurezza.

4.2 La Commissione è inoltre incoraggiata a incaricare l'ENISA di elaborare e adottare un apposito sistema, nell'ambito del regolamento sulla cibersicurezza, per la certificazione del portafoglio sul piano della cibersicurezza. Fino a quando tale sistema non viene sviluppato, il sistema europeo di certificazione della cibersicurezza basato su criteri comuni (EUCC), pubblicato a norma del regolamento sulla cibersicurezza, sarà utilizzato come metodologia di riferimento per la certificazione dei portafogli. Per i requisiti non connessi alla cibersicurezza, in particolare quelli riguardanti altri aspetti funzionali e operativi del portafoglio, deve essere stabilito un elenco di specifiche, procedure e norme di riferimento. Tali requisiti sono soggetti a certificazione.

5. Periodo di attuazione per la fornitura del portafoglio

Sulla base degli orientamenti forniti dagli Stati membri, è stato proposto che il periodo di attuazione di 24 mesi decorra dall'adozione degli atti di esecuzione di cui all'**articolo 6 bis, paragrafo 11**, e all'**articolo 6 quater, paragrafo 4**.

6. Costi

All'**articolo 6 bis, paragrafo 6 bis**, e al corrispondente considerando è stato chiarito che l'emissione, l'uso per l'autenticazione e la revoca dei portafogli dovrebbero essere gratuiti per le persone fisiche. Tranne quando i portafogli sono utilizzati per l'autenticazione, i servizi che si basano sull'uso del portafoglio possono comportare costi, ad esempio per il rilascio degli attestati elettronici di attributi al portafoglio.

7. Accesso a componenti hardware e software, compreso l'elemento sicuro

La presidenza ha proposto di prevedere un collegamento esplicito con il regolamento (UE) 2022/1925, che garantisce l'accesso alle componenti hardware e software nell'ambito dei servizi di piattaforma di base forniti dai gatekeeper. Il nuovo **articolo 12 ter** aggiunto chiarisce che i fornitori di portafogli e gli emittenti di mezzi di identificazione elettronica notificati che agiscono a titolo commerciale o professionale sono utenti commerciali dei gatekeeper ai sensi della rispettiva definizione nella normativa sui mercati digitali. È stata aggiunta la formulazione del considerando per illustrare le implicazioni dell'interconnessione con la normativa sui mercati digitali, vale a dire che i gatekeeper dovrebbero essere tenuti a garantire, a titolo gratuito, l'effettiva interoperabilità con lo stesso sistema operativo e le stesse componenti hardware o software disponibili o utilizzati nella fornitura dei suoi servizi complementari e di supporto, come pure a garantirne l'accesso ai fini dell'interoperabilità.

8. Possibilità alternative di rilasciare attestati elettronici di attributi da parte di organismi del settore pubblico

È stato mantenuto il rilascio di attestati elettronici di attributi qualificati da parte di fornitori qualificati, compreso l'obbligo per gli Stati membri di garantire che gli attributi possano essere verificati rispetto a una fonte autentica all'interno del settore pubblico. Inoltre, è stata introdotta la possibilità che un attestato elettronico di attributi con gli stessi effetti giuridici degli attestati elettronici di attributi qualificati possa essere rilasciato al portafoglio direttamente dall'organismo del settore pubblico responsabile della fonte autentica o da un organismo del settore pubblico designato, per conto di un organismo del settore pubblico responsabile di una fonte autentica, purché siano soddisfatti i requisiti necessari. La proposta trova riscontro nei nuovi **articoli 45 bis**, **45 quinquies bis** e nell'**allegato VII**.

9. Abbinamento delle registrazioni

L'**articolo 11 bis** originale è stato rinominato "Abbinamento delle registrazioni" per riflettere meglio l'obiettivo della disposizione. Sulla base della discussione, il concetto di identificatore unico e persistente è stato mantenuto per i portafogli. La rispettiva definizione chiarisce che l'identificatore può consistere in una combinazione di diversi dati di identificazione nazionali o settoriali, nella misura in cui persegue il suo scopo. È esplicitamente indicato che l'abbinamento delle registrazioni può essere agevolato da attestati elettronici di attributi qualificati. Inoltre, all'**articolo 11 bis** è stata inserita una disposizione di salvaguardia secondo cui gli Stati membri garantiscono la protezione dei dati personali e impediscono la profilazione degli utenti. Infine, gli Stati membri, in qualità di parti facenti affidamento sulla certificazione, garantiscono l'abbinamento delle registrazioni.

VI. CONCLUSIONE

1. Alla luce di quanto precede, si invita il Consiglio a:

   – esaminare il testo di compromesso che figura nell'allegato della presente nota;

   – confermare un orientamento generale sulla proposta di regolamento relativo a un'identità digitale europea (eID europea) nella sessione del Consiglio TTE (Telecomunicazioni) del 6 dicembre 2022.

ALLEGATO

Proposta di

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione di un quadro per un'identità digitale europea

IL PARLAMENTO EUROPEO E IL CONSIGLIO DELL'UNIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea, in particolare l'articolo 114,

vista la proposta della Commissione europea,

previa trasmissione del progetto di atto legislativo ai parlamenti nazionali,

visto il parere del Comitato economico e sociale europeo[3],

deliberando secondo la procedura legislativa ordinaria,

considerando quanto segue:

(1) Nella comunicazione della Commissione del 19 febbraio 2020 intitolata "Plasmare il futuro digitale dell'Europa"[4] si annunciava la revisione del regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio con l'obiettivo di migliorarne l'efficacia, estenderne i benefici al settore privato e promuovere identità digitali affidabili per tutti gli europei.

[3] GU C del [...], pag.[...].
[4] COM/2020/67 final

(2) Nelle sue conclusioni dell'1-2 ottobre 2020[5], il Consiglio europeo ha chiesto alla Commissione di proporre lo sviluppo di un quadro a livello dell'UE per l'identificazione elettronica pubblica e sicura, ivi incluse le firme digitali interoperabili, che garantisca alle persone il controllo della loro identità e dei loro dati online e consenta l'accesso a servizi digitali pubblici, privati e transfrontalieri.

(3) Nella comunicazione della Commissione del 9 marzo 2021 intitolata "Bussola per il digitale 2030: il modello europeo per il decennio digitale"[6] è fissato l'obiettivo di un quadro dell'Unione che, entro il 2030, porti a un'ampia diffusione di un'identità affidabile e controllata dagli utenti, che consenta a ciascun cittadino di controllare le proprie interazioni e la propria presenza online.

(4) Un approccio maggiormente armonizzato all'identificazione digitale dovrebbe ridurre i rischi e i costi dell'attuale frammentazione dovuta all'uso di soluzioni nazionali divergenti e rafforzerà il mercato unico consentendo ai cittadini, agli altri residenti quali definiti dalle legislazioni nazionali e alle imprese di identificarsi online in modo pratico e uniforme in tutta l'Unione. Il portafoglio europeo di identità digitale fornirà alle persone fisiche e giuridiche di tutta l'Unione un mezzo di identificazione elettronica armonizzato che consentirà loro di autenticare e condividere dati collegati alla loro identità. Tutti dovrebbero poter accedere in modo sicuro a servizi pubblici e privati che fanno affidamento su un ecosistema migliorato per i servizi fiduciari e su prove dell'identità e attestati di attributi verificati, come un diploma universitario legalmente riconosciuto e accettato in tutta l'Unione. L'obiettivo del quadro per un'identità digitale europea è il passaggio dalla dipendenza esclusiva da soluzioni di identità digitale nazionali alla fornitura di attestati elettronici di attributi validi a livello europeo. I fornitori di attestati elettronici di attributi dovrebbero beneficiare di un insieme di regole chiaro e uniforme, e le amministrazioni pubbliche dovrebbero potersi avvalere di documenti elettronici in un formato prestabilito.

---

5 https://www.consilium.europa.eu/it/press/press-releases/2020/10/02/european-council-conclusions-1-2-october-2020/.

6 COM/2021/118 final/2

(4 bis) Vari Stati membri hanno attuato e utilizzano ampiamente mezzi di identificazione elettronica che oggi sono accettati dai prestatori di servizi nell'Unione. Inoltre sono stati effettuati investimenti in soluzioni sia nazionali che transfrontaliere basate sull'attuale regolamento eIDAS, compresa l'infrastruttura tecnica di interoperabilità dei nodi eIDAS. Al fine di garantire la complementarità e una rapida adozione dei portafogli europei di identità digitale da parte degli attuali utenti di mezzi di identificazione elettronica notificati e di ridurre al minimo l'impatto sui prestatori di servizi esistenti, i portafogli europei di identità digitale dovrebbero trarre vantaggio dall'esperienza acquisita con i mezzi di identificazione elettronica esistenti e dall'utilizzo dell'infrastruttura eIDAS installata a livello europeo e nazionale.

(5) Al fine di sostenere la competitività delle imprese europee, i prestatori di servizi online dovrebbero potersi avvalere di soluzioni di identità digitale riconosciute in tutta l'Unione, indipendentemente dallo Stato membro in cui sono state fornite, traendo in tal modo vantaggio da un approccio europeo armonizzato in materia di fiducia, sicurezza e interoperabilità. Tanto gli utenti quanto i prestatori di servizi dovrebbero poter beneficiare in tutta l'Unione dello stesso valore giuridico conferito agli attestati elettronici di attributi.

(6) Il regolamento (UE) 2016/679[7] si applica al trattamento dei dati personali nell'attuazione del presente regolamento. Il presente regolamento dovrebbe pertanto stabilire garanzie specifiche al fine di impedire ai fornitori di mezzi di identificazione elettronica e di attestati elettronici di attributi di combinare i dati personali provenienti da altri servizi con i dati personali relativi ai servizi che rientrano nell'ambito di applicazione del presente regolamento. I dati personali relativi alla fornitura dei portafogli europei di identità digitale dovrebbero essere tenuti logicamente separati dagli altri dati detenuti dall'emittente. Il presente regolamento non impedisce agli emittenti di portafogli europei di identità digitale di applicare misure tecniche supplementari che contribuiscano alla protezione dei dati personali, quali la separazione fisica dei dati personali relativi alla fornitura dei portafogli da qualsiasi altro dato detenuto dall'emittente.

[7] 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).

(7) È necessario stabilire le condizioni armonizzate per l'istituzione di un quadro per i portafogli europei di identità digitale che saranno forniti dagli Stati membri, che dovrebbero consentire a tutti i cittadini dell'Unione e agli altri residenti quali definiti dalle legislazioni nazionali di condividere in sicurezza i dati relativi alla loro identità in modo pratico e intuitivo e con il controllo esclusivo dell'utente. Le tecnologie utilizzate per conseguire tali obiettivi dovrebbero essere sviluppate cercando di ottenere il massimo livello di sicurezza, riservatezza, praticità per gli utenti e ampia usabilità. Gli Stati membri dovrebbero garantire a tutti i loro cittadini e residenti la parità di accesso all'identificazione digitale.

(8) Per garantire che le parti facenti affidamento sulla certificazione possano avvalersi dei portafogli europei di identità digitale e per proteggere l'utente dall'uso illecito di dati sensibili, le parti facenti affidamento sulla certificazione dovrebbero essere registrate nell'ambito di un processo di notifica. Nella maggior parte dei casi gli obblighi di notifica applicabili alle parti facenti affidamento sulla certificazione dovrebbero basarsi sulla fornitura di una quantità limitata di informazioni necessarie per l'autenticazione della parte facente affidamento sulla certificazione nel portafoglio europeo di identità digitale. Tali obblighi dovrebbero inoltre consentire l'uso di procedure di autodichiarazione automatizzate o semplici, comprese procedure in cui gli Stati membri si affidano e ricorrono a registri esistenti. Allo stesso tempo, per le categorie di dati sensibili potrebbero esistere regimi specifici, a livello nazionale o dell'Unione, che possano imporre alle parti facenti affidamento sulla certificazione obblighi di registrazione e autorizzazione più rigorosi al fine di prevenire l'uso illecito dei dati di identità in tali casi. In altri casi d'uso, le parti facenti affidamento sulla certificazione possono essere esentate dal notificare la loro intenzione di avvalersi del portafoglio digitale europeo, ad esempio quando il diritto di verificare attributi specifici non richiede o consente l'autenticazione mediante mezzi elettronici della parte facente affidamento sulla certificazione. In genere, in questi scenari in presenza l'utente è in grado di identificare la parte facente affidamento sulla certificazione grazie al contesto, ad esempio quando interagisce con un addetto al noleggio auto o un farmacista. Il processo di notifica dovrebbe essere guidato da normative settoriali dell'Unione o nazionali, in quanto ciò consente di tenere conto di vari casi d'uso che possono differire in termini di obblighi di registrazione, modalità di funzionamento (online/offline) o in termini di obbligo di autenticazione dei dispositivi in grado di interfacciarsi con il portafoglio europeo di identità digitale. Non si dovrebbe imporre l'applicazione, a livello del portafoglio europeo di identità digitale, della verifica dell'uso del portafoglio europeo di identità digitale ad opera delle parti facenti affidamento sulla certificazione.

(9) Tutti i portafogli europei di identità digitale dovrebbero consentire agli utenti di identificarsi e autenticarsi elettronicamente online e offline a livello transfrontaliero per accedere a un'ampia gamma di servizi pubblici e privati. Fatte salve le prerogative degli Stati membri per quanto riguarda l'identificazione dei loro cittadini e residenti, i portafogli possono anche rispondere alle esigenze istituzionali delle amministrazioni pubbliche, delle organizzazioni internazionali e delle istituzioni, degli organi e degli organismi dell'Unione. L'uso offline sarebbe importante in molti settori, compreso il settore sanitario nel quale i servizi sono spesso forniti mediante interazioni faccia a faccia, e per le ricette elettroniche dovrebbe essere possibile avvalersi di codici QR o tecnologie simili che consentano di verificarne l'autenticità. Contando su un livello di garanzia "elevato", i portafogli europei di identità digitale dovrebbero sfruttare il potenziale offerto da soluzioni a prova di manomissione quali gli elementi sicuri al fine di rispettare i requisiti di sicurezza di cui al presente regolamento. I portafogli europei di identità digitale dovrebbero inoltre consentire agli utenti di creare e utilizzare firme e sigilli elettronici qualificati accettati in tutta l'UE. Al fine di conseguire vantaggi in termini di semplificazione e riduzione dei costi per le persone e le imprese in tutta l'UE, anche mediante la concessione di poteri di rappresentanza e mandati elettronici, gli Stati membri dovrebbero emettere portafogli europei di identità digitale basati su norme comuni per garantire un'interoperabilità senza soluzione di continuità e un elevato livello di sicurezza. Solo le autorità competenti degli Stati membri possono fornire un grado elevato di sicurezza nella determinazione dell'identità di una persona e garantire quindi che la persona che rivendica o afferma una determinata identità sia effettivamente colui o colei che dice di essere. È pertanto necessario che i portafogli europei di identità digitale si basino sull'identità giuridica dei cittadini, degli altri residenti o delle entità giuridiche. La fiducia nei portafogli europei di identità digitale aumenterebbe se i soggetti emittenti fossero tenuti ad attuare misure tecniche e organizzative adeguate per garantire un livello di sicurezza commisurato ai rischi per i diritti e le libertà delle persone fisiche, conformemente al regolamento (UE) 2016/679. L'emissione, l'uso per l'autenticazione e la revoca dei portafogli europei di identità digitale sono gratuiti per le persone fisiche. I servizi che si basano sull'uso del portafoglio possono comportare costi connessi, ad esempio, al rilascio degli attestati elettronici di attributi al portafoglio.

(9 bis) È utile facilitare l'adozione e l'uso dei portafogli europei di identità digitale integrandoli senza soluzione di continuità con l'ecosistema dei servizi digitali pubblici e privati già attuati a livello nazionale, locale o regionale. Per conseguire tale obiettivo, gli Stati membri possono prevedere misure giuridiche e organizzative al fine di aumentare la flessibilità per gli emittenti dei portafogli europei di identità digitale e consentire funzionalità aggiuntive dei portafogli europei di identità digitale al di là di quanto stabilito dal presente regolamento, anche attraverso una maggiore interoperabilità con i mezzi nazionali di identificazione elettronica esistenti. Ciò non dovrebbe in alcun modo andare a scapito delle funzioni fondamentali dei portafogli europei di identità digitale di cui al presente regolamento né promuovere le soluzioni nazionali esistenti rispetto ai portafogli europei di identità digitale. Poiché vanno al di là del presente regolamento, tali funzionalità aggiuntive non beneficiano delle disposizioni in materia di ricorso transfrontaliero ai portafogli europei di identità digitale di cui al presente regolamento.

(10) Al fine di conseguire un livello elevato di protezione dei dati, sicurezza e fiducia, il presente regolamento dovrebbe istituire un quadro armonizzato che precisi i requisiti e le specifiche comuni applicabili ai portafogli europei di identità digitale. La conformità dei portafogli europei di identità digitale a tali requisiti dovrebbe essere certificata da organismi accreditati di valutazione della conformità designati dagli Stati membri. La certificazione dovrebbe basarsi in particolare sui pertinenti sistemi europei di certificazione della cibersicurezza, o loro parti, istituiti a norma del regolamento (UE) 2019/881[8], nella misura in cui essi contemplino i requisiti di cibersicurezza applicabili ai portafogli europei di identità digitale. Basarsi su sistemi europei di certificazione della cibersicurezza dovrebbe portare a un livello armonizzato di fiducia nella sicurezza dei portafogli europei di identità digitale, indipendentemente dal luogo in cui sono emessi in tutta l'Unione. La certificazione della cibersicurezza dei portafogli europei di identità digitale dovrebbe prendere le mosse dal ruolo svolto dalle autorità nazionali di certificazione della cibersicurezza, ossia la vigilanza e il monitoraggio della conformità dei certificati rilasciati dagli organismi di valutazione della conformità nella loro giurisdizione ai pertinenti sistemi europei di cibersicurezza. Analogamente, la certificazione dovrebbe sfruttare, se del caso, le norme e le specifiche tecniche di cui al regolamento (UE) 2019/881. Tali specifiche possono essere utilizzate come documenti allo stato dell'arte, secondo quando specificato nell'ambito dei pertinenti sistemi di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881. Qualora nessun pertinente sistema europeo di certificazione della cibersicurezza istituito a norma del regolamento (UE) 2019/881 contempli la certificazione di servizi o processi pertinenti che contribuiscono alla sicurezza del portafoglio, dovrebbero essere creati sistemi adeguati in conformità del titolo III del regolamento (UE) 2019/881. È opportuno istituire un sistema comune e armonizzato per la certificazione dei portafogli europei di identità digitale che valuti la loro conformità alle specifiche e ai requisiti comuni di cui al presente regolamento diversi da quelli relativi alla cibersicurezza e alla protezione dei dati, in particolare le specifiche e i requisiti riguardanti gli aspetti funzionali e operativi. Per quanto riguarda tale certificazione, al fine di garantire un elevato livello di fiducia e trasparenza, è opportuno istituire meccanismi e procedure volti a promuovere l'apprendimento tra pari e la cooperazione tra Stati membri per quanto riguarda il monitoraggio e il riesame degli organismi di certificazione nonché dei certificati e delle relazioni di certificazione da essi rilasciati. Tale meccanismo di apprendimento tra pari dovrebbe lasciare impregiudicati il regolamento (UE) 2016/679 e il regolamento (UE) 2019/881. La certificazione del portafoglio a norma del regolamento (UE) 2016/679 è uno degli strumenti volontari che possono essere utilizzati per dimostrare la conformità ai requisiti di cui al regolamento (UE) 2016/679 che si applicano ai portafogli europei di identità digitale e alla fornitura di questi ultimi ai cittadini europei.

---

8 Regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio, del 17 aprile 2019, relativo all'ENISA, l'Agenzia dell'Unione europea per la cibersicurezza, e alla certificazione della cibersicurezza per le tecnologie dell'informazione e della comunicazione, e che abroga il regolamento (UE) n. 526/2013 ("regolamento sulla cibersicurezza") (GU L 151 del 7.6.2019, pag. 15).

(10 bis) L'*onboarding* nel portafoglio europeo di identità digitale dei cittadini e dei residenti dovrebbe essere agevolato ricorrendo a mezzi di identificazione elettronica rilasciati a un livello di garanzia "elevato". I mezzi di identificazione elettronica rilasciati a un livello di garanzia "significativo" dovrebbero essere utilizzati solo nei casi in cui le specifiche tecniche e operative armonizzate che utilizzano mezzi di identificazione elettronica rilasciati a un livello di garanzia "significativo" in combinazione con altri mezzi complementari di verifica dell'identità consentiranno di soddisfare i requisiti di cui al presente regolamento per quanto riguarda il livello di garanzia "elevato". Tali mezzi o misure complementari dovrebbero essere affidabili e di facile utilizzo da parte degli utenti e potrebbero basarsi sulla possibilità di utilizzare procedure di *onboarding* a distanza, certificati qualificati che supportano firme qualificate, attestati elettronici di attributi qualificati o una loro combinazione. Al fine di garantire un livello sufficiente di adozione dei portafogli europei di identità digitale, è opportuno stabilire, mediante atti di esecuzione, specifiche tecniche e operative armonizzate per l'*onboarding* degli utenti utilizzando mezzi di identificazione elettronica, compresi quelli rilasciati a un livello di garanzia "significativo".

(10 ter) L'obiettivo del presente regolamento è fornire all'utente un portafoglio europeo di identità digitale interamente mobile, sicuro e di facile utilizzo. Come misura transitoria fino alla disponibilità di soluzioni certificate a prova di manomissione, come ad esempio elementi sicuri all'interno dei dispositivi degli utenti, i portafogli europei di identità digitale potrebbero basarsi su elementi sicuri esterni certificati per la protezione del materiale crittografico e di altri dati sensibili o su soluzioni nazionali notificate a un livello di garanzia "elevato" al fine di dimostrare la conformità ai pertinenti requisiti del regolamento per quanto riguarda il livello di garanzia del portafoglio. Il ricorso alla suddetta misura transitoria dovrebbe essere limitato ai casi che richiedono un livello di garanzia "elevato", quali l'*onboarding* dell'utente nel portafoglio e l'autenticazione a servizi che richiedono un livello di garanzia "elevato". Quando autenticano servizi che richiedono un livello di affidabilità "significativo", i portafogli europei di identità digitale non dovrebbero imporre il ricorso alla misura transitoria di cui sopra. Il presente regolamento dovrebbe lasciare impregiudicate le condizioni nazionali per il rilascio e l'uso di elementi sicuri esterni certificati nel caso in cui tale misura transitoria vi ricorra.

(11) I portafogli europei di identità digitale dovrebbero garantire il massimo livello di protezione e sicurezza dei dati personali utilizzati per l'autenticazione, indipendentemente dal fatto che tali dati siano conservati localmente o attraverso soluzioni basate sul cloud, tenendo conto dei diversi livelli di rischio. Il trattamento di dati biometrici come fattore di autenticazione nell'ambito dell'identificazione forte dell'utente è uno dei metodi di identificazione che offrono un elevato livello di sicurezza, in particolare se utilizzato in combinazione con altri elementi di autenticazione. Poiché i dati biometrici rappresentano una caratteristica unica di una persona, il trattamento dei dati biometrici è consentito solo a norma delle eccezioni di cui all'articolo 9, paragrafo 2, del regolamento (UE) 2016/679 e richiede garanzie adeguate, commisurate al rischio che tale trattamento può comportare per i diritti e le libertà delle persone fisiche.

(11 bis) Il funzionamento dei portafogli europei di identità digitale dovrebbe essere trasparente e consentire un trattamento dei dati personali verificabile. A tal fine, gli Stati membri sono incoraggiati a divulgare il codice sorgente dei componenti software dei portafogli europei di identità digitale che sono connessi al trattamento dei dati personali e dei dati delle persone giuridiche. La divulgazione di tale codice sorgente consente alla società, utenti e sviluppatori compresi, di comprenderne il funzionamento, il che, a sua volta, può aumentare la fiducia degli utenti nell'ecosistema dei portafogli e contribuire alla sicurezza dei portafogli consentendo a chiunque di segnalare vulnerabilità ed errori nel codice. Ciò spinge i fornitori a offrire e mantenere un prodotto altamente sicuro. Inoltre, se del caso, gli Stati membri sono anche incoraggiati a rendere disponibile il codice sorgente nell'ambito di una licenza open source. Una licenza open source consente alla società, utenti e sviluppatori compresi, di modificare e riutilizzare il codice sorgente.

(12) Al fine di garantire che il quadro per un'identità digitale europea sia aperto all'innovazione e agli sviluppi tecnologici e adatto alle esigenze future, gli Stati membri dovrebbero essere incoraggiati a istituire spazi di sperimentazione comuni per testare le soluzioni innovative in un ambiente controllato e sicuro, in particolare per migliorare la funzionalità, la protezione dei dati personali, la sicurezza e l'interoperabilità delle soluzioni e disporre di dati su cui basare i futuri aggiornamenti dei riferimenti tecnici e dei requisiti giuridici. Tale ambiente dovrebbe favorire l'inclusione delle piccole e medie imprese, delle start-up e dei singoli innovatori e ricercatori europei.

(13) Il regolamento (UE) 2019/1157[9] rafforza la sicurezza delle carte d'identità mediante caratteristiche di sicurezza rafforzate entro agosto 2021. Gli Stati membri dovrebbero valutare se sia fattibile notificarle nell'ambito dei regimi di identificazione elettronica al fine di estendere la disponibilità transfrontaliera dei mezzi di identificazione elettronica.

(14) Il processo di notifica dei regimi di identificazione elettronica dovrebbe essere semplificato e accelerato al fine di promuovere l'accesso a soluzioni di autenticazione e identificazione pratiche, affidabili, sicure e innovative e, ove opportuno, di incoraggiare i gestori di identità (identity provider) privati a offrire regimi di identificazione elettronica alle autorità degli Stati membri affinché siano notificati come regimi nazionali di identificazione elettronica a norma del regolamento (UE) n. 910/2014.

(15) La razionalizzazione delle attuali procedure di notifica e valutazione tra pari eviterà approcci eterogenei alla valutazione dei vari regimi di identificazione elettronica notificati e faciliterà la creazione di un clima di fiducia tra gli Stati membri. I nuovi meccanismi semplificati dovrebbero promuovere la cooperazione tra gli Stati membri in materia di sicurezza e interoperabilità dei rispettivi regimi di identificazione elettronica notificati.

(16) Gli Stati membri dovrebbero beneficiare di strumenti nuovi e flessibili per garantire il rispetto dei requisiti di cui al presente regolamento e ai pertinenti atti di esecuzione. Il presente regolamento dovrebbe consentire agli Stati membri di utilizzare relazioni e valutazioni, realizzate da organismi di valutazione della conformità accreditati, come previsto nei sistemi di certificazione che devono essere istituiti a livello dell'Unione a norma del regolamento (UE) 2019/881, a sostegno delle loro dichiarazioni di conformità dei regimi, o di parti di essi, ai requisiti di cui al regolamento in materia di interoperabilità e sicurezza dei regimi di identificazione elettronica notificati.

[9] Regolamento (UE) 2019/1157 del Parlamento europeo e del Consiglio, del 20 giugno 2019, sul rafforzamento della sicurezza delle carte d'identità dei cittadini dell'Unione e dei titoli di soggiorno rilasciati ai cittadini dell'Unione e ai loro familiari che esercitano il diritto di libera circolazione (GU L 188 del 12.7.2019, pag. 67).

(17 bis) L'uso di identificatori unici e persistenti rilasciati dagli Stati membri o generati dal portafoglio europeo di identità digitale, unitamente all'uso di dati di identificazione personale, è essenziale per garantire che l'identità dell'utente, in particolare nel settore pubblico e laddove previsto dal diritto nazionale o dell'Unione, possa essere verificata. Il presente regolamento dovrebbe garantire che il portafoglio europeo di identità digitale possa fornire un meccanismo che consenta l'abbinamento delle registrazioni, anche mediante l'uso di attestati elettronici di attributi qualificati, e permettere l'inclusione di identificatori unici e persistenti nell'insieme di dati di identificazione personale. Un identificatore unico e persistente può consistere in dati di identificazione unici o multipli che possono essere settoriali, purché servano a identificare in modo univoco l'utente in tutta l'Unione. Il portafoglio europeo di identità digitale dovrebbe inoltre prevedere un meccanismo che consenta l'uso di identificatori specifici alla parte facente affidamento sulla certificazione nei casi in cui l'uso di un identificatore unico e persistente sia richiesto dal diritto nazionale o dell'Unione. In tutti i casi, il meccanismo previsto per facilitare l'abbinamento delle registrazioni e l'uso di identificatori unici e persistenti dovrebbe garantire che l'utente sia protetto contro l'uso abusivo dei dati personali ai sensi del presente regolamento e del diritto applicabile dell'Unione, in particolare il regolamento (UE) 2016/679, anche contro il rischio di profilazione e tracciamento connesso all'uso del portafoglio europeo di identità digitale.

(17 bis bis) È essenziale tenere conto delle esigenze degli utenti, stimolando la domanda di portafogli europei di identità digitale. Dovrebbero essere disponibili casi d'uso e servizi online significativi che si basano sui portafogli europei di identità digitale. Per comodità degli utenti e per garantire la disponibilità transfrontaliera di tali servizi, è importante intraprendere azioni volte a facilitare un approccio analogo alla progettazione, allo sviluppo e all'attuazione di servizi online in tutti gli Stati membri. Orientamenti non vincolanti in materia di progettazione, sviluppo e attuazione dei servizi online che si basano sui portafogli europei di identità digitale hanno il potenziale di diventare uno strumento utile per conseguire tale obiettivo. Tali orientamenti dovrebbero essere elaborati tenendo debitamente conto del quadro di interoperabilità dell'Unione. Gli Stati membri dovrebbero avere un ruolo guida quanto alla loro adozione.

(18) Conformemente alla direttiva (UE) 2019/882[10], le persone con disabilità dovrebbero poter utilizzare in condizioni di parità con gli altri utenti i portafogli europei di identità digitale, i servizi fiduciari e i prodotti destinati all'utente finale impiegati per la prestazione di tali servizi.

(19) Il presente regolamento non dovrebbe contemplare aspetti legati alla conclusione e alla validità di contratti o di altri vincoli giuridici nei casi in cui il diritto nazionale o dell'Unione stabilisca obblighi quanto alla forma. Non dovrebbe inoltre avere ripercussioni sugli obblighi di forma nazionali relativi ai registri pubblici, in particolare i registri commerciali e catastali.

(20) La prestazione e l'uso di servizi fiduciari stanno acquisendo una sempre maggiore importanza per il commercio e la cooperazione internazionali. I partner internazionali dell'UE stanno istituendo quadri fiduciari che si ispirano al regolamento (UE) n. 910/2014. Pertanto, al fine di facilitare il riconoscimento di tali servizi e dei relativi prestatori, la normativa di attuazione può fissare le condizioni alle quali i quadri fiduciari dei paesi terzi potrebbero essere considerati equivalenti ai quadri fiduciari per i servizi fiduciari qualificati e i relativi prestatori di cui al presente regolamento, a integrazione della possibilità di riconoscimento reciproco dei servizi fiduciari e dei relativi prestatori stabiliti nell'Unione e in paesi terzi conformemente all'articolo 218 del trattato. Nel fissare le condizioni alle quali i quadri fiduciari dei paesi terzi potrebbero essere considerati equivalenti ai quadri fiduciari per i servizi fiduciari qualificati e i relativi prestatori di cui al presente regolamento, è opportuno garantire anche il rispetto delle pertinenti disposizioni di cui alla direttiva XXXX/XXXX (direttiva NIS 2) e al regolamento (UE) 2016/679, nonché l'uso di elenchi di fiducia quali elementi essenziali per costruire la fiducia.

[10] 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).

(21) Il presente regolamento dovrebbe basarsi sugli atti dell'Unione che garantiscono mercati equi e contendibili nel settore digitale. Esso si basa in particolare sul regolamento (UE) 2022/195, che introduce norme per i fornitori di servizi di piattaforma di base designati come gatekeeper e, tra l'altro, impedisce ai gatekeeper di imporre agli utenti commerciali l'utilizzo o l'offerta di un servizio di identificazione del gatekeeper, o l'interoperabilità con lo stesso, nel contesto dei servizi offerti dagli utenti commerciali che si avvalgono dei servizi di piattaforma di base di tale gatekeeper. A norma dell'articolo 6, paragrafo 7, del regolamento (UE) 2022/1925, i gatekeeper sono tenuti a consentire agli utenti commerciali e ai fornitori di servizi ausiliari l'accesso allo stesso sistema operativo e alle stesse componenti hardware o software disponibili o utilizzati nella fornitura di servizi ausiliari da parte del gatekeeper e l'interoperabilità con gli stessi. Conformemente all'articolo 2, punto 15, del regolamento sui mercati digitali, i servizi di identificazione sono un tipo di servizi ausiliari. Agli utenti commerciali e ai fornitori di servizi ausiliari dovrebbe quindi essere garantito l'accesso a componenti hardware o software, quali gli elementi sicuri degli smartphone, e l'interoperabilità con gli stessi mediante i portafogli europei di identità digitale o i mezzi di identificazione elettronica notificati degli Stati membri.

(22) Al fine di razionalizzare gli obblighi in materia di cibersicurezza imposti ai prestatori di servizi fiduciari, nonché di consentire a tali prestatori e alle rispettive autorità competenti di beneficiare del quadro giuridico istituito dalla direttiva XXXX/XXXX (direttiva NIS2), a norma di tale direttiva i servizi fiduciari sono tenuti ad adottare misure tecniche e organizzative adeguate, quali misure per far fronte a guasti del sistema, errori umani, azioni malevole o fenomeni naturali, per gestire i rischi posti alla sicurezza dei sistemi informatici e di rete che tali prestatori utilizzano nella prestazione dei loro servizi, nonché per notificare incidenti significativi e minacce informatiche conformemente alla medesima direttiva. Per quanto riguarda la segnalazione di incidenti, i prestatori di servizi fiduciari dovrebbero notificare eventuali incidenti che abbiano un impatto significativo sulla prestazione dei loro servizi, compresi quelli causati dal furto o dalla perdita di dispositivi o da danni ai cavi di rete, o quelli verificatisi nel contesto dell'identificazione di persone. Le prescrizioni in materia di gestione e segnalazione dei rischi di cibersicurezza a norma della direttiva XXXX/XXXX [NIS2] dovrebbero essere considerate complementari agli obblighi imposti ai prestatori di servizi fiduciari a norma del presente regolamento. Ove opportuno, le autorità competenti designate a norma della direttiva XXXX/XXXX (direttiva NIS2) dovrebbero continuare ad applicare le prassi o gli orientamenti nazionali consolidati per quanto riguarda l'attuazione delle prescrizioni in materia di sicurezza e comunicazione e la vigilanza della conformità a tali prescrizioni a norma del regolamento (UE) n. 910/2014. Le prescrizioni a norma del presente regolamento fanno salvo l'obbligo di notificare le violazioni dei dati personali a norma del regolamento (UE) 2016/679.

(23) È opportuno prestare la dovuta attenzione per garantire una cooperazione efficace tra le autorità NIS ed eIDAS. Qualora gli organismi di vigilanza a norma del presente regolamento siano diversi dalle autorità competenti designate a norma della direttiva XXXX/XXXX [NIS2], tali autorità dovrebbero cooperare strettamente e in maniera puntuale scambiandosi le pertinenti informazioni al fine di garantire un'efficace vigilanza dei prestatori di servizi fiduciari e il rispetto da parte loro dei requisiti di cui al presente regolamento e alla direttiva XXXX/XXXX [NIS2]. In particolare, gli organismi di vigilanza a norma del presente regolamento dovrebbero poter richiedere alle autorità competenti a norma della direttiva XXXX/XXXX [NIS2] di fornire le pertinenti informazioni necessarie per concedere la qualifica e svolgere azioni di vigilanza volte a verificare la conformità dei prestatori di servizi fiduciari alle pertinenti prescrizioni di cui alla direttiva NIS2 o a imporre loro di rimediare alla mancata conformità.

(24) È essenziale prevedere un quadro giuridico per agevolare il riconoscimento transfrontaliero tra gli ordinamenti giuridici nazionali esistenti relativi ai servizi elettronici di recapito certificato. Tale quadro potrebbe aprire inoltre per i prestatori di servizi fiduciari dell'Unione nuove opportunità di mercato per l'offerta di nuovi servizi elettronici di recapito certificati paneuropei. Al fine di garantire che i dati trasmessi mediante servizio elettronico di recapito certificato qualificato giungano al destinatario corretto, i servizi elettronici di recapito certificato qualificati dovrebbero garantire con assoluta certezza l'identificazione del destinatario, mentre per quanto riguarda l'identificazione del mittente basterebbe un elevato livello di sicurezza. Gli Stati membri dovrebbero incoraggiare i prestatori di servizi elettronici di recapito certificato qualificati a far sì che i loro servizi siano interoperabili con i servizi elettronici di recapito certificato qualificati prestati da altri prestatori di servizi fiduciari qualificati, al fine di trasferire facilmente i dati elettronici registrati tra due o più prestatori di servizi fiduciari qualificati e di promuovere pratiche leali nel mercato interno.

(25) Nella maggior parte dei casi i cittadini e gli altri residenti non possono scambiare digitalmente e a livello transfrontaliero, in modo sicuro e con un livello elevato di protezione dei dati, informazioni relative alla loro identità quali indirizzi, età e qualifiche professionali, patenti di guida e altri permessi e dati di pagamento.

(26) Dovrebbe essere possibile emettere e gestire attributi digitali affidabili e contribuire a ridurre gli oneri amministrativi, consentendo ai cittadini e agli altri residenti di utilizzare tali attributi nelle loro transazioni pubbliche e private. I cittadini e gli altri residenti dovrebbero poter, ad esempio, dimostrare di possedere una patente di guida in corso di validità rilasciata dall'autorità di uno Stato membro, che possa essere verificata e ritenuta affidabile dalle autorità competenti di altri Stati membri, e dovrebbero potersi inoltre avvalere in un contesto transfrontaliero delle proprie credenziali relative alla sicurezza sociale o di futuri documenti di viaggio digitali.

(27) Qualsiasi soggetto che raccolga, crei e rilasci attributi attestati quali diplomi, licenze o certificati di nascita dovrebbe poter diventare un fornitore di attestati elettronici di attributi Le parti facenti affidamento sulla certificazione dovrebbero utilizzare gli attestati elettronici di attributi come equivalenti agli attestati in formato cartaceo. Agli attestati elettronici di attributi non dovrebbero pertanto essere negati gli effetti giuridici a motivo della loro forma elettronica o perché non soddisfano i requisiti degli attestati elettronici di attributi qualificati. A tal fine è opportuno stabilire requisiti generali per garantire che gli effetti giuridici degli attestati elettronici di attributi qualificati siano equivalenti a quelli degli attestati in formato cartaceo rilasciati legalmente. Tali requisiti dovrebbero tuttavia applicarsi fatta salva la normativa dell'Unione o nazionale che definisce ulteriori requisiti di forma settoriali aventi effetti giuridici e, in particolare, il riconoscimento transfrontaliero degli attestati elettronici di attributi qualificati, ove opportuno.

(28) Per essere ampiamente disponibili e usabili, i portafogli europei di identità digitale devono essere accettati dai prestatori di servizi privati. Le parti private facenti affidamento sulla certificazione che prestano servizi 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 dovrebbero accettare l'uso dei portafogli europei di identità digitale per la prestazione di servizi per i quali la normativa dell'Unione o nazionale o gli obblighi contrattuali impongono un'autenticazione forte dell'utente. Per agevolare l'uso e l'accettazione del portafoglio europeo di identità digitale, è opportuno tenere conto delle norme e delle specifiche del settore ampiamente accettate. Qualora le piattaforme online di dimensioni molto grandi quali definite all'articolo 25, paragrafo 1, del regolamento [riferimento alla legge sui servizi digitali] impongano agli utenti di autenticarsi per accedere ai servizi online, tali piattaforme dovrebbero essere tenute ad accettare l'uso dei portafogli europei di identità digitale su richiesta volontaria dell'utente. Gli utenti non dovrebbero essere obbligati a usare il portafoglio per accedere ai servizi privati, ma qualora desiderassero usarlo le piattaforme online di dimensioni molto grandi dovrebbero accettare l'impiego del portafoglio europeo di identità digitale a tale scopo nel rispetto del principio della minimizzazione dei dati. Si tratta di un aspetto necessario al fine di aumentare la tutela degli utenti dalle frodi e garantire un livello elevato di protezione dei dati, considerata l'importanza che le piattaforme online di dimensioni molto grandi rivestono per via del loro raggio d'azione, espresso in particolare come numero di destinatari del servizio e di transazioni economiche. È opportuno elaborare codici di condotta di autoregolamentazione a livello dell'Unione ("codici di condotta") per contribuire all'ampia disponibilità e usabilità dei mezzi di identificazione elettronica, compresi i portafogli europei di identità digitale che rientrano nell'ambito di applicazione del presente regolamento. I codici di condotta dovrebbero agevolare la diffusa accettazione dei mezzi di identificazione elettronica, compresi i portafogli europei di identità digitale, da parte dei prestatori di servizi che non sono considerati piattaforme di dimensioni molto grandi e che si avvalgono di servizi di identificazione elettronica di terzi per l'autenticazione degli utenti. Tali codici dovrebbero essere elaborati entro 12 mesi dall'adozione del presente regolamento. La Commissione dovrebbe valutare l'efficacia delle disposizioni volte a garantire la disponibilità e l'usabilità dei portafogli europei di identità digitale per gli utenti dopo 24 mesi dalla loro introduzione.

(29) La divulgazione selettiva è un concetto che conferisce al proprietario dei dati il potere di divulgare solo alcune parti di un insieme di dati più ampio, affinché il soggetto ricevente ottenga solo le informazioni necessarie, ad esempio un utente che comunica a una parte facente affidamento sulla certificazione solo i dati necessari per la prestazione di un servizio richiesto da un utente. Il portafoglio europeo di identità digitale dovrebbe consentire, a livello tecnico, la divulgazione selettiva degli attributi alle parti facenti affidamento sulla certificazione. Tali attributi divulgati selettivamente, anche quando in origine sono parti di una serie di attestati elettronici distinti, possono essere successivamente combinati e presentati alle parti facenti affidamento sulla certificazione. Tale caratteristica dovrebbe diventare una caratteristica di progettazione di base, rafforzando in tal modo la praticità e la tutela dei dati personali, compresa la minimizzazione di questi ultimi.

(30) Gli attributi forniti dai prestatori di servizi fiduciari qualificati nell'ambito degli attestati di attributi qualificati dovrebbero essere verificati rispetto alle fonti autentiche, direttamente dal prestatore di servizi fiduciari qualificato oppure tramite intermediari designati riconosciuti a livello nazionale conformemente al diritto nazionale o dell'Unione ai fini dello scambio sicuro di attributi attestati tra i gestori di identità o i prestatori di servizi di attestazione di attributi e le parti facenti affidamento sulla certificazione. Gli Stati membri dovrebbero istituire meccanismi appropriati a livello nazionale per far sì che i prestatori di servizi fiduciari qualificati che rilasciano attestati elettronici di attributi qualificati siano in grado, sulla base del consenso della persona a cui è rilasciato l'attestato, di verificare l'autenticità degli attributi che fanno affidamento su fonti autentiche. Tra i meccanismi appropriati figurano il ricorso a intermediari specifici o a soluzioni tecniche conformi al diritto nazionale che consentono l'accesso a fonti autentiche. Garantire la disponibilità di un meccanismo che consenta la verifica degli attributi rispetto alle fonti autentiche dovrebbe facilitare la conformità dei prestatori di servizi fiduciari qualificati che forniscono attestati elettronici di attributi qualificati agli obblighi loro imposti dal presente regolamento. L'allegato VI contiene un elenco di categorie di attributi per i quali gli Stati membri dovrebbero assicurare che siano adottate misure per consentire ai fornitori qualificati di attestati elettronici di attributi di verificare mediante mezzi elettronici, su richiesta dell'utente, la loro autenticità rispetto alla fonte autentica pertinente. Gli Stati membri dovrebbero concordare attributi specifici che rientrano in queste categorie.

(31) L'identificazione elettronica sicura e la fornitura di attestati di attributi dovrebbero offrire al settore dei servizi finanziari una maggiore flessibilità e ulteriori soluzioni per consentire l'identificazione di clienti e lo scambio di attributi specifici necessari per rispettare, ad esempio, le prescrizioni in materia di adeguata verifica della clientela di cui al regolamento antiriciclaggio [riferimento da aggiungere dopo l'adozione della proposta] o i requisiti di idoneità derivanti dalla normativa in materia di protezione degli investitori, oppure per sostenere l'adempimento delle prescrizioni in materia di autenticazione forte del cliente per l'identificazione online ai fini dell'accesso all'account e l'avvio di transazioni nel settore dei servizi di pagamento.

(31 bis) Per garantire la coerenza delle pratiche di certificazione in tutta l'UE, la Commissione dovrebbe emanare orientamenti in materia di certificazione e ricertificazione dei dispositivi qualificati per la creazione di una firma elettronica e dei dispositivi qualificati per la creazione di un sigillo elettronico, anche per quanto riguarda la loro validità e le relative limitazioni temporali. Il presente regolamento non impedisce agli Stati membri di autorizzare gli organismi pubblici o privati che dispongono di dispositivi qualificati per la creazione di una firma elettronica certificati di prorogare temporaneamente la validità della certificazione qualora non sia stato possibile effettuare una ricertificazione dello stesso dispositivo entro il termine stabilito per legge per un motivo diverso da una violazione o da un incidente di sicurezza, e fatta salva la pratica di certificazione applicabile.

(32) I servizi di autenticazione dei siti web offrono agli utenti un elevato livello di garanzia del fatto che dietro a quei siti web vi sono entità reali e legittime, indipendentemente dalla piattaforma utilizzata per la visualizzazione. Tali servizi contribuiscono a diffondere sicurezza e fiducia nelle transazioni commerciali online e a ridurre i casi di frode online. L'uso dei servizi di autenticazione dei siti web da parte di siti web dovrebbe essere volontario. Tuttavia, affinché l'autenticazione dei siti web divenga un mezzo per rafforzare la fiducia, fornire un'esperienza migliore all'utente e promuovere la crescita nel mercato interno, il presente regolamento dovrebbe stabilire obblighi minimi in materia di sicurezza e responsabilità per i prestatori di servizi di autenticazione dei siti web e i loro servizi. A tal fine i fornitori di browser web dovrebbero garantire il supporto dei certificati qualificati di autenticazione di siti web e l'interoperabilità con gli stessi a norma del regolamento (UE) n. 910/2014. Dovrebbero riconoscere i certificati qualificati di autenticazione dei siti web e consentire all'utente finale di visualizzare i dati di identità certificati nell'ambiente del browser sulla base delle specifiche stabilite in conformità del presente regolamento. Il riconoscimento di un certificato qualificato di autenticazione dei siti web quale certificato qualificato rilasciato da un prestatore di servizi fiduciari qualificato dovrebbe garantire che i dati di identità inclusi nel certificato possano essere autenticati e verificati conformemente al presente regolamento. Ciò non dovrebbe pregiudicare la possibilità per i fornitori di browser web di affrontare non conformità gravi connesse alla violazione della sicurezza e alla perdita di integrità di singoli certificati, contribuendo in tal modo alla sicurezza online degli utenti finali. Le autorità pubbliche degli Stati membri dovrebbero valutare la possibilità di integrare nei loro siti web i certificati qualificati di autenticazione di siti web al fine di promuoverne l'utilizzo e proteggere ulteriormente i cittadini.

(33) Molti Stati membri hanno introdotto requisiti nazionali per i servizi che forniscono un'archiviazione digitale sicura e affidabile al fine di consentire la conservazione a lungo termine di dati elettronici e per i servizi fiduciari associati. Al fine di garantire la certezza del diritto, la fiducia e l'armonizzazione in tutti gli Stati membri, è opportuno istituire un quadro giuridico per i servizi di archiviazione elettronica qualificati, ispirato al quadro per gli altri servizi fiduciari di cui al presente regolamento. Tale quadro dovrebbe offrire ai prestatori di servizi fiduciari e agli utenti un pacchetto di strumenti efficiente che comprenda requisiti funzionali per il servizio di archiviazione elettronica, nonché chiari effetti giuridici in caso di utilizzo di un servizio di archiviazione elettronica qualificato. Tali disposizioni dovrebbero applicarsi ai documenti creati elettronicamente e ai documenti cartacei che sono stati scannerizzati e digitalizzati. Ove necessario, tali disposizioni dovrebbero consentire che i dati elettronici conservati siano trasferiti su supporti o formati diversi al fine di estenderne la durabilità e la leggibilità oltre il periodo di validità tecnologica, riducendo nel contempo al minimo, nella misura più ampia possibile, le perdite e le alterazioni. Quando i dati elettronici trasmessi al servizio di archiviazione digitale contengono una o più firme elettroniche qualificate ovvero uno o più sigilli elettronici qualificati, il servizio dovrebbe utilizzare procedure e tecnologie in grado di estendere la loro affidabilità per il periodo di conservazione di tali dati, eventualmente ricorrendo all'uso di altri servizi fiduciari elettronici qualificati istituiti dal presente regolamento. Per la creazione delle prove di conservazione in caso di utilizzo di firme elettroniche, sigilli elettronici o validazioni temporali elettroniche, è opportuno utilizzare servizi fiduciari elettronici qualificati. Nella misura in cui i servizi di archiviazione elettronica non sono armonizzati dal presente regolamento, gli Stati membri possono mantenere o introdurre disposizioni nazionali, in conformità del diritto dell'Unione, relative a tali servizi, quali disposizioni specifiche che consentano alcune deroghe per i servizi integrati in un'organizzazione e utilizzati esclusivamente per gli "archivi interni" di tale organizzazione. Il presente regolamento non dovrebbe distinguere tra documenti creati elettronicamente e documenti fisici che sono stati digitalizzati.

(33 bis) Gli archivi nazionali e le istituzioni della memoria, in qualità di organizzazioni preposte alla conservazione del patrimonio documentario nell'interesse pubblico, sono generalmente incaricati di svolgere le rispettive attività dal diritto nazionale e non forniscono necessariamente servizi fiduciari ai sensi del presente regolamento. Nella misura in cui tali istituzioni non forniscono siffatti servizi, il presente regolamento non ne pregiudica il funzionamento.

(34) I registri elettronici sono una sequenza di registrazioni di dati elettronici che ne garantiscono l'integrità e l'accuratezza dell'ordine cronologico. Lo scopo dei registri elettronici è stabilire una sequenza cronologica delle registrazioni di dati per evitare che i beni digitali siano copiati e venduti a vari destinatari. I registri elettronici possono essere utilizzati, ad esempio, per le registrazioni digitali della proprietà nel commercio mondiale, del finanziamento esteso alla filiera, della digitalizzazione dei diritti di proprietà intellettuale o di prodotti di base come l'energia elettrica. Congiuntamente ad altre tecnologie, possono contribuire a fornire soluzioni per servizi pubblici più efficienti e trasformativi, quali il voto elettronico, la cooperazione transfrontaliera delle autorità doganali, la cooperazione transfrontaliera delle istituzioni accademiche o la registrazione delle proprietà immobiliari nei registri catastali decentrati. I registri elettronici qualificati creano una presunzione legale per l'ordine cronologico sequenziale univoco e accurato e l'integrità della registrazione dei dati nel registro. Gli attributi specifici dei registri elettronici, ossia l'ordine cronologico sequenziale delle registrazioni di dati, distinguono i registri elettronici da altri servizi fiduciari quali le validazioni temporali elettroniche e i servizi elettronici di recapito certificato. In particolare, né la validazione temporale dei documenti digitali, né il loro trasferimento mediante servizi elettronici di recapito certificato potrebbero impedire in misura sufficiente, in assenza di ulteriori misure tecniche o organizzative, che lo stesso bene digitale sia copiato e venduto più di una volta a parti diverse. Il processo di creazione e aggiornamento di un registro elettronico dipende dal tipo di registro utilizzato (centralizzato o distribuito).

(35) Al fine di evitare la frammentazione del mercato interno è opportuno stabilire un quadro giuridico paneuropeo che consenta il riconoscimento transfrontaliero dei servizi fiduciari per la registrazione dei dati nei registri elettronici qualificati. I prestatori di servizi fiduciari per i registri elettronici dovrebbero essere incaricati di verificare la registrazione sequenziale dei dati nel registro. Il presente regolamento lascia impregiudicati gli obblighi giuridici che gli utenti dei registri elettronici potrebbero dover rispettare ai sensi del diritto dell'Unione e nazionale. Ad esempio, i casi d'uso che comportano il trattamento di dati personali dovrebbero rispettare il regolamento (UE) 2016/679. I casi d'uso che riguardano cripto-attività dovrebbero essere conformi a tutte le norme finanziarie applicabili, ad esempio la direttiva relativa ai mercati degli strumenti finanziari[11], la direttiva relativa ai servizi di pagamento[12], la direttiva sulla moneta elettronica[13] e il possibile futuro regolamento relativo ai mercati delle cripto-attività, nonché alle norme antiriciclaggio che potrebbero essere incluse nel regolamento sul trasferimento di fondi[14], e potrebbero richiedere ai prestatori di servizi per le cripto-attività di verificare l'identità degli utenti dei registri elettronici al fine di rispettare le norme internazionali antiriciclaggio.

---

11 Direttiva 2014/65/UE del Parlamento europeo e del Consiglio, del 15 maggio 2014, relativa ai mercati degli strumenti finanziari e che modifica la direttiva 2002/92/CE (GU L 173 del 12.6.2014, pag. 349).

12 Direttiva (UE) 2015/2366 del Parlamento europeo e del Consiglio, del 25 novembre 2015, relativa ai servizi di pagamento nel mercato interno, che modifica le direttive 2002/65/CE, 2009/110/CE e 2013/36/UE e il regolamento (UE) n. 1093/2010, e abroga la direttiva 2007/64/CE (GU L 337 del 23.12.2015, pag. 35).

13 Direttiva 2009/110/CE del Parlamento europeo e del Consiglio, del 16 settembre 2009, concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica, che modifica le direttive 2005/60/CE e 2006/48/CE e che abroga la direttiva 2000/46/CE (GU L 267 del 10.10.2009, pag. 7).

14 Cfr. la proposta della Commissione, del 20.7.2021, relativa alla rifusione del regolamento (UE) 2015/847 del Parlamento europeo e del Consiglio, del 20 maggio 2015, riguardante i dati informativi che accompagnano i trasferimenti di fondi, COM/2021/422 final.

(36) Al fine di evitare la frammentazione e gli ostacoli dovuti a norme divergenti e restrizioni tecniche e di garantire un processo coordinato per non compromettere l'attuazione del futuro quadro per un'identità digitale europea, è necessario un processo per la cooperazione stretta e strutturata tra la Commissione, gli Stati membri e il settore privato. Per conseguire tale obiettivo gli Stati membri dovrebbero cooperare nell'ambito del quadro istituito dalla raccomandazione XXX/XXXX della Commissione [relativa a un pacchetto di strumenti comuni dell'Unione per un approccio coordinato verso un quadro europeo relativo a un'identità digitale][15] al fine di individuare un pacchetto di strumenti per un quadro per un'identità digitale europea. Il pacchetto di strumenti dovrebbe comprendere un'architettura tecnica completa e un quadro di riferimento, un insieme comune di norme e di riferimenti tecnici e una serie di orientamenti e descrizioni di migliori prassi che contemplino almeno tutti gli aspetti relativi alle funzionalità e all'interoperabilità dei portafogli europei di identità digitale, comprese le firme elettroniche, e del servizio fiduciario qualificato per gli attestati di attributi di cui al presente regolamento. In tale contesto, gli Stati membri dovrebbero anche raggiungere un accordo in merito agli elementi comuni di un modello di business e di una struttura tariffaria per i portafogli europei di identità digitale al fine di agevolarne l'adozione, in particolare da parte delle piccole e medie imprese in un contesto transfrontaliero. Il contenuto del pacchetto di strumenti dovrebbe evolvere di pari passo con i risultati della discussione e del processo di adozione del quadro per un'identità digitale europea e rispecchiare tali risultati.

(36 bis) Gli Stati membri dovrebbero stabilire norme relative alle sanzioni applicabili a violazioni quali le pratiche dirette o indirette che generano confusione tra servizi fiduciari non qualificati e servizi fiduciari qualificati o l'uso abusivo del marchio di fiducia UE da parte di prestatori di servizi fiduciari non qualificati. Il marchio di fiducia UE non dovrebbe essere utilizzato in condizioni che, direttamente o indirettamente, inducano a credere che i servizi fiduciari non qualificati offerti da tale prestatore siano qualificati.

---

15 [Inserire riferimento dopo l'adozione].

(36 ter) Il presente regolamento dovrebbe garantire un livello armonizzato di qualità, affidabilità e sicurezza dei servizi fiduciari qualificati, indipendentemente dal luogo in cui sono effettuate le operazioni. Pertanto, un prestatore di servizi fiduciari qualificato dovrebbe essere autorizzato a esternalizzare le sue operazioni relative alla prestazione di un servizio fiduciario qualificato al di fuori dell'Unione, qualora fornisca garanzie, assicurando che le attività di vigilanza e le verifiche possano essere eseguite come se tali operazioni fossero effettuate nell'Unione. Ove la conformità al regolamento non possa essere pienamente garantita, gli organismi di vigilanza dovrebbero poter adottare misure proporzionate e giustificate, compresa la revoca della qualifica del servizio fiduciario prestato.

(36 quater) Per garantire la certezza giuridica della validità delle firme elettroniche avanzate basate su certificati qualificati, è essenziale specificare le componenti della firma elettronica avanzata basata su certificati qualificati, che dovrebbero essere valutate dalla parte facente affidamento sulla certificazione che effettua la convalida di tale firma.

(36 quinquies) I prestatori di servizi fiduciari dovrebbero utilizzare algoritmi crittografici che riflettano le migliori pratiche vigenti e attuazioni affidabili di tali algoritmi al fine di garantire la sicurezza e l'affidabilità dei loro servizi fiduciari.

(36 sexies) Il presente regolamento dovrebbe stabilire l'obbligo per i prestatori di servizi fiduciari qualificati di verificare l'identità di una persona fisica o giuridica cui è rilasciato il certificato qualificato sulla base di vari metodi armonizzati in tutta l'UE. Tali metodi possono includere il ricorso a mezzi di identificazione elettronica che soddisfano i requisiti del livello di garanzia "significativo" in combinazione con ulteriori procedure armonizzate a distanza che garantiscono l'identificazione della persona con un elevato livello di affidabilità.

(36 septies) Gli emittenti dei portafogli europei di identità digitale e gli emittenti di mezzi di identificazione elettronica notificati che agiscono a titolo commerciale o professionale utilizzando i servizi di piattaforma di base offerti dai gatekeeper ai fini della fornitura di beni e servizi agli utenti finali o nel corso della stessa dovrebbero essere considerati utenti commerciali a norma dell'articolo 2, punto 21), del regolamento (UE) 2022/1925. I gatekeeper dovrebbero pertanto essere tenuti a garantire, a titolo gratuito, l'effettiva interoperabilità con lo stesso sistema operativo e le stesse componenti hardware o software disponibili o utilizzati nella fornitura dei loro servizi complementari e di supporto e di hardware, come pure a garantirne l'accesso ai fini dell'interoperabilità. Ciò dovrebbe consentire agli emittenti di portafogli europei di identità digitale e agli emittenti di mezzi di identificazione elettronica notificati di interconnettersi, attraverso interfacce o soluzioni analoghe, alle rispettive componenti con la stessa efficacia dei servizi o dell'hardware propri del gatekeeper.

(36 octies) Per mantenere il presente regolamento in linea con gli sviluppi attuali e seguire le pratiche sul mercato interno, gli atti delegati e di esecuzione adottati dalla Commissione dovrebbero essere riesaminati e, se necessario, aggiornati periodicamente. La valutazione della necessità di tali aggiornamenti dovrebbe tenere conto delle nuove tecnologie, pratiche, norme o specifiche tecniche emerse nel mercato interno.

(37) Il Garante europeo della protezione dei dati è stato consultato a norma dell'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio[16].

(38) È pertanto opportuno modificare di conseguenza il regolamento (UE) n. 910/2014,

---

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

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

Il regolamento (UE) n. 910/2014 è così modificato:

1) l'articolo 1 è sostituito dal seguente:

"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. A tal fine, il presente regolamento:

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

a ter) fissa le condizioni alle quali gli Stati membri 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, la convalida elettronica delle firme elettroniche, dei sigilli elettronici e dei relativi certificati, la convalida elettronica dei certificati di autenticazione di siti web, la conservazione elettronica delle firme elettroniche, dei sigilli elettronici e dei relativi certificati, l'archiviazione elettronica, gli attestati elettronici di attributi, la gestione di dispositivi qualificati per la creazione di firme elettroniche e sigilli elettronici a distanza e i registri elettronici;"

2) l'articolo 2 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

"1. Il presente regolamento si applica ai regimi di identificazione elettronica che sono stati notificati da uno Stato membro, ai portafogli europei di identità elettronica forniti dagli Stati membri e ai prestatori di servizi fiduciari che sono stabiliti nell'Unione.";

b) il paragrafo 3 è sostituito dal seguente:

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

3) l'articolo 3 è così modificato:

X) il punto 1 è sostituito dal seguente:

"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 una persona fisica o giuridica;"

a) il punto 2 è sostituito dal seguente:

"2) "mezzi di identificazione elettronica", un'unità materiale e/o immateriale, compresi i portafogli europei di identità digitale, contenente dati di identificazione personale e utilizzata per l'autenticazione per un servizio online o, se del caso, per un servizio offline;"

a bis) il punto 3 è sostituito dal seguente:

"3) "dati di identificazione personale", un insieme di dati, rilasciati conformemente al diritto dell'Unione o nazionale, che consente di stabilire l'identità di una persona fisica o giuridica, o di una persona fisica che rappresenta una persona fisica o giuridica;"

b) il punto 4 è sostituito dal seguente:

"4) "regime di identificazione elettronica", un sistema di identificazione elettronica nell'ambito del quale si forniscono mezzi di identificazione elettronica alle persone fisiche o giuridiche, o alle persone fisiche che rappresentano persone fisiche o giuridiche;"

b bis) il punto 5 è sostituito dal seguente:

"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;"

b ter) è inserito il seguente punto 5 bis):

"5 bis) "utente", una persona fisica o giuridica, o una persona fisica che rappresenta una persona fisica o giuridica, che utilizza servizi fiduciari o mezzi di identificazione elettronica, forniti a norma del presente regolamento;"

c) il punto 14 è sostituito dal seguente:

"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;"

d) il punto 16 è sostituito dal seguente:

"16) "servizio fiduciario", un servizio elettronico fornito normalmente dietro remunerazione e consistente nei seguenti elementi:

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

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

b) creazione di firme elettroniche o di sigilli elettronici;

c) convalida di firme elettroniche o di sigilli elettronici;

d) conservazione di firme elettroniche, di sigilli elettronici, di certificati di firme elettroniche o di certificati di sigilli elettronici;

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

f) rilascio di attestati elettronici di attributi;

f bis) convalida di attestati elettronici di attributi;

g) creazione di validazioni temporali elettroniche;

g bis) convalida di validazioni temporali elettroniche;

g ter) prestazione di servizi elettronici di recapito certificato;

g quater) convalida dei dati trasmessi tramite servizi elettronici di recapito certificato e relative prove;

h) archiviazione elettronica di dati elettronici; oppure

i) registrazione di dati elettronici in un registro elettronico;"

d bis) il punto 18 è sostituito dal seguente:

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

e) il punto 21 è sostituito dal seguente:

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

f) sono inseriti i seguenti punti 23 bis e 23 ter:

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

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

g) il punto 29 è sostituito dal seguente:

"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;"

h) il punto 41 è sostituito dal seguente:

"41) "convalida", il processo di verifica e conferma della validità dei dati in forma elettronica conformemente ai requisiti del presente regolamento;"

i) sono inseriti i seguenti punti da 42) a 55 ter):

"42) "portafoglio europeo di identità digitale", un mezzo di identificazione elettronica che consente all'utente di conservare e consultare dati di identità, compresi dati di identificazione personale, e attestati elettronici di attributi collegati alla sua identità, fornirli su richiesta alle parti facenti affidamento sulla certificazione e utilizzarli per l'autenticazione, online e, se del caso, offline, per un servizio, conformemente all'articolo 6 bis, e che consente di firmare mediante firme elettroniche qualificate e 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;

45 bis) "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 a norma dell'articolo 45 quinquies bis e che soddisfa i requisiti di cui all'allegato VII;

46) "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 ed 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;

47) "archiviazione elettronica", un servizio che consente la ricezione, la conservazione, la consultazione e la cancellazione di dati 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;

48) "servizio di archiviazione elettronica qualificato", un servizio di archiviazione elettronica che soddisfa i requisiti di cui all'articolo 45 octies bis;

49) "marchio di fiducia UE per i portafogli di identità digitale", un'indicazione verificabile semplice, riconoscibile e chiara del fatto che un portafoglio europeo di identità digitale è stato fornito conformemente al presente regolamento;

50) "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;

53) "registro elettronico", una sequenza di registrazioni di dati elettronici che ne garantisce l'integrità e l'accuratezza dell'ordine cronologico;

53 bis) "registro elettronico qualificato", un registro elettronico che soddisfa i requisiti di cui all'articolo 45 decies;

54) "dati personali", qualsiasi informazione di cui all'articolo 4, punto 1, del regolamento (UE) 2016/679;

55) "abbinamento delle registrazioni": un processo in cui i dati di identificazione personale, i mezzi di identificazione personale, gli attestati elettronici di attributi qualificati o gli attestati di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto sono abbinati o collegati a un account esistente appartenente alla stessa persona;

55 bis) "identificatore unico e persistente", un identificatore che può consistere in dati di identificazione nazionali o settoriali unici o multipli, associato a un unico utente all'interno di un determinato sistema e persistente nel tempo;

55 ter) "registrazione di dati", dati elettronici registrati con i metadati (o attributi) connessi che supportano il trattamento dei dati;

55 quater) "uso offline dei portafogli europei di identità digitale", un'interazione tra un utente e una parte facente affidamento sulla certificazione in un luogo fisico, laddove il portafoglio non è tenuto ad accedere a sistemi a distanza tramite reti di comunicazione elettronica ai fini dell'interazione.

Articolo 5

Pseudonimi nelle transazioni elettroniche

Fatti salvi gli effetti giuridici che il diritto nazionale attribuisce agli pseudonimi, l'uso di pseudonimi nelle transazioni elettroniche non è vietato.";

5) al capo II, prima dell'articolo 6 bis è inserito il titolo seguente:

"SEZIONE I

Portafogli europei di identità digitale;

7) sono inseriti gli articoli 6 bis, 6 ter, 6 quater e 6 quinquies seguenti:

"*Articolo 6 bis*

Portafogli europei di identità digitale

1. Al fine di garantire che tutte le persone fisiche e giuridiche nell'Unione abbiano un accesso sicuro, affidabile e transfrontaliero senza soluzione di continuità a servizi pubblici e privati, ciascuno Stato membro garantisce la fornitura di un portafoglio europeo di identità digitale entro 24 mesi dall'entrata in vigore degli atti di esecuzione di cui al paragrafo 11 e all'articolo 6 quater, paragrafo 4.

2. I portafogli europei di identità digitale sono forniti:

   a) dagli Stati membri;

   b) su incarico di uno Stato membro; o

   c) a titolo indipendente da uno Stato membro ma sono riconosciuti dagli Stati membri.

3. I portafogli europei di identità digitale sono mezzi di identificazione elettronica che consentono all'utente, in modo trasparente e tracciabile da quest'ultimo di:

   a) richiedere, selezionare, combinare, conservare, cancellare e presentare in modo sicuro gli attestati elettronici di attributi e i dati di identificazione personale alle parti facenti affidamento sulla certificazione, anche per l'autenticazione online e, se del caso, offline al fine di utilizzare servizi pubblici e privati, garantendo nel contempo che sia possibile la divulgazione selettiva dei dati;

   b) firmare mediante firme elettroniche qualificate e apporre sigilli mediante sigilli elettronici qualificati.

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

a) forniscono un insieme comune di interfacce:

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

2) alle parti facenti affidamento sulla certificazione ai fini della richiesta dei dati di identificazione personale e degli attestati elettronici di attributi;

3) per la presentazione alle parti facenti affidamento sulla certificazione di dati di identificazione personale o attestati elettronici di attributi online e, se del caso, anche offline;

4) 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";

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

b bis) garantiscono che l'identità delle parti facenti affidamento sulla certificazione possa essere convalidata mediante l'attuazione di meccanismi di autenticazione a norma dell'articolo 6 ter;

c) soddisfano i requisiti di cui all'articolo 8 per quanto riguarda il livello di garanzia "elevato" applicabile, mutatis mutandis, alla gestione e all'uso dei dati di identificazione personale attraverso il portafoglio, comprese l'identificazione e l'autenticazione elettroniche;

e) garantiscono che i dati di identificazione personale di cui all'articolo 12, paragrafo 4, lettera d), rappresentino in modo univoco e persistente la persona fisica, la persona giuridica o la persona fisica che rappresenta la persona fisica o giuridica associata al portafoglio.

4 bis. Gli Stati membri prevedono procedure che consentano all'utente di segnalare eventuali perdite o abusi del portafoglio e di chiederne la revoca.

5. Gli Stati membri prevedono meccanismi di convalida per i portafogli europei di identità digitale:

a) per garantire che sia possibile verificarne l'autenticità e la validità;

d) per consentire all'utente di autenticare le parti facenti affidamento sulla certificazione conformemente all'articolo 6 ter.

6. I portafogli europei di identità digitale sono emessi nell'ambito di un regime di identificazione elettronica notificato il cui livello di garanzia è "elevato".

6 bis. L'emissione, l'uso per l'autenticazione e la revoca dei portafogli europei di identità digitale sono gratuiti per le persone fisiche.

6 ter. Fatto salvo l'articolo 6 quinquies ter, 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.

7. Gli utenti hanno il pieno controllo dell'uso del portafoglio europeo di identità digitale e dei dati in esso contenuti. L'emittente del portafoglio europeo di identità digitale non raccoglie informazioni relative all'uso del portafoglio che non sono necessarie per la prestazione dei servizi del portafoglio, né combina i dati di identificazione personale e 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 emittente o da servizi di terzi che non sono necessari per la prestazione dei servizi del portafoglio, a meno che l'utente non l'abbia richiesto espressamente. I dati personali relativi alla fornitura dei portafogli europei di identità digitale sono tenuti logicamente separati dagli altri dati detenuti dall'emittente dei portafogli europei di identità digitale. Se il portafoglio europeo di identità digitale è fornito da soggetti privati conformemente al paragrafo 2, lettere b) e c), si applicano, mutatis mutandis, le disposizioni di cui all'articolo 45 septies, paragrafo 4.

7 bis. 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 notificate che intendono avvalersi dei portafogli europei di identità digitale a norma dell'articolo 6 ter, paragrafo 2;

b) gli organismi responsabili della fornitura dei portafogli europei di identità digitale a norma dell'articolo 6 bis, paragrafo 1;

c) gli organismi responsabili di garantire che i dati di identificazione personale siano associati al portafoglio a norma dell'articolo 6 bis, paragrafo 4, lettera e);

La notifica fornisce inoltre informazioni sul meccanismo che consente la convalida dei dati di identificazione personale di cui all'articolo 12, paragrafo 4, e dell'identità delle parti facenti affidamento sulla certificazione.

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

8. L'articolo 11 si applica, mutatis mutandis, al portafoglio europeo di identità digitale.

9. L'articolo 24, paragrafo 2, lettere b), e), g) e h), si applica, mutatis mutandis, all'emittente dei portafogli europei di identità digitale.

10. Il portafoglio europeo di identità digitale è reso accessibile alle persone con disabilità conformemente ai requisiti di accessibilità di cui alla direttiva (UE) 2019/882.

11. Entro 6 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante un atto di esecuzione relativo all'implementazione del portafoglio europeo di identità digitale, stabilisce specifiche tecniche e operative e norme di riferimento applicabili ai requisiti di cui ai paragrafi 3, 4, 5 e 7 bis. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

11 bis. La Commissione stabilisce specifiche tecniche e operative nonché norme di riferimento per facilitare l'acquisizione (*onboarding* nel portafoglio europeo di identità digitale degli utenti che utilizzano mezzi di identificazione elettronica conformi al livello "elevato" o mezzi di identificazione elettronica conformi al livello "significativo" unitamente a ulteriori procedure di *onboarding* a distanza che, insieme, soddisfano i requisiti del livello di garanzia "elevato". Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 6 ter

Parti facenti affidamento sulla certificazione dei portafogli europei di identità digitale

1. Qualora intendano avvalersi dei portafogli europei di identità digitale forniti conformemente al presente regolamento, le parti facenti affidamento sulla certificazione che forniscono servizi pubblici o privati ne danno notifica allo Stato membro in cui sono stabilite.

1 bis. La procedura di notifica è efficace sotto il profilo dei costi e proporzionata al rischio e garantisce che le parti facenti affidamento sulla certificazione forniscano almeno le informazioni necessarie per autenticarsi nei portafogli europei di identità digitale. Ciò dovrebbe comprendere, come minimo, lo Stato membro in cui sono stabilite e il nome della parte facente affidamento sulla certificazione e, se del caso, il suo numero di registrazione quale appare nei documenti ufficiali.

1 ter. L'obbligo di notifica lascia impregiudicati altri obblighi di notifica e registrazione in conformità del diritto dell'Unione o nazionale, come quelli applicabili a categorie particolari di dati personali, che possono richiedere ulteriori obblighi di autorizzazione.

1 quater. Gli Stati membri possono esentare le parti facenti affidamento sulla certificazione dall'obbligo di notifica qualora il diritto dell'Unione o nazionale non preveda specifici obblighi di notifica o registrazione per accedere alle informazioni fornite mediante il portafoglio europeo di identità digitale. Non è necessario che le parti facenti affidamento sulla certificazione esentate siano tenute ad autenticarsi nel portafoglio europeo di identità digitale.

1 quinquies. Le parti facenti affidamento sulla certificazione notificate a norma del presente articolo informano senza indugio lo Stato membro in merito a qualsiasi successiva modifica delle informazioni inizialmente fornite.

2. Le parti facenti affidamento sulla certificazione garantiscono l'attuazione dei meccanismi di autenticazione di cui all'articolo 6 bis, paragrafo 4, lettera b bis).

3. Le parti facenti affidamento sulla certificazione sono responsabili dell'esecuzione della procedura di autenticazione delle persone e della convalida degli attestati elettronici di attributi provenienti dai portafogli europei di identità digitale ottenuti tramite l'interfaccia comune conformemente all'articolo 6 bis, paragrafo 4, lettera a), punto 2).

4. Entro 6 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante un atto di esecuzione relativo all'implementazione dei portafogli europei di identità digitale di cui all'articolo 6 bis, paragrafo 11, stabilisce specifiche tecniche e operative per i requisiti di cui ai paragrafi 1, 1 bis e 1 quinquies. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 6 quater

Certificazione dei portafogli europei di identità digitale

1. La conformità dei portafogli europei di identità digitale ai requisiti di cui all'articolo 6 bis, paragrafi 3, 4 e 5, al requisito della separazione logica di cui all'articolo 6 bis, paragrafo 7, e, se del caso, ai requisiti di cui all'articolo 6 bis, paragrafo 11 bis, è certificata da organismi di valutazione della conformità accreditati a norma dell'articolo 60 del regolamento sulla cibersicurezza e ai sistemi, alle specifiche, alle norme e alle procedure di cui al paragrafo 4, lettere a), a bis) e a bis bis), e designati dagli Stati membri. La certificazione non supera i cinque anni, subordinatamente a una valutazione delle vulnerabilità periodica effettuata ogni due anni. Qualora siano individuate vulnerabilità a cui non è posto rimedio entro tre mesi, la certificazione è annullata.

2. Per quanto riguarda la conformità ai requisiti in materia di protezione dei dati di cui all'articolo 6 bis, paragrafo 7, la certificazione di cui al paragrafo 1 può essere integrata da una certificazione a norma dell'articolo 42 del regolamento (UE) 2016/679.

3. La conformità dei portafogli europei di identità digitale, o di parti di essi, ai pertinenti requisiti in materia di cibersicurezza di cui all'articolo 6 bis, paragrafi 3, 4, 5, 7 e, se del caso, paragrafo 11 bis, è certificata dagli organismi di valutazione della conformità di cui al paragrafo 1, nell'ambito dei pertinenti sistemi di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881, come menzionato conformemente al paragrafo 4, lettere a) e a bis).

3 bis. I portafogli europei di identità digitale certificati non sono soggetti ai requisiti di cui agli articoli 7 e 9.

4. Entro 6 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, redige:

a) un elenco dei sistemi di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881, necessari per la certificazione dei portafogli europei di identità digitale di cui al paragrafo 3;

a bis) specifiche, procedure e norme di riferimento per il loro uso nell'ambito dei pertinenti sistemi di certificazione della cibersicurezza elencati conformemente alla lettera a);

a bis bis) un elenco di specifiche, procedure e norme di riferimento che stabiliscono requisiti comuni di certificazione non contemplati dai pertinenti sistemi di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881 ai fini della certificazione di cui al paragrafo 1, nell'intento di dimostrare che un portafoglio europeo di identità digitale soddisfa i requisiti di cui al paragrafo 1;

b) specifiche tecniche, procedurali, organizzative e operative per la designazione degli organismi di valutazione della conformità di cui al paragrafo 1 e, per quanto riguarda i requisiti di certificazione stabiliti a norma della lettera a bis bis), per il monitoraggio e il riesame dei sistemi di certificazione e dei relativi metodi di valutazione utilizzati da tali organismi, nonché dei certificati e delle relazioni di certificazione da essi rilasciati.

5. Gli Stati membri comunicano alla Commissione i nomi e gli indirizzi degli organismi pubblici o privati di cui al paragrafo 1. La Commissione mette tali informazioni a disposizione degli Stati membri.

6. Gli atti di esecuzione di cui al paragrafo 4 sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 6 quinquies

Pubblicazione di un elenco dei portafogli europei di identità digitale certificati

1. Gli Stati membri informano senza indebito ritardo la Commissione in merito ai portafogli europei di identità digitale che sono stati forniti a norma dell'articolo 6 bis e certificati dagli organismi di cui all'articolo 6 quater, paragrafo 1. Essi informano inoltre senza indebito ritardo la Commissione dell'eventuale annullamento della certificazione.

2. Sulla base delle informazioni pervenutele, la Commissione redige, pubblica e aggiorna un elenco a lettura ottica dei portafogli europei di identità digitale certificati.

3. Entro 6 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante un atto di esecuzione relativo all'implementazione dei portafogli europei di identità digitale di cui all'articolo 6 bis, paragrafo 11, definisce i formati e le procedure applicabili ai fini dei paragrafi 1 e 2. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 6 quinquies bis

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 6 bis e dei meccanismi di convalida di cui all'articolo 6 bis, paragrafo 5, lettere a), d) o e), tale da pregiudicare la loro affidabilità o l'affidabilità di altri portafogli europei di identità digitale, l'emittente dei portafogli interessati, senza indebito ritardo, sospende l'emissione e l'uso del portafoglio europeo di identità digitale. Lo Stato membro in cui sono stati forniti i portafogli interessati informa gli Stati membri e la Commissione senza indebito ritardo. L'emittente dei portafogli interessati o lo Stato membro informa di conseguenza le parti facenti affidamento sulla certificazione e gli utenti.

2. Una volta posto rimedio alla violazione o alla compromissione di cui al paragrafo 1, l'emittente del portafoglio ristabilisce l'emissione e l'utilizzo del portafoglio europeo di identità digitale. Lo Stato membro in cui sono stati forniti i portafogli interessati informa gli Stati membri e la Commissione senza indebito ritardo. L'emittente dei portafogli interessati o lo Stato membro informa senza indebito ritardo le parti facenti affidamento sulla certificazione e gli utenti.

3. Qualora non sia posto rimedio alla violazione o alla compromissione di cui al paragrafo 1 entro tre mesi dalla sospensione, lo Stato membro interessato ritira il portafoglio europeo di identità digitale in questione e informa di conseguenza gli altri Stati membri e la Commissione. Qualora ciò sia giustificato dalla gravità della violazione, il passaporto europeo di identità digitale interessato è ritirato senza indebito ritardo.

4. La Commissione pubblica senza indebito ritardo le corrispondenti modifiche dell'elenco di cui all'articolo 6 quinquies nella *Gazzetta ufficiale dell'Unione europea*.

5. Entro 6 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante un atto di esecuzione relativo all'implementazione dei portafogli europei di identità digitale di cui all'articolo 6 bis, paragrafo 11, specifica ulteriormente le misure di cui ai paragrafi 1, 2 e 3. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 6 quinquies ter

Ricorso transfrontaliero ai portafogli europei di identità digitale

1. Qualora gli Stati membri richiedano l'identificazione elettronica mediante un mezzo di identificazione elettronica e un'autenticazione 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 per l'autenticazione dell'utente.

2. Qualora a norma del diritto nazionale o dell'Unione le parti private facenti affidamento sulla certificazione che forniscono servizi, ad eccezione delle microimprese e delle piccole imprese quali definite nella raccomandazione 2003/361/CE della Commissione, siano tenute a utilizzare l'autenticazione forte dell'utente per l'identificazione online, o qualora l'identificazione forte dell'utente 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, le parti private facenti affidamento sulla certificazione, entro 12 mesi dalla data della fornitura dei portafogli europei di identità digitale a norma dell'articolo 6 bis, paragrafo 1, e rigorosamente su richiesta volontaria dell'utente, accettano anche l'uso dei portafogli europei di identità digitale forniti conformemente al presente regolamento per quanto riguarda i dati minimi necessari per lo specifico servizio online per il quale è richiesta l'autenticazione degli utenti.

3. Qualora le piattaforme online di dimensioni molto grandi quali definite all'articolo 25, paragrafo 1, del regolamento [riferimento alla legge sui servizi digitali] impongano agli utenti di autenticarsi per accedere ai servizi online, esse accettano anche l'uso dei portafogli europei di identità digitale forniti conformemente al presente regolamento per l'autenticazione degli utenti, rigorosamente su richiesta volontaria dell'utente e per quanto riguarda i dati minimi necessari per lo specifico servizio online per il quale è richiesta l'autenticazione.

4. In collaborazione con gli Stati membri la Commissione incoraggia e facilita l'elaborazione di codici di condotta per contribuire all'ampia disponibilità e usabilità dei portafogli europei di identità digitale che rientrano nell'ambito di applicazione del presente regolamento. Tali codici di condotta facilitano l'accettazione dei mezzi di identificazione elettronica, compresi i portafogli europei di identità digitale che rientrano nell'ambito di applicazione del presente regolamento, in particolare da parte di prestatori di servizi facenti affidamento su servizi di identificazione elettronica di terzi per l'autenticazione degli utenti. La Commissione faciliterà l'elaborazione di tali codici di condotta in stretta collaborazione con tutti i pertinenti portatori di interessi e incoraggerà i prestatori di servizi a ultimare l'elaborazione dei codici di condotta entro 12 mesi dall'adozione del presente regolamento e ad attuarli efficacemente entro 18 mesi dall'adozione del medesimo.

5. Entro 24 mesi dall'introduzione dei portafogli europei di identità digitale la Commissione valuta se, sulla base dei dati relativi alla loro domanda, disponibilità e usabilità, sia opportuno imporre ad altri prestatori privati di servizi online di accettare l'uso dei portafogli europei di identità digitale, rigorosamente su richiesta volontaria dell'utente. I criteri di valutazione includono le dimensioni della base utenti, la presenza transfrontaliera dei prestatori di servizi, gli sviluppi tecnologici, l'evoluzione dei modelli di utilizzo e la domanda dei consumatori.";

8) prima dell'articolo 7 è inserito il titolo seguente:

"SEZIONE II

REGIMI DI IDENTIFICAZIONE ELETTRONICA";

9) la frase introduttiva dell'articolo 7 è così modificata:

"A norma dell'articolo 9, paragrafo 1, gli Stati membri che non l'abbiano ancora fatto notificano, entro 24 mesi dall'entrata in vigore degli atti di esecuzione di cui all'articolo 6 bis, paragrafo 11, e all'articolo 6 quater, paragrafo 4, almeno un regime di identificazione elettronica comprendente almeno un mezzo di identificazione del livello di garanzia "elevato". Un regime di identificazione elettronica è ammesso alla notifica ai sensi dell'articolo 9, paragrafo 1, purché soddisfi tutte le seguenti condizioni:";

10) all'articolo 9, i paragrafi 2 e 3 sono sostituiti dai seguenti:

"2. La Commissione pubblica nella *Gazzetta ufficiale dell'Unione europea* un elenco dei regimi di identificazione elettronica notificati a norma del paragrafo 1 e le informazioni fondamentali al riguardo.

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.";

12) è inserito il seguente articolo 11 bis:

"*Articolo 11 bis*

Abbinamento delle registrazioni

1. Quando i mezzi di identificazione elettronica notificati o i portafogli europei di identità digitale sono usati per l'autenticazione, gli Stati membri in qualità di parti facenti affidamento sulla certificazione garantiscono l'abbinamento delle registrazioni.

2. Al fine di fornire i portafogli europei di identità digitale gli Stati membri includono nell'insieme minimo di dati di identificazione personale di cui all'articolo 12, paragrafo 4, lettera d), almeno un identificatore unico e persistente conformemente al diritto dell'Unione e nazionale, al fine di identificare l'utente, su sua richiesta, nei casi in cui l'identificazione dell'utente sia prescritta dalla legge.

2 bis. Gli Stati membri prevedono misure tecniche e organizzative per garantire un livello elevato di protezione dei dati personali utilizzati per l'abbinamento delle registrazioni e per prevenire la profilazione degli utenti.

2 bis bis. Gli Stati membri possono disporre, conformemente al diritto nazionale, che l'utente del portafoglio europeo di identità digitale sia in grado di chiedere che un identificatore unico e persistente incluso nell'insieme minimo di dati di identificazione personale e associato al portafoglio a norma dell'articolo 6 bis, paragrafo 4, lettera e), sia sostituito da un altro identificatore unico e persistente rilasciato dallo Stato membro.

3. Entro 6 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante un atto di esecuzione, specifica ulteriormente le misure di cui al paragrafo 1. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

3 bis. Entro 6 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante un atto di esecuzione, specifica ulteriormente le misure di cui ai paragrafi 2 e 2 bis bis. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

13) l'articolo 12 è così modificato:

Cooperazione e interoperabilità

a) al paragrafo 3, la lettera d) è soppressa;

b) al paragrafo 4, la lettera d) è sostituita dalla seguente:

"d) un riferimento a un insieme minimo di dati di identificazione personale necessari a rappresentare in modo univoco e persistente una persona fisica, una persona giuridica o una persona fisica che rappresenta una persona fisica o giuridica;"

b bis) al paragrafo 5, è aggiunta la seguente lettera c):

"c) un approccio analogo nei confronti di servizi online che accettano l'uso dei portafogli europei di identità digitale forniti a norma del presente regolamento.";

c) al paragrafo 6, la lettera a) è sostituita dalla seguente:

"a) lo scambio di informazioni, esperienze e buone prassi per quanto riguarda i regimi di identificazione elettronica e, in particolare, i requisiti tecnici connessi all'interoperabilità, all'abbinamento delle registrazioni e ai livelli di garanzia;"

c bis) al paragrafo 6, è aggiunta la seguente lettera e):

"e) lo scambio di informazioni, esperienze e buone prassi e la pubblicazione di orientamenti sulle modalità di progettazione, sviluppo e attuazione dei servizi online al fine di avvalersi dei portafogli digitali europei.";

14) sono inseriti i seguenti articoli 12 bis e 12 ter:

"Articolo 12 bis

Certificazione dei regimi di identificazione elettronica

1. La conformità dei regimi di identificazione elettronica da notificare ai requisiti di cui al presente regolamento è certificata per dimostrare la conformità di tali regimi o di parti di essi ai requisiti di cui all'articolo 8, paragrafo 2, per quanto riguarda i livelli di garanzia dei regimi di identificazione elettronica nell'ambito di un pertinente sistema di certificazione della cibersicurezza a norma del regolamento (UE) 2019/881, o di parti di essi, nella misura in cui il certificato di cibersicurezza o parti di esso contemplino i requisiti di cui all'articolo 8, paragrafo 2, per quanto riguarda i livelli di garanzia dei regimi di identificazione elettronica. La certificazione non supera i cinque anni, subordinatamente a una valutazione delle vulnerabilità periodica effettuata ogni due anni. Qualora siano individuate vulnerabilità a cui non è posto rimedio entro tre mesi, la certificazione è annullata.

   La certificazione è effettuata da organismi di valutazione della conformità, pubblici o privati accreditati, designati dagli Stati membri e in conformità del regolamento (CE) n. 765/2008.

2. La valutazione tra pari dei regimi di identificazione elettronica di cui all'articolo 12, paragrafo 6, lettera c), non si applica ai regimi di identificazione elettronica, o a parti di essi, certificati conformemente al paragrafo 1.

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

3. Gli Stati membri notificano alla Commissione i nomi e gli indirizzi degli organismi pubblici o privati di cui al paragrafo 1. La Commissione mette tali informazioni a disposizione degli Stati membri.

Articolo 12 ter

Accesso a componenti hardware e software

Gli emittenti dei portafogli europei di identità digitale e gli emittenti di mezzi di identificazione elettronica notificati che agiscono a titolo commerciale o professionale utilizzando i servizi di piattaforma di base definiti all'articolo 2, paragrafo 2, del regolamento (UE) 2022/1925 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 a norma dell'articolo 2, punto 21), del regolamento (UE) 2022/1925.";

17) all'articolo 13, il paragrafo 1 è sostituito dal seguente:

"1. Fatto salvo il paragrafo 2, i prestatori di servizi fiduciari sono responsabili di danni causati, con dolo o per negligenza, a qualsiasi persona fisica o giuridica in seguito a un mancato adempimento degli obblighi di cui al presente regolamento.

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 di un prestatore di servizi fiduciari qualificato, salvo se questi dimostra che il danno di cui al primo comma si è verificato senza suo dolo o negligenza.";

18) l'articolo 14 è sostituito dal seguente:

"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 da un'organizzazione internazionale siano riconosciuti a norma di una decisione di esecuzione o un accordo concluso fra l'Unione e il paese terzo o l'organizzazione internazionale a norma dell'articolo 218 del trattato.

2. Le decisioni di esecuzione e gli accordi 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 o presso le organizzazioni internazionali 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.

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

3. Le decisioni di esecuzione di cui al paragrafo 1 sono adottate secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

19) l'articolo 15 è sostituito dal seguente:

"*Articolo 15*

Accessibilità per le persone con disabilità

La fornitura di servizi fiduciari e di prodotti destinati all'utente finale impiegati per la prestazione di tali servizi è resa accessibile alle persone con disabilità conformemente ai requisiti di accessibilità di cui alla direttiva (UE) 2019/882 sui requisiti di accessibilità dei prodotti e dei servizi.";

20) l'articolo 17 è così modificato:

a) il paragrafo 4 è così modificato:

1) al paragrafo 4, la lettera c) è sostituita dalla seguente:

"c) informare le pertinenti autorità nazionali competenti degli Stati membri interessati, designate a norma della direttiva (UE) XXXX/XXXX [NIS2], in merito a violazioni significative della sicurezza o a perdite di integrità di cui vengono a conoscenza nello svolgimento dei loro compiti. Qualora la violazione significativa della sicurezza o la perdita di integrità riguardi altri Stati membri, l'organismo di vigilanza informa il punto di contatto unico dello Stato membro interessato designato a norma della direttiva (UE) XXXX/XXXX [NIS2] e gli organismi di vigilanza designati a norma dell'articolo 17 del presente regolamento degli altri Stati membri interessati. L'organismo di vigilanza notificato informa il pubblico o impone al prestatore di servizi fiduciari di farlo, ove accerti che la divulgazione della violazione della sicurezza o della perdita di integrità sia nell'interesse pubblico;"

2) la lettera f) è sostituita dalla seguente:

"f) cooperare con le competenti autorità di controllo istituite a norma 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;"

b) il paragrafo 6 è sostituito dal seguente:

"6. Entro il 31 marzo di ogni anno ciascun organismo di vigilanza presenta alla Commissione una relazione sulle sue principali attività del precedente anno civile.";

c) il paragrafo 8 è sostituito dal seguente:

"8. Entro 12 mesi dall'entrata in vigore del presente regolamento, la Commissione adotta orientamenti sull'esercizio, da parte degli organismi di vigilanza, dei compiti di cui al paragrafo 4 e, mediante atti di esecuzione adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2, definisce i formati e le procedure relativi alla relazione di cui al paragrafo 6.";

21) l'articolo 18 è così modificato:

a) il titolo dell'articolo 18 è sostituito dal seguente:

"Assistenza reciproca e cooperazione";

b) il paragrafo 1 è sostituito dal seguente:

"1. Gli organismi di vigilanza collaborano fra loro al fine di scambiarsi buone prassi e informazioni relative alla prestazione di servizi fiduciari.";

c) sono aggiunti i seguenti paragrafi 4 e 5:

"4. Gli organismi di vigilanza e le autorità nazionali competenti a norma della direttiva (UE) XXXX/XXXX del Parlamento europeo e del Consiglio [NIS2] cooperano e si assistono reciprocamente al fine di garantire che i prestatori di servizi fiduciari rispettino i requisiti di cui al presente regolamento e alla direttiva (UE) XXXX/XXXX [NIS2]. Gli organismi di vigilanza chiedono alle autorità nazionali competenti a norma della direttiva XXXX/XXXX [NIS2] di svolgere azioni di vigilanza per verificare il rispetto, da parte dei prestatori di servizi fiduciari, dei requisiti di cui alla direttiva XXXX/XXXX (NIS2), di imporre ai prestatori di servizi fiduciari di rimediare a eventuali mancati adempimenti di tali requisiti, di fornire tempestivamente i risultati di eventuali attività di vigilanza connesse ai prestatori di servizi fiduciari e di informare gli organismi di vigilanza in merito a pertinenti incidenti notificati conformemente alla direttiva XXXX/XXXX [NIS2].

5. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le modalità procedurali necessarie per facilitare la cooperazione tra le autorità di vigilanza di cui al paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

21 bis) è inserito il seguente 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 genere, sia diretti che indiretti, per la prestazione del servizio fiduciario non qualificato. Fatte salve le disposizioni di cui all'articolo 18 della direttiva (UE) XXXX/XXX [NIS2], tali misure comprendono almeno:

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

ii) misure relative ai controlli procedurali o amministrativi;

iii) misure relative alla gestione e all'attuazione dei servizi;

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

2. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, specifica le caratteristiche tecniche delle misure di cui al paragrafo 1, lettera a). Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

22) l'articolo 20 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

"1. I prestatori di servizi fiduciari qualificati sono sottoposti, a proprie spese 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 18 della direttiva (UE) XXXX/XXXX [NIS2]. I prestatori di servizi fiduciari qualificati presentano la pertinente relazione di valutazione della conformità all'organismo di vigilanza entro tre giorni lavorativi dalla sua ricezione.";

a bis) è inserito il paragrafo seguente:

"1 bis. Gli Stati membri possono prevedere che i prestatori di servizi fiduciari qualificati informino in anticipo l'organismo di vigilanza in merito alle verifiche programmate e consentano, su richiesta, la partecipazione dell'organismo di vigilanza in qualità di osservatore.";

b) al paragrafo 2, l'ultima frase è sostituita dalla seguente:

"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) 2016/67.";

c) i paragrafi 3 e 4 sono sostituiti dai seguenti:

"3. Qualora il prestatore di servizi fiduciari qualificato non adempia 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, ove applicabile entro il termine fissato dall'organismo di vigilanza, quest'ultimo, tenendo conto in particolare della portata, della durata e delle conseguenze di tale inadempienza, può revocare la qualifica di tale prestatore o del servizio interessato da esso prestato.

3 bis. Qualora l'organismo di vigilanza sia informato dalle autorità nazionali competenti a norma della direttiva (UE) XXXX/XXXX [NIS2] del fatto che il fornitore di servizi fiduciari qualificati non adempie nessuno dei requisiti di cui all'articolo 18 della direttiva (UE) XXXX/XXXX [NIS2], l'organismo di vigilanza, tenendo in considerazione in particolare la portata, la durata e le conseguenze di tale inadempienza, può revocare la qualifica di tale prestatore o del servizio interessato da esso prestato.

3 ter. Qualora l'organismo di vigilanza sia informato dalle autorità di vigilanza di cui al regolamento (UE) 2016/679 del fatto che il fornitore di servizi fiduciari qualificati non adempie nessuno dei requisiti di cui al regolamento (UE) 2016/679, l'organismo di vigilanza, tenendo in considerazione in particolare la portata, la durata e le conseguenze di tale inadempienza, può revocare 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 di cui all'articolo 22, paragrafo 3, ai fini dell'aggiornamento degli elenchi di fiducia di cui all'articolo 22, paragrafo 1, e l'autorità nazionale competente di cui alla direttiva XXXX [NIS2].

4. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche e i numeri di riferimento delle norme 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 in materia di audit in base alle quali gli organismi di valutazione della conformità effettueranno le loro valutazioni della conformità 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.";

23) l'articolo 21 è così modificato:

"1. Qualora i prestatori di servizi fiduciari intendano avviare la prestazione di un servizio fiduciario qualificato, trasmettono all'organismo di vigilanza una notifica della 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 18 della direttiva (UE) XXXX/XXXX [NIS2].";

a) il paragrafo 2 è sostituito dal seguente:

"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.

Al fine di verificare il rispetto dei requisiti di cui all'articolo 18 della direttiva XXXX [NIS2] da parte del prestatore di servizi fiduciari, l'organismo di vigilanza chiede alle autorità competenti di cui a detta direttiva di svolgere azioni di vigilanza in tal senso e di fornire informazioni sui risultati senza indebito ritardo ed entro due mesi dal ricevimento della richiesta da parte delle autorità competenti di cui alla direttiva XXXX [NIS2]. Se la verifica non si è conclusa entro due mesi dalla notifica, le autorità competenti di cui alla direttiva XXXX [NIS2] 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.

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) il paragrafo 4 è sostituito dal seguente:

"4. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, definisce i formati e le procedure relativi alla notifica e alla verifica ai fini dei paragrafi 1 e 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

25) l'articolo 24 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

"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 sarà rilasciato il certificato qualificato o l'attestato elettronico di attributi qualificato.

Le informazioni di cui al primo comma sono verificate dal prestatore di servizi fiduciari qualificato, direttamente o ricorrendo a un terzo, in uno qualsiasi dei modi seguenti:

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

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 secondo procedure adeguate e conformemente alla legislazione nazionale.";

b) è aggiunto il seguente paragrafo 1 bis:

"1 bis. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce specifiche tecniche minime, norme e procedure relative alla verifica dell'identità e degli attributi conformemente al paragrafo 1, lettera c). Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

c) il paragrafo 2 è così modificato:

0) la lettera a) è così modificata:

"a) informa l'organismo di vigilanza almeno un mese prima dell'attuazione di qualsiasi modifica nella prestazione dei suoi servizi fiduciari qualificati o almeno tre mesi qualora intenda cessare tali attività. L'organismo di vigilanza può chiedere informazioni supplementari o il risultato di una valutazione della conformità prima di concedere l'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.";

1) le lettere d) ed e) sono sostituite dalle seguenti:

"d) prima di avviare una relazione contrattuale informa chiunque intenda utilizzare un servizio fiduciario qualificato, in modo chiaro, completo e facilmente accessibile, in uno spazio accessibile al pubblico e individualmente, 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 utilizzando nei sistemi, nei prodotti e nei processi che assicurano algoritmi crittografici, lunghezze di chiave e funzioni hash adeguati;"

2) sono inserite le nuove lettere f bis) e f ter):

"f bis) dispone di politiche adeguate e adotta misure corrispondenti per la gestione dei rischi giuridici, commerciali, operativi e di altro genere, sia diretti che indiretti, per la prestazione del servizio fiduciario qualificato. Fatte salve le disposizioni di cui all'articolo 18 della direttiva (UE) XXXX/XXX [NIS2], tali misure comprendono almeno:

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

ii) misure relative ai controlli procedurali o amministrativi;

iii) misure relative alla gestione e all'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 o perturbazioni connesse alla prestazione del servizio o all'attuazione delle misure di cui alla lettera f bis), punti i), ii) e iii), aventi un impatto significativo sui servizi fiduciari prestati o sui dati personali ivi custoditi.";

3) le lettere g) e h) sono sostituite dalle seguenti:

"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 giudiziali e per assicurare la continuità del servizio. Tali registrazioni possono essere elettroniche;";

4) la lettera j) è soppressa;

d) è aggiunto il seguente paragrafo 4 bis:

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

e) il paragrafo 5 è sostituito dal seguente:

"5. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche, le procedure e i numeri di riferimento delle norme applicabili ai requisiti di cui al paragrafo 2. Si presume che i requisiti di cui al presente articolo siano stati rispettati, ove siano rispettate tali specifiche tecniche, procedure e norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

f) è inserito il seguente paragrafo 6:

"6. Alla Commissione è conferito il potere di adottare atti di esecuzione che specifichino le caratteristiche tecniche delle misure di cui al paragrafo 2, lettera f bis).";

25 bis) l'articolo 26 è così modificato:

"2. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche e i numeri di riferimento delle norme applicabili alle firme elettroniche avanzate. Si presume che i requisiti delle firme elettroniche avanzate siano stati rispettati ove una firma elettronica avanzata adempia dette specifiche e norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

25 ter) l'articolo 27 è così modificato:

il paragrafo 4 è soppresso;

26) all'articolo 28, il paragrafo 6 è sostituito dal seguente:

"6. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche e i numeri di riferimento delle norme 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 adempia tali specifiche e norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

27) all'articolo 29 è aggiunto il seguente paragrafo 1 bis:

"1 bis. La generazione e la gestione dei dati per la creazione di una firma elettronica per conto del firmatario o la duplicazione dei dati per la creazione di tale firma a fini di back-up possono essere effettuate solo 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.";

28) è inserito il seguente articolo 29 bis:

"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 può essere 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), può duplicare i dati per la creazione di una firma elettronica solo a fini di back-up, a condizione che siano soddisfatti i seguenti requisiti:

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 eccede il minimo necessario per garantire la continuità del servizio;

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

2. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche e i numeri di riferimento delle norme applicabili ai fini del paragrafo 1.";

29) all'articolo 30 è inserito il seguente paragrafo 3 bis:

"3 bis. La validità di una certificazione di cui al paragrafo 1 non supera i cinque anni, subordinatamente a una valutazione delle vulnerabilità periodica effettuata ogni due anni. Qualora siano individuate vulnerabilità a cui non è posto rimedio, la certificazione è annullata.";

30) all'articolo 31, il paragrafo 3 è sostituito dal seguente:

"3. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, definisce i formati e le procedure applicabili ai fini del paragrafo 1. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

31) l'articolo 32 è così modificato:

a) al paragrafo 1 è aggiunto il seguente comma:

"Si presume che i requisiti di cui al primo comma siano stati rispettati ove la convalida delle firme elettroniche qualificate adempia le specifiche e le norme di cui al paragrafo 3.";

b) il paragrafo 3 è sostituito dal seguente:

"3. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche e i numeri di riferimento delle norme 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.";

31 bis) è inserito il seguente 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 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) l'integrità dei dati firmati non sia stata compromessa;

g) i requisiti di cui all'articolo 26 fossero soddisfatti al momento della firma. Si presume che i requisiti di cui al primo comma siano stati rispettati ove la convalida delle firme elettroniche avanzate basate su certificati qualificati adempia le specifiche e le norme di cui al paragrafo 3.

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 questioni attinenti alla sicurezza.

3. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche e i numeri di riferimento delle norme applicabili alla convalida delle firme elettroniche avanzate basate su certificati qualificati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

31 ter) l'articolo 33 è così modificato:

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

"2. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche e i numeri di riferimento delle norme applicabili al servizio di convalida qualificato di cui al paragrafo 1. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il servizio di convalida di una firma elettronica qualificata risponda a dette specifiche e norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

32) l'articolo 34 è sostituito dal seguente:

"*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.

2. 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 adempiano le specifiche e le norme di cui al paragrafo 3.

3. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche e i numeri di riferimento delle norme 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.";

32 bis) all'articolo 36 è aggiunto un nuovo paragrafo 2:

"2. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche e i numeri di riferimento delle norme applicabili ai sigilli elettronici avanzati.

Si presume che i requisiti dei sigilli elettronici avanzati siano rispettati ove un sigillo elettronico avanzato adempia dette specifiche e norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

33) l'articolo 37 è così modificato:

il paragrafo 4 è soppresso;

34) l'articolo 38 è così modificato:

a) il paragrafo 1 è sostituito dal seguente:

"1. I certificati qualificati dei sigilli elettronici soddisfano i requisiti di cui all'allegato III. Si presume che i requisiti di cui all'allegato III siano stati rispettati ove un certificato qualificato di sigillo elettronico adempia le specifiche e le norme di cui al paragrafo 6.";

b) il paragrafo 6 è sostituito dal seguente:

"6. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche e i numeri di riferimento delle norme applicabili ai certificati qualificati dei sigilli elettronici. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

35) è inserito il seguente articolo 39 bis:

"*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.";

35 bis) è inserito il seguente articolo 40 bis:

"*Articolo 40 bis*

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

(1) L'articolo 32 bis si applica mutatis mutandis alla convalida dei sigilli elettronici avanzati basati su certificati qualificati.";

36) l'articolo 42 è così modificato:

a) è inserito il seguente paragrafo 1 bis:

"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 la fonte accurata di misurazione del tempo adempiano le specifiche e le norme di cui al paragrafo 2.";

b) il paragrafo 2 è sostituito dal seguente:

"2. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche e i numeri di riferimento delle norme applicabili sia al collegamento della data e dell'ora ai dati sia a fonti accurate di misurazione del tempo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

36 bis) all'articolo 43 è aggiunto un nuovo paragrafo 3:

"2 bis. Un servizio elettronico di recapito certificato qualificato in uno Stato membro è riconosciuto quale servizio elettronico di recapito certificato qualificato in tutti gli altri Stati membri.";

37) l'articolo 44 è così modificato:

a) è aggiunto il seguente paragrafo 1 bis:

"1 bis. Si presume che i requisiti di cui al paragrafo 1 siano stati rispettati ove il processo di invio e ricezione dei dati adempia le specifiche e le norme di cui al paragrafo 2.";

b) il paragrafo 2 è sostituito dal seguente:

"2. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche e i numeri di riferimento delle norme 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.";

c) sono inseriti i seguenti paragrafi 3 e 4:

"3. 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. Il rispetto è confermato da un organismo di valutazione della conformità.

4. La Commissione, mediante un atto di esecuzione, può stabilire le specifiche tecniche e i numeri di riferimento delle norme al fine di agevolare il trasferimento dei dati fra due o più prestatori di servizi fiduciari qualificati. Le specifiche tecniche e il contenuto delle norme sono efficaci sotto il profilo dei costi e proporzionati. Tale atto di esecuzione è adottato secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

38) l'articolo 45 è sostituito dal seguente:

"*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 dei requisiti di cui all'allegato IV è effettuata conformemente alle specifiche e alle norme di cui al paragrafo 4.

2. I certificati qualificati di autenticazione di siti web di cui al paragrafo 1 sono riconosciuti dai browser web. A tal fine i browser web garantiscono che i dati di identità forniti mediante uno qualsiasi dei metodi siano visualizzati in maniera tale da risultare facilmente consultabili. I browser web garantiscono il supporto dei certificati qualificati di autenticazione di siti web di cui al paragrafo 1 e l'interoperabilità con gli stessi, a eccezione delle imprese considerate microimprese e piccole imprese conformemente alla raccomandazione 2003/361/CE della Commissione nei loro primi cinque anni di attività come prestatori di servizi di navigazione in rete.

4. Entro 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche e i numeri di riferimento delle norme applicabili ai certificati qualificati di autenticazione di siti web di cui ai paragrafi 1 e 2. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

39) dopo l'articolo 45 sono inserite le seguenti sezioni 9, 10 e 11:

"SEZIONE 9

ATTESTATI ELETTRONICI DI ATTRIBUTI

Articolo 45 bis

Effetti giuridici degli attestati elettronici di attributi

1. A un attestato elettronico di attribuiti non sono 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 gli attestati elettronici di attributi qualificati.

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

4. Un attestato di attributi rilasciato da un organismo del settore pubblico responsabile di una fonte autentica 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 ter

Attestati elettronici di attributi nei servizi pubblici

Qualora il diritto nazionale richieda l'identificazione elettronica mediante un mezzo di identificazione elettronica e un'autenticazione 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, ai fini dell'identificazione elettronica, l'identificazione elettronica mediante un mezzo di identificazione elettronica e un'autenticazione, a meno che ciò non sia specificamente consentito dallo Stato membro. In tal caso sono accettati anche gli attestati elettronici di attributi qualificati provenienti da altri Stati membri.

Articolo 45 quater

Requisiti per gli attestati elettronici di attributi qualificati

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

1 bis. La valutazione del rispetto dei requisiti di cui all'allegato V è effettuata conformemente alle specifiche e alle norme di cui al paragrafo 4.

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

3. 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.

4. Entro 6 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante un atto di esecuzione relativo all'implementazione dei portafogli europei di identità digitale di cui all'articolo 6 bis, paragrafo 11, stabilisce le specifiche tecniche e i numeri di riferimento delle norme applicabili agli attestati elettronici di attributi qualificati.

Articolo 45 quinquies

Verifica degli attributi rispetto a fonti autentiche

1. Entro 24 mesi dall'entrata in vigore degli atti di esecuzione di cui all'articolo 6 bis, paragrafo 11, e all'articolo 6 quater, paragrafo 4, 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 fornitori qualificati di attestati elettronici di attributi di verificare questi attributi mediante mezzi elettronici, su richiesta dell'utente e conformemente al diritto nazionale o dell'Unione.

2. Entro 6 mesi dall'entrata in vigore del presente regolamento, tenendo conto delle pertinenti norme internazionali, la Commissione, mediante un atto di esecuzione relativo all'implementazione dei portafogli europei di identità digitale di cui all'articolo 6 bis, paragrafo 11, stabilisce le specifiche tecniche minime, le norme e le procedure per quanto riguarda il catalogo di attributi e i regimi per gli attestati di attributi e le procedure di verifica degli attestati elettronici di attributi qualificati.

Articolo 45 quinquies bis

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 seguenti requisiti:

a) i requisiti di cui all'allegato VII;

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, paragrafo 45 bis, identificato come l'emittente di cui all'allegato VII, lettera b), contiene 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 nazionale o dell'Unione 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 nazionale o dell'Unione di cui al punto i).

2. Lo Stato membro in cui sono stabiliti gli organismi del settore pubblico di cui all'articolo 3, punto 45 bis, provvede affinché gli organismi del settore pubblico che rilasciano attestati elettronici di attributi soddisfino il livello di affidabilità equivalente a quello dei prestatori di servizi fiduciari qualificati conformemente all'articolo 24.

2 bis. Gli Stati membri notificano alla Commissione gli organismi del settore pubblico di cui all'articolo 3, punto 45 bis. 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 rende pubblico, attraverso un canale sicuro, l'elenco degli organismi del settore pubblico di cui all'articolo 3, punto 45 bis, in forma firmata o sigillata elettronicamente e adatta al trattamento automatizzato.

3. 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. Dopo la revoca, la situazione di revoca dell'attestato elettronico non è ripristinata.

4. 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 adempie le norme di cui al paragrafo 5.

5. Entro 6 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante un atto di esecuzione relativo all'implementazione dei portafogli europei di identità digitale di cui all'articolo 6 bis, paragrafo 11, stabilisce le specifiche tecniche e i numeri di riferimento delle norme applicabili agli attestati elettronici di attributi rilasciati da un organismo del settore pubblico responsabile di una fonte autentica o per suo conto.

5 bis. Entro 6 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante un atto di esecuzione relativo all'implementazione dei portafogli europei di identità digitale di cui all'articolo 6 bis, paragrafo 11, definisce i formati, le procedure, le specifiche e le norme applicabili ai fini del paragrafo 2 bis.

6. Gli organismi del settore pubblico di cui all'articolo 3, punto 45 bis, che rilasciano un attestato elettronico di attributi forniscono un'interfaccia con i portafogli europei di identità digitale forniti conformemente all'articolo 6 bis.

Articolo 45 sexies

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

I fornitori di attestati elettronici di attributi qualificati forniscono un'interfaccia con i portafogli europei di identità digitale forniti conformemente all'articolo 6 bis.

Articolo 45 septies

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

1. I prestatori di servizi di attestazione elettronica di attributi qualificati e non qualificati 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.

4. I prestatori di servizi di attestazione elettronica di attributi qualificati attuano una separazione funzionale per prestare tali servizi.

SEZIONE 10

SERVIZI DI ARCHIVIAZIONE ELETTRONICA

Articolo 45 octies

Effetti giuridici di un servizio di archiviazione elettronica

1. Ai dati elettronici conservati mediante un servizio di archiviazione elettronica 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 sono conservati mediante un servizio di archiviazione elettronica qualificato.

2. I dati elettronici conservati mediante un servizio di archiviazione elettronica qualificato godono della presunzione della loro integrità e della loro origine per la durata del periodo di conservazione da parte del prestatore di servizi fiduciari qualificato.

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

Articolo 45 octies bis

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 estendere la durabilità e la leggibilità dei dati 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'origine;

c) assicurano che i dati elettronici siano conservati in modo tale da essere protetti dal rischio di perdita e alterazione, ad eccezione delle modifiche riguardanti il loro supporto o la loro forma elettronica;

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 consultati da un archivio elettronico qualificato godono della presunzione di integrità dei dati dall'inizio del periodo di conservazione fino al momento della consultazione. Tale relazione 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 12 mesi dall'entrata in vigore del presente regolamento la Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche e i numeri di riferimento delle norme 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 adempia dette specifiche e norme. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

SEZIONE 11

REGISTRI ELETTRONICI

Articolo 45 nonies

Effetti giuridici dei registri elettronici

1. A un registro elettronico non sono 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 registri elettronici qualificati.

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.

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

Articolo 45 decies

Requisiti per i registri elettronici qualificati

1. I registri elettronici qualificati soddisfano i requisiti seguenti:

   a) sono creati 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 adempia le specifiche e le norme di cui al paragrafo 3.

3. La Commissione, mediante atti di esecuzione, stabilisce le specifiche tecniche e i numeri di riferimento delle norme applicabili alla creazione e al funzionamento di un registro elettronico qualificato. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

40) è inserito il seguente articolo 48 bis:

"*Articolo 48 bis*

Obblighi di comunicazione

1. Gli Stati membri provvedono affinché siano raccolte statistiche relative al funzionamento dei portafogli europei di identità digitale, una volta che saranno 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) una relazione di sintesi che include dati riguardanti gli incidenti che impediscono l'uso dei portafogli europei di identità digitale.

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

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

41) l'articolo 49 è sostituito dal seguente:

"*Articolo 49*

Riesame

1. La Commissione riesamina l'applicazione del presente regolamento e presenta una relazione in proposito al Parlamento europeo e al Consiglio entro 36 mesi dalla sua entrata in vigore. La Commissione valuta in particolare l'ambito di applicazione degli articoli 6 e 6 quinquies ter e se sia opportuno modificare l'ambito di applicazione del presente regolamento o sue disposizioni specifiche, tenendo conto dell'esperienza acquisita nell'applicazione del regolamento stesso nonché della domanda dei clienti, dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi giuridici. Se necessario, la relazione è corredata di una proposta di modifica del presente regolamento.

2. La relazione di valutazione comprende una valutazione della disponibilità e dell'usabilità dei portafogli europei di identità digitale che rientrano nell'ambito di applicazione del presente regolamento ed esamina se sia necessario imporre a tutti i prestatori di servizi privati online che fanno affidamento su servizi di identificazione elettronica di terzi per l'autenticazione degli utenti di accettare l'utilizzo dei portafogli europei di identità digitale.

3. Ogni quattro anni dopo la presentazione della relazione di cui al paragrafo 1 la Commissione presenta inoltre al Parlamento europeo e al Consiglio una relazione sui progressi compiuti nel conseguimento degli obiettivi del presente regolamento.";

42) l'articolo 51 è sostituito dal seguente:

"*Articolo 51*

Disposizioni 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 a 36 mesi dall'entrata in vigore del presente regolamento.

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 a 24 mesi dall'entrata in vigore del presente regolamento.

2 bis. La gestione di dispositivi qualificati per la creazione di firme elettroniche 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 firme elettroniche e di sigilli elettronici a distanza conformemente agli articoli 29 bis e 39 bis continua a essere presa in considerazione senza la necessità di ottenere la qualifica per la fornitura di tali servizi di gestione fino a 24 mesi dall'entrata in vigore del presente regolamento.

2 ter. I prestatori di servizi fiduciari qualificati cui è stata assegnata la qualifica a norma del presente regolamento prima del [data di entrata in vigore del regolamento modificativo] che utilizzano metodi di verifica dell'identità per il rilascio di certificati qualificati in conformità dell'articolo 24, paragrafo 1, presentano all'organismo di vigilanza una relazione di valutazione della conformità che attesti il rispetto dell'articolo 24, paragrafo 1, quanto prima e comunque entro 30 mesi dall'entrata in vigore del regolamento modificativo. Fino alla presentazione di tale relazione di valutazione della conformità e al completamento della sua valutazione da parte dell'organismo di vigilanza, il prestatore di servizi fiduciari qualificato può continuare a fare affidamento sull'uso dei metodi di verifica dell'identità di cui all'articolo 24, paragrafo 1, del regolamento (UE) n. 910/2014.";

43) l'allegato I è modificato conformemente all'allegato I del presente regolamento;

44) l'allegato II è sostituito dal testo figurante nell'allegato II del presente regolamento;

45) l'allegato III è modificato conformemente all'allegato III del presente regolamento;

46) l'allegato IV è modificato conformemente all'allegato IV del presente regolamento;

47) è aggiunto un nuovo allegato V il cui testo figura nell'allegato V del presente regolamento;

48) è aggiunto un nuovo allegato VI al presente regolamento.

Articolo 52

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

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

Fatto a Bruxelles, il

Per il Parlamento europeo	Per il Consiglio
Il presidente	Il presidente

ALLEGATO I

Nell'allegato I, la lettera i) è sostituita dalla seguente:

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

ALLEGATO II

REQUISITI RELATIVI AI DISPOSITIVI QUALIFICATI PER LA CREAZIONE DI UNA FIRMA ELETTRONICA

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

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

   (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 per creare una firma elettronica possono essere attendibilmente protetti dal firmatario legittimo contro l'uso da parte di terzi.

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

ALLEGATO III

Nell'allegato III, la lettera i) è sostituita dalla seguente:

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

ALLEGATO IV

Nell'allegato IV, la lettera j) è sostituita dalla seguente:

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

ALLEGATO V

REQUISITI PER GLI ATTESTATI ELETTRONICI DI ATTRIBUTI QUALIFICATI

Gli attestati elettronici di attributi qualificati contengono:

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

(f) 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

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

– per una persona fisica: il nome della persona;

(g) 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;

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

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

(j) 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;

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

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

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

ALLEGATO VI

ELENCO MINIMO DI ATTRIBUTI

A norma dell'articolo 45 quinquies, gli Stati membri garantiscono l'adozione di misure volte a consentire ai fornitori 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 nazionale o dell'Unione 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. licenze e permessi pubblici;
10. dati societari e finanziari.

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 attribuiti 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 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.