UNIONE EUROPEA

IL PARLAMENTO EUROPEO **IL CONSIGLIO**

Bruxelles, 11 aprile 2024
(OR. en)

2021/0136(COD)
LEX 2318

PE-CONS 68/1/23
REV 1

TELECOM 351
COMPET 1163
MI 1028
DATAPROTECT 329
JAI 1550
CODEC 2237

REGOLAMENTO DEL PARLAMENTO EUROPEO E DEL CONSIGLIO CHE MODIFICA IL REGOLAMENTO (UE) N. 910/2014 PER QUANTO RIGUARDA L'ISTITUZIONE DEL QUADRO EUROPEO RELATIVO A UN'IDENTITÀ DIGITALE

REGOLAMENTO (UE) 2024/…
DEL PARLAMENTO EUROPEO E DEL CONSIGLIO

dell'11 aprile 2024

che modifica il regolamento (UE) n. 910/2014 per quanto riguarda l'istituzione del quadro europeo relativo a un'identità digitale

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[1],

visto il parere del Comitato delle regioni[2],

deliberando secondo la procedura legislativa ordinaria[3],

---

1 GU C 105 del 4.3.2022, pag. 81.
2 GU C 61 del 4.2.2022, pag. 42.
3 Posizione del Parlamento europeo del 29 febbraio 2024 (non ancora pubblicata nella Gazzetta ufficiale) e decisione del Consiglio del 26 marzo 2024.

considerando quanto segue:

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

(2) Nelle sue conclusioni dell'1-2 ottobre 2020, 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) Il programma strategico per il decennio digitale 2030, istituito dalla decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio[5], stabilisce le finalità e gli obiettivi digitali di un quadro dell'Unione che dovrebbero condurre entro il 2030 a un'ampia diffusione di un'identità digitale affidabile, volontaria e controllata dagli utenti che sia riconosciuta in tutta l'Unione e consenta a ciascun utente di controllare i propri dati nelle interazioni online.

---

4 Regolamento (UE) n. 910/2014 del Parlamento europeo e del Consiglio, del 23 luglio 2014, in materia di identificazione elettronica e servizi fiduciari per le transazioni elettroniche nel mercato interno e che abroga la direttiva 1999/93/CE (GU L 257 del 28.8.2014, pag. 73).

5 Decisione (UE) 2022/2481 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, che istituisce il programma strategico per il decennio digitale 2030 (GU L 323 del 19.12.2022, pag. 4).

(4) La "dichiarazione europea sui diritti e i principi digitali per il decennio digitale", proclamata dal Parlamento europeo, dal Consiglio e dalla Commissione[6] ("dichiarazione"), sottolinea il diritto di ogni persona di avere accesso a tecnologie, prodotti e servizi digitali che siano sicuri e protetti e tutelino la vita privata fin dalla progettazione. Ciò include la garanzia che a tutte le persone che vivono nell'Unione sia offerta un'identità digitale accessibile, sicura e affidabile che dia accesso a un'ampia gamma di servizi online e offline, protetti contro i rischi di cibersicurezza e la criminalità informatica, anche per quanto riguarda le violazioni dei dati e i furti o le manipolazioni dell'identità. La dichiarazione stabilisce inoltre che ogni persona ha diritto alla protezione dei propri dati personali. Tale diritto comprende il controllo su come i dati sono utilizzati e con chi sono condivisi.

(5) I cittadini e i residenti dell'Unione dovrebbero avere il diritto a un'identità digitale che sia sotto il loro controllo esclusivo e che consenta loro di esercitare i propri diritti nell'ambiente digitale e di partecipare all'economia digitale. Per conseguire tale obiettivo è opportuno istituire un quadro europeo relativo a un'identità digitale che consenta ai cittadini e ai residenti dell'Unione di accedere a servizi pubblici e privati online e offline in tutta l'Unione.

(6) Un quadro armonizzato relativo all'identità digitale contribuirebbe alla creazione di un'Unione più integrata dal punto di vista digitale, riducendo gli ostacoli digitali tra gli Stati membri e consentendo ai cittadini e ai residenti dell'Unione di godere dei vantaggi della digitalizzazione, aumentando nel contempo la trasparenza e la protezione dei loro diritti.

---

[6] GU C 23 del 23.1.2023, pag. 1.

(7) Un approccio maggiormente armonizzato all'identificazione elettronica dovrebbe ridurre i rischi e i costi dell'attuale frammentazione dovuta all'uso di soluzioni nazionali divergenti oppure, in alcuni Stati membri, all'assenza di tali soluzioni di identificazione elettronica. Un tale approccio dovrebbe rafforzare il mercato interno consentendo ai cittadini e ai residenti dell'Unione, quali definiti dalle legislazioni nazionali, e alle imprese di identificarsi e di fornire un'autenticazione della propria identità online e offline in modo sicuro, affidabile, di facile utilizzo, pratico, accessibile e armonizzato in tutta l'Unione. Il portafoglio europeo di identità digitale dovrebbe fornire alle persone fisiche e giuridiche di tutta l'Unione un mezzo di identificazione elettronica armonizzato che consenta l'autenticazione e la condivisione dei dati collegati alla loro identità. Tutti dovrebbero poter accedere a servizi pubblici e privati in modo sicuro, sulla base di un ecosistema migliorato per i servizi fiduciari e su prove dell'identità e attestati elettronici di attributi verificati, come qualifiche accademiche, compresi diplomi universitari o altri titoli di studio o qualifiche professionali. Il quadro europeo relativo a un'identità digitale è inteso consentire il passaggio dalla dipendenza esclusiva da soluzioni di identità digitale nazionali alla fornitura di attestati elettronici di attributi validi e legalmente riconosciuti in tutta l'Unione. I fornitori di attestati elettronici di attributi dovrebbero beneficiare di un insieme di norme chiaro e uniforme, mentre le amministrazioni pubbliche dovrebbero potersi avvalere di documenti elettronici in un formato prestabilito.

(8) Vari Stati membri hanno attuato e utilizzano mezzi di identificazione elettronica che sono accettati dai prestatori di servizi nell'Unione. Inoltre sono stati effettuati investimenti in soluzioni sia nazionali che transfrontaliere sulla base del regolamento (UE) n. 910/2014, compresa l'interoperabilità dei regimi di identificazione elettronica notificati ai sensi di tale regolamento. 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'infrastruttura dei regimi di identificazione elettronica notificati utilizzati a livello dell'Unione e nazionale.

(9) Il regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio[7] e, se del caso, la direttiva 2002/58/CE del Parlamento europeo e del Consiglio[8] si applicano a tutte le attività di trattamento dei dati personali ai sensi del regolamento (UE) n. 910/2014. Anche le soluzioni nell'ambito del quadro di interoperabilità di cui al presente regolamento sono conformi a tali norme. La normativa dell'Unione in materia di protezione dei dati stabilisce principi di protezione dei dati, quali la minimizzazione dei dati e il principio di limitazione delle finalità, e obblighi in materia, ad esempio la protezione dei dati fin dalla progettazione e per impostazione predefinita.

---

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).

8 Direttiva 2002/58/CE del Parlamento europeo e del Consiglio, del 12 luglio 2002, relativa al trattamento dei dati personali e alla tutela della vita privata nel settore delle comunicazioni elettroniche (direttiva relativa alla vita privata e alle comunicazioni elettroniche) (GU L 201 del 31.7.2002, pag. 37).

(10) Al fine di sostenere la competitività delle imprese dell'Unione, i prestatori di servizi sia online che offline dovrebbero potersi avvalere di soluzioni di identità digitale riconosciute in tutta l'Unione, indipendentemente dallo Stato membro in cui tali soluzioni sono fornite, traendo in tal modo vantaggio da un approccio armonizzato a livello dell'Unione in materia di fiducia, sicurezza e interoperabilità. Sia gli utenti che i prestatori di servizi dovrebbero poter beneficiare in tutta l'Unione dello stesso valore giuridico conferito agli attestati elettronici di attributi. Un quadro armonizzato in materia di identità digitale ha l'obiettivo di creare valore economico fornendo un accesso più agevole a beni e servizi e riducendo in modo significativo i costi operativi legati alle procedure di identificazione e autenticazione elettroniche, ad esempio durante l'onboarding (acquisizione) di nuovi clienti, riducendo il rischio di reati informatici, quali furto di identità, furto di dati e frodi online, così da favorire guadagni in termini di efficienza e promuovere la trasformazione digitale sicura delle microimprese e delle piccole e medie imprese (PMI) dell'Unione.

(11) I portafogli europei di identità digitale dovrebbero facilitare l'applicazione del principio "una tantum", in modo da ridurre gli oneri amministrativi e sostenere la mobilità transfrontaliera per i cittadini e i residenti dell'Unione e le imprese in tutta l'Unione e promuovere lo sviluppo di servizi interoperabili di e-government in tutta l'Unione.

(12) Il regolamento (UE) 2016/679, il regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio[9] e la direttiva 2002/58/CE si applicano 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 ottenuti nella prestazione di altri servizi con i dati personali trattati al fine della prestazione dei 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 dal fornitore del portafoglio europeo di identità digitale. Il presente regolamento non dovrebbe impedire ai fornitori 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 europei di identità digitale da qualsiasi altro dato detenuto dal fornitore. Fatto salvo il regolamento (UE) 2016/679, il presente regolamento specifica ulteriormente l'applicazione dei principi di limitazione delle finalità, minimizzazione dei dati e protezione dei dati fin dalla progettazione e per impostazione predefinita.

---

9 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).

(13) I portafogli europei di identità digitale dovrebbero disporre, tra le proprie funzioni, di un pannello di gestione comune incorporato nella progettazione, al fine di garantire un livello più elevato di trasparenza, di tutela della vita privata e di controllo sui dati personali da parte degli utenti. Tale funzione dovrebbe prevedere un'interfaccia semplice e di facile utilizzo con una panoramica di tutte le parti facenti affidamento sulla certificazione con cui l'utente condivide dati, inclusi gli attributi, e del tipo di dati condivisi con ciascuna parte facente affidamento sulla certificazione. Dovrebbe consentire agli utenti di tracciare tutte le transazioni eseguite tramite il portafoglio europeo di identità digitale con almeno i seguenti dati: l'ora e la data della transazione, l'identificazione della controparte, i dati personali richiesti e i dati condivisi. Tali informazioni dovrebbero essere memorizzate anche se la transazione non è stata conclusa. Non dovrebbe essere possibile contestare l'autenticità delle informazioni contenute nella cronologia delle transazioni. Tale funzione dovrebbe essere attiva per impostazione predefinita. Dovrebbe consentire agli utenti di chiedere facilmente che una parte facente affidamento sulla certificazione cancelli immediatamente dati personali ai sensi dell'articolo 17 del regolamento (UE) 2016/679 e di segnalare facilmente la parte facente affidamento sulla certificazione all’autorità nazionale di protezione dei dati competente, in caso di ricezione di una richiesta di dati personali asseritamente illecita o sospetta, direttamente tramite il portafoglio europeo di identità digitale.

(14) Gli Stati membri dovrebbero integrare nel portafoglio europeo di identità digitale diverse tecnologie che preservino la riservatezza, come ad esempio la dimostrazione a conoscenza zero. Tali metodi crittografici dovrebbero consentire a una parte facente affidamento sulla certificazione di convalidare la veridicità di una determinata dichiarazione sulla base dei dati di identificazione e dell'attestato di attributi della persona in questione, senza rivelare alcun dato su cui si basa tale dichiarazione, così da preservare la vita privata dell’utente.

(15) Il presente regolamento stabilisce le condizioni armonizzate per l'istituzione di un quadro per i portafogli europei di identità digitale che saranno forniti dagli Stati membri. Tutti i cittadini e i residenti dell'Unione quali definiti dal diritto nazionale dovrebbero poter richiedere, selezionare, combinare, conservare, cancellare, condividere e presentare in sicurezza i dati relativi alla loro identità e richiedere la cancellazione dei loro dati personali in modo pratico e intuitivo, con il controllo esclusivo dell'utente, consentendo al contempo la divulgazione selettiva dei dati personali. Il presente regolamento riflette i valori europei condivisi e rispetta i diritti fondamentali, le garanzie giuridiche e la responsabilità, proteggendo in tal modo le società democratiche, i cittadini e i residenti dell'Unione. Le tecnologie utilizzate per conseguire tali obiettivi dovrebbero essere sviluppate cercando di ottenere il massimo livello di sicurezza, riservatezza, praticità per gli utenti, accessibilità, ampia utilizzabilità e interoperabilità senza soluzione di continuità. Gli Stati membri dovrebbero garantire a tutti i loro cittadini e residenti la parità di accesso all'identificazione elettronica. Gli Stati membri non dovrebbero limitare, direttamente o indirettamente, l'accesso a servizi pubblici o privati da parte di persone fisiche o giuridiche che scelgono di non utilizzare i portafogli europei di identità digitale e dovrebbero mettere a disposizione soluzioni alternative adeguate.

(16) Gli Stati membri dovrebbero avvalersi delle possibilità offerte dal presente regolamento per fornire, sotto la propria responsabilità, portafogli europei di identità digitale destinati a essere utilizzati dalle persone fisiche e giuridiche che risiedono o sono stabilite nel loro territorio. Al fine di offrire flessibilità agli Stati membri e sfruttare lo stato dell''arte tecnologico, il presente regolamento dovrebbe consentire la fornitura di portafogli europei di identità digitale direttamente da parte di uno Stato membro, sotto il mandato di uno Stato membro o indipendentemente da uno Stato membro, ma riconosciuti da tale Stato membro.

(17) Ai fini della registrazione, le parti facenti affidamento sulla certificazione dovrebbero fornire le informazioni necessarie a consentire la loro identificazione e autenticazione elettroniche nei portafogli europei di identità digitale. Nel dichiarare l'uso previsto del portafoglio europeo di identità digitale, le parti facenti affidamento sulla certificazione dovrebbero fornire informazioni in merito ai dati che richiederanno, se del caso, ai fini della prestazione dei loro servizi come anche il motivo della richiesta. La registrazione delle parti facenti affidamento sulla certificazione agevola la verifica da parte degli Stati membri per quanto concerne la legittimità delle attività di tali parti, in conformità del diritto dell'Unione. L'obbligo di registrazione di cui al presente regolamento dovrebbe lasciare impregiudicati gli obblighi stabiliti da altre normative dell'Unione o nazionali, ad esempio per quanto riguarda le informazioni da fornire agli interessati ai sensi del regolamento (UE) 2016/679. Le parti facenti affidamento sulla certificazione dovrebbero rispettare le garanzie offerte dagli articoli 35 e 36 di tale regolamento, in particolare effettuando valutazioni d'impatto sulla protezione dei dati e consultando le autorità competenti in materia di protezione dei dati prima del trattamento dei dati, laddove le valutazioni d'impatto sulla protezione dei dati indichino che il trattamento comporterebbe un rischio elevato. Tali garanzie dovrebbero sostenere il trattamento lecito dei dati personali da parte delle parti facenti affidamento sulla certificazione, in particolare per quanto riguarda categorie particolari di dati, quali i dati sanitari. La registrazione delle parti facenti affidamento sulla certificazione è intesa accrescere la trasparenza e la fiducia nell'uso dei portafogli europei di identità digitale. La registrazione dovrebbe essere efficace sotto il profilo dei costi e proporzionata ai relativi rischi per garantire l'uso da parte dei prestatori di servizi. In tale contesto, la registrazione dovrebbe prevedere l'uso di procedure automatizzate, compresi il ricorso e l'uso di registri esistenti da parte degli Stati membri, e non dovrebbe comportare una procedura di autorizzazione preventiva. La procedura di registrazione dovrebbe consentire una serie di casi d'uso che possono variare in termini di modalità di funzionamento, in modalità online o offline, o in termini di obbligo di autenticazione dei dispositivi al fine di interfacciarsi con il portafoglio europeo di identità digitale. La registrazione dovrebbe applicarsi esclusivamente alle parti facenti affidamento sulla certificazione che prestano servizi mediante interazione digitale.

(18) Proteggere i cittadini e i residenti dell'Unione dall'uso non autorizzato o fraudolento dei portafogli europei di identità digitale è di grande importanza al fine di garantire la fiducia negli stessi e la loro ampia diffusione. Agli utenti dovrebbe essere garantita una protezione efficace contro tale uso improprio. In particolare, ove nel contesto di un'altra procedura un'autorità giudiziaria nazionale accerti la sussistenza di fatti alla base di un uso fraudolento o in altro modo illecito di un portafoglio europeo di identità digitale, gli organismi di vigilanza responsabili per gli emittenti di portafogli europei di identità digitale dovrebbero, previa notifica, adottare le misure necessarie per garantire che la registrazione della parte facente affidamento sulla certificazione e l'inclusione delle parti facenti affidamento sulla certificazione nel meccanismo di autenticazione siano ritirate o sospese fino a quando l'autorità che ha effettuato la notifica confermi che è stato posto rimedio alle irregolarità rilevate.

(19) Tutti i portafogli europei di identità digitale dovrebbero consentire agli utenti di identificarsi e autenticarsi elettronicamente in modalità 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 europei di identità digitale possono anche rispondere alle esigenze istituzionali delle amministrazioni pubbliche, delle organizzazioni internazionali e delle istituzioni, degli organi e degli organismi dell'Unione. L'autenticazione in modalità 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 per quanto riguarda i regimi di identificazione elettronica, 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 ai sensi del 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'Unione. Una volta effettuato l'onboarding in un portafoglio europeo di identità digitale, le persone fisiche dovrebbero poterlo utilizzare per firmare con firme elettroniche qualificate, per impostazione predefinita e gratuitamente, senza dover sottostare a ulteriori procedure amministrative. Gli utenti dovrebbero poter apporre firme o sigilli su attributi o dichiarazioni autocertificati. Al fine di conseguire vantaggi in termini di semplificazione e riduzione dei costi per le persone e le imprese in tutta l'Unione, anche mediante la concessione di poteri di rappresentanza e mandati elettronici, gli Stati membri dovrebbero fornire portafogli europei di identità digitale che si basano su norme comuni e specifiche tecniche per garantire un'interoperabilità senza soluzione di continuità e aumentare adeguatamente la sicurezza informatica, rafforzare la solidità contro gli attacchi informatici e in tal modo ridurre significativamente i potenziali rischi che la digitalizzazione in atto pone a cittadini e a residenti dell'Unione e alle imprese.

Solo le autorità competenti degli Stati membri possono fornire un livello 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 la persona che dice di essere. È pertanto necessario che la fornitura di portafogli europei di identità digitale si basi sull'identità giuridica dei cittadini dell'Unione, dei residenti dell'Unione o delle persone giuridiche. Il ricorso all'identità giuridica non dovrebbe ostacolare l'accesso ai servizi da parte degli utenti dei portafogli europei di identità digitale sotto pseudonimo, laddove non sussista alcun requisito giuridico relativo all'utilizzo dell'identità giuridica ai fini dell'autenticazione. La fiducia nei portafogli europei di identità digitale aumenterebbe se i soggetti emittenti e gestori fossero tenuti ad attuare misure tecniche e organizzative adeguate per garantire il massimo livello di sicurezza commisurato ai rischi per i diritti e le libertà delle persone fisiche, conformemente al regolamento (UE) 2016/679.

(20) L'uso di una firma elettronica qualificata dovrebbe essere gratuito per tutte le persone fisiche a fini non professionali. Gli Stati membri dovrebbero poter prevedere misure che impediscano l'uso gratuito di firme elettroniche qualificate da parte di persone fisiche a fini professionali, garantendo al contempo che tali misure siano proporzionate ai rischi individuati e siano giustificate.

(21) 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 dovrebbero poter prevedere misure giuridiche e organizzative al fine di aumentare la flessibilità per i fornitori dei portafogli europei di identità digitale e consentire funzionalità aggiuntive dei portafogli europei di identità digitale rispetto a quelle previste dal presente regolamento, anche attraverso una maggiore interoperabilità con i mezzi nazionali di identificazione elettronica esistenti. Tali funzionalità aggiuntive non dovrebbero 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.

(22) I portafogli europei di identità digitale dovrebbero includere una funzionalità per generare pseudonimi scelti e gestiti dall'utente ai fini dell'autenticazione in caso di accesso a servizi online.

(23) Al fine di conseguire un livello elevato di sicurezza e fiducia, il presente regolamento stabilisce i requisiti per i 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.

(24) Al fine di evitare approcci divergenti e armonizzare l'attuazione dei requisiti stabiliti dal presente regolamento, è opportuno che la Commissione, ai fini della certificazione dei portafogli europei di identità digitale, adotti atti di esecuzione per stabilire un elenco di norme di riferimento e stabilire, se necessario, specifiche e procedure allo scopo di definire specifiche tecniche dettagliate relative a tali requisiti. Nella misura in cui la certificazione della conformità dei portafogli europei di identità digitale con i pertinenti requisiti di cibersicurezza non sia contemplata dai sistemi di certificazione della cibersicurezza esistenti cui si fa riferimento nel presente regolamento, e per quanto riguarda i requisiti non relativi alla cibersicurezza pertinenti per i portafogli europei di identità digitale, gli Stati membri dovrebbero istituire sistemi nazionali di certificazione conformemente ai requisiti armonizzati definiti nel presente regolamento e adottati a norma dello stesso. Gli Stati membri dovrebbero trasmettere i loro progetti di sistemi di certificazione nazionali al gruppo europeo di cooperazione sull'identità digitale, che dovrebbe essere in grado di formulare pareri e raccomandazioni.

(25) La certificazione della conformità con i requisiti di cibersicurezza definiti al presente regolamento dovrebbe basarsi sui pertinenti sistemi europei di certificazione della cibersicurezza, se disponibili, istituiti a norma del regolamento (UE) 2019/881 del Parlamento europeo e del Consiglio[10], che istituisce un quadro europeo di certificazione della cibersicurezza volontario per i prodotti, i processi e i servizi TIC.

---

10 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).

(26) Al fine di valutare e attenuare costantemente i rischi connessi alla sicurezza, i portafogli europei di identità digitale certificati dovrebbero essere oggetto di valutazioni periodiche delle vulnerabilità volte a rilevare eventuali vulnerabilità nei componenti certificati connessi ai prodotti, nei componenti certificati connessi ai processi e nei componenti certificati connessi ai servizi del portafoglio europeo di identità digitale.

(27) Proteggendo gli utenti e le imprese dai rischi di cibersicurezza, i requisiti essenziali di cibersicurezza stabiliti nel presente regolamento contribuiscono inoltre a migliorare la protezione dei dati personali e della vita privata delle persone. Dovrebbero essere considerate le sinergie sia nell'ambito della normazione che della certificazione relativamente agli aspetti di cibersicurezza attraverso la cooperazione tra la Commissione, le organizzazioni europee di normazione, l'Agenzia dell'Unione europea per la cibersicurezza (ENISA), il comitato europeo per la protezione dei dati istituito dal regolamento (UE) 2016/679 e le autorità nazionali di controllo della protezione dei dati.

(28) L'onboarding nel portafoglio europeo di identità digitale dei cittadini e dei residenti dell'Unione 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 laddove le specifiche e procedure tecniche armonizzate che utilizzano mezzi di identificazione elettronica rilasciati a un livello di garanzia significativo in combinazione con mezzi complementari di verifica dell'identità consentano di soddisfare i requisiti di cui al presente regolamento per quanto riguarda il livello di garanzia elevato. Tali mezzi complementari dovrebbero essere affidabili e di facile utilizzo e potrebbero basarsi sulla possibilità di utilizzare procedure di onboarding a distanza, certificati qualificati supportati da firme elettroniche qualificate, attestati elettronici qualificati di attributi 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 e procedure tecniche armonizzate per l'onboarding degli utenti utilizzando mezzi di identificazione elettronica, compresi quelli rilasciati a un livello di garanzia significativo.

(29) 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 dovrebbero potersi basare su elementi sicuri esterni certificati per la protezione del materiale crittografico e di altri dati sensibili o su mezzi di identificazione elettronica notificate a un livello di garanzia elevato al fine di dimostrare la conformità ai pertinenti requisiti del presente regolamento per quanto riguarda il livello di garanzia del portafoglio europeo di identità digitale. Il presente regolamento dovrebbe lasciare impregiudicate le condizioni nazionali per quanto riguarda il rilascio e l'uso di un elemento sicuro esterno certificato, qualora la misura transitoria ne dipenda.

(30) I portafogli europei di identità digitale dovrebbero garantire il massimo livello di protezione e sicurezza dei dati ai fini dell'identificazione e autenticazione elettroniche per agevolare l'accesso a servizi pubblici e privati, indipendentemente dal fatto che tali dati siano conservati localmente o attraverso soluzioni basate sul cloud, tenendo debitamente conto dei diversi livelli di rischio.

(31) I portafogli europei di identità digitale dovrebbero essere sicuri fin dalla progettazione e dovrebbero attuare caratteristiche di sicurezza avanzate per proteggere dal furto di identità e di altri dati, dal diniego di servizio (*denial of service*) e da qualsiasi altra minaccia informatica. Tale sicurezza dovrebbe includere metodi di cifratura e archiviazione all'avanguardia che siano accessibili solo all'utente, e decifrabili solo da quest'ultimo, e che si basino sulla comunicazione cifrata end-to-end con altri portafogli europei di identità digitale e parti facenti affidamento sulla certificazione. I portafogli europei di identità digitale dovrebbero inoltre richiedere la conferma sicura, esplicita e attiva dell'utente per le operazioni effettuate tramite i portafogli europei di identità digitale.

(32) L'utilizzo gratuito dei portafogli europei di identità digitale non dovrebbe comportare il trattamento di dati al di là di quanto necessario per la fornitura dei servizi dei portafogli europei di identità digitale. Il presente regolamento non dovrebbe consentire il trattamento, da parte del fornitore del portafoglio europeo di identità digitale, dei dati personali conservati nel portafoglio europeo di identità digitale o risultanti dall'uso dello stesso, se non ai fini della fornitura dei servizi dei portafogli europei di identità digitale. Per garantire la tutela della vita privata, i fornitori di portafogli europei di identità digitale dovrebbero garantire la non osservabilità, evitando di raccogliere dati e non avendo conoscenza delle transazioni degli utenti del portafoglio europeo di identità digitale. Tale non osservabilità comporta che i fornitori non possano vedere i dettagli delle transazioni effettuate dall'utente. In casi specifici tuttavia, sulla base del previo consenso esplicito dell'utente per ciascuno di tali casi specifici e nel pieno rispetto del regolamento (UE) 2016/679, ai fornitori di portafogli europei di identità digitale potrebbe essere concesso l'accesso alle informazioni necessarie per la fornitura di un particolare servizio connesso ai portafogli europei di identità digitale.

(33) La trasparenza dei portafogli europei di identità digitale e l'obbligo di rendiconto dei loro fornitori sono elementi chiave per creare fiducia sociale e promuovere l'accettazione del quadro. Il funzionamento dei portafogli europei di identità digitale dovrebbe pertanto essere trasparente e, in particolare, consentire un trattamento verificabile dei dati personali. A tal fine, gli Stati membri dovrebbero divulgare il codice sorgente dei componenti software dell'applicazione utente dei portafogli europei di identità digitale, compresi quelli connessi al trattamento dei dati personali e dei dati delle persone giuridiche. La pubblicazione di tale codice sorgente nell'ambito di una licenza open source dovrebbe consentire alla società, utenti e sviluppatori compresi, di comprenderne il funzionamento e di sottoporre il codice ad audit e a esame. Ciò aumenterebbe la fiducia degli utenti nell'ecosistema e contribuirebbe alla sicurezza dei portafogli europei di identità digitale consentendo a chiunque di segnalare vulnerabilità ed errori nel codice. Nel complesso ciò incentiverebbe i fornitori a offrire e mantenere un prodotto altamente sicuro. In taluni casi tuttavia, gli Stati membri, per motivi debitamente giustificati, soprattutto per motivi di pubblica sicurezza, potrebbero limitare la divulgazione del codice sorgente per le librerie utilizzate, il canale di comunicazione o altri elementi non ospitati sul dispositivo dell'utente.

(34) L'utilizzo dei portafogli europei di identità digitale così come l'interruzione del loro utilizzo dovrebbero essere un diritto e una scelta esclusivi degli utenti. Gli Stati membri dovrebbero elaborare procedure semplici e sicure con cui gli utenti possano richiedere la revoca immediata della validità dei portafogli europei di identità digitale, anche in caso di perdita o furto. Dovrebbe essere istituito un meccanismo che, in caso di morte dell'utente o di cessazione dell'attività di una persona giuridica, consenta all'autorità preposta al regolamento della successione della persona fisica o dei beni della persona giuridica di richiedere la revoca immediata del portafoglio europeo di identità digitale.

(35) Al fine di promuovere la diffusione dei portafogli europei di identità digitale e un uso più ampio delle identità digitali, gli Stati membri dovrebbero non solo promuovere i benefici dei servizi pertinenti, ma anche, in cooperazione con il settore privato, i ricercatori e il mondo accademico, sviluppare programmi di formazione volti a rafforzare le competenze digitali dei loro cittadini e residenti, in particolare per i gruppi vulnerabili, quali le persone con disabilità e gli anziani. Gli Stati membri dovrebbero inoltre sensibilizzare in merito ai benefici e ai rischi dei portafogli europei di identità digitale mediante campagne di comunicazione.

(36) Al fine di garantire che il quadro europeo relativo a un'identità digitale sia aperto all'innovazione e agli sviluppi tecnologici e adatto alle esigenze future, gli Stati membri sono incoraggiati congiuntamente a istituire spazi di sperimentazione 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 plasmare i futuri aggiornamenti dei riferimenti tecnici e dei requisiti giuridici. Tale ambiente dovrebbe favorire l'inclusione delle PMI, delle start-up e dei singoli innovatori e ricercatori, nonché dei pertinenti portatori di interessi dell'industria. Tali iniziative dovrebbero contribuire e rafforzare il rispetto della normativa e la robustezza tecnica dei portafogli europei di identità digitale da fornire ai cittadini e ai residenti dell'Unione, impedendo in tal modo lo sviluppo di soluzioni che non sono conformi alla normativa dell'Unione in materia di protezione dei dati o sono aperte a vulnerabilità di sicurezza.

(37) Il regolamento (UE) 2019/1157 del Parlamento europeo e del Consiglio[11] 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.

(38) 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.

(39) 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 sono intesi promuovere la cooperazione tra gli Stati membri in materia di sicurezza e interoperabilità dei rispettivi regimi di identificazione elettronica notificati.

(40) 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 adottati a norma dello stesso. Il presente regolamento dovrebbe consentire agli Stati membri di utilizzare relazioni e valutazioni, realizzate da organismi di valutazione della conformità accreditati, come previsto nel contesto dei 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 al regolamento (UE) n. 910/2014 dei regimi, o di parti di essi.

---

11 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).

(41) I fornitori di servizi pubblici utilizzano i dati di identificazione personale messi a disposizione da mezzi di identificazione elettronica ai sensi del regolamento (UE) n. 910/2014 per stabilire una corrispondenza tra l'identità elettronica degli utenti di altri Stati membri e i dati di identificazione personale forniti a tali utenti nello Stato membro che stabilisce la corrispondenza dell'identità a livello transfrontaliero. In molti casi, tuttavia, malgrado l'uso dell'insieme minimo di dati fornito nell'ambito dei regimi di identificazione elettronica notificati, per garantire un'accurata corrispondenza dell'identità nel caso in cui gli Stati membri fungano da parti facenti affidamento sulla certificazione, sono necessarie ulteriori informazioni relative all'utente e procedure specifiche complementari di identificazione univoca da eseguire a livello nazionale. Per sostenere ulteriormente l'utilizzabilità dei mezzi di identificazione elettronica, fornire migliori servizi pubblici online e accrescere la certezza giuridica relativamente all'identità elettronica degli utenti, il regolamento (UE) n. 910/2014 dovrebbe imporre agli Stati membri l'adozione di specifiche misure online per garantire una corrispondenza univoca dell'identità quando gli utenti intendono accedere online a servizi pubblici transfrontalieri.

(42) Nello sviluppo dei portafogli europei di identità digitale è essenziale tenere conto delle esigenze degli utenti. Dovrebbero essere disponibili casi d'uso significativi e servizi online basati 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 alla progettazione, allo sviluppo e all'attuazione di servizi online che sia simile 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 conto del quadro di interoperabilità dell'Unione. Gli Stati membri dovrebbero svolgere un ruolo di primo piano nell'adozione di tali orientamenti.

(43) Conformemente alla direttiva (UE) 2019/882 del Parlamento europeo e del Consiglio[12], 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.

(44) Al fine di garantire l'efficace applicazione del presente regolamento, è opportuno stabilire un limite minimo per il livello massimo di sanzioni amministrative per i prestatori di servizi fiduciari sia qualificati che non qualificati. Gli Stati membri dovrebbero prevedere sanzioni effettive, proporzionate e dissuasive. Nel determinare le sanzioni è opportuno tenere debitamente conto delle dimensioni dei soggetti interessati, dei loro modelli di business e della gravità delle violazioni.

(45) 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 ritenere che i servizi fiduciari non qualificati offerti da tali prestatori siano qualificati.

(46) 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 dell'Unione o nazionale stabilisca obblighi quanto alla forma. Inoltre, non dovrebbe avere ripercussioni sugli obblighi di forma nazionali relativi ai registri pubblici, in particolare i registri commerciali e catastali.

---

12 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).

(47) La prestazione e l'uso di servizi fiduciari così come i benefici apportati in termini di praticità e certezza giuridica nel contesto di transazioni transfrontaliere, in particolare nel caso in cui si utilizzino servizi fiduciari qualificati, stanno acquisendo una sempre maggiore importanza per il commercio e la cooperazione internazionali. I partner internazionali dell'Unione stanno istituendo quadri fiduciari che si ispirano al regolamento (UE) n. 910/2014. Al fine di facilitare il riconoscimento di servizi fiduciari qualificati e dei relativi prestatori, la Commissione può adottare atti di esecuzione per 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. Un tale approccio dovrebbe integrare la possibilità di riconoscimento reciproco dei servizi fiduciari e dei relativi prestatori stabiliti nell'Unione e in paesi terzi conformemente all'articolo 218 del trattato sul funzionamento dell'Unione europea (TFUE). 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 ai sensi del regolamento (UE) n. 910/2014, è opportuno garantire il rispetto delle pertinenti disposizioni di cui alla direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio[13] e al regolamento (UE) 2016/679, nonché l'uso di elenchi di fiducia quali elementi essenziali per costruire la fiducia.

---

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

(48) Il presente regolamento dovrebbe promuovere la scelta tra i portafogli europei di identità digitale e la possibilità di passare da uno all'altro, qualora uno Stato membro abbia approvato più di una soluzione di portafoglio europeo di identità digitale nel proprio territorio. Al fine di evitare effetti di lock-in in tali situazioni, se tecnicamente possibile i fornitori di portafogli europei di identità digitale dovrebbero garantire l'effettiva portabilità dei dati su richiesta degli utenti dei portafogli europei di identità digitale e non dovrebbero essere autorizzati a utilizzare ostacoli contrattuali, economici o tecnici per impedire o scoraggiare l'effettivo passaggio tra diversi portafogli europei di identità digitale.

(49) Al fine di garantire il corretto funzionamento dei portafogli europei di identità digitale, i fornitori di portafogli europei di identità digitale necessitano di interoperabilità effettiva e di condizioni eque, ragionevoli e non discriminatorie affinché i portafogli europei di identità digitale possano accedere a specifici componenti hardware e software dei dispositivi mobili. Tali componenti dovrebbero includere in particolare antenne NFC (*near field communication*) ed elementi sicuri, tra cui carte universali a circuiti integrati, elementi sicuri integrati, schede micro SD e Bluetooth a bassa energia. L'accesso a tali componenti potrebbe avvenire sotto il controllo di operatori di reti mobili e costruttori di apparecchiature. Pertanto, i costruttori di apparecchiature originali di dispositivi mobili o i prestatori di servizi di comunicazione elettronica non dovrebbero rifiutare l'accesso a tali componenti, se necessario ai fini della prestazione dei servizi dei portafogli europei di identità digitale. Inoltre le imprese designate come gatekeeper per i servizi di piattaforma di base elencati dalla Commissione ai sensi del regolamento (UE) 2022/1925 del Parlamento europeo e del Consiglio[14] dovrebbero rimanere soggette alle specifiche disposizioni di tale regolamento, sulla base dell'articolo 6, paragrafo 7, dello stesso.

---

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

(50) 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 (UE) 2022/2555, 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 informativi e di rete che tali prestatori utilizzano nella prestazione dei loro servizi, nonché per notificare minacce informatiche e incidenti significativi 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. I requisiti in materia di gestione dei rischi di cibersicurezza e gli obblighi di segnalazione a norma della direttiva (UE) 2022/2555 dovrebbero essere considerati complementari ai requisiti imposti ai prestatori di servizi fiduciari a norma del presente regolamento. Ove opportuno, le autorità competenti designate a norma della direttiva (UE) 2022/2555 dovrebbero continuare ad applicare le prassi o gli orientamenti nazionali consolidati per quanto riguarda l'attuazione dei requisiti in materia di sicurezza e comunicazione e la vigilanza della conformità a tali requisiti a norma del regolamento (UE) n. 910/2014. Il presente regolamento fa salvo l'obbligo di notificare le violazioni dei dati personali a norma del regolamento (UE) 2016/679.

(51) È opportuno prestare la dovuta attenzione per garantire una cooperazione efficace tra gli organismi di vigilanza designati a norma dell'articolo 46 ter del regolamento (UE) n. 910/2014 e le autorità competenti designate o istituite a norma dell'articolo 8, paragrafo 1, della direttiva (UE) 2022/2555. Qualora gli organismi di vigilanza siano diversi dalle autorità competenti, tali soggetti 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 di questi ultimi, dei requisiti di cui al regolamento (UE) n. 910/2014 e alla direttiva (UE) 2022/2555. In particolare, gli organismi di vigilanza designati a norma del regolamento (UE) n. 910/2014 dovrebbero essere autorizzati a richiedere alle autorità competenti designate o istituite a norma della direttiva (UE) 2022/2555 di fornire le pertinenti informazioni necessarie per concedere la qualifica e svolgere azioni di vigilanza volte a verificare il rispetto, da parte dei prestatori di servizi fiduciari, dei pertinenti requisiti di cui alla direttiva (UE) 2022/2555 o a imporre loro di rimediare al mancato rispetto.

(52) 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 certificato in tutta l'Unione. 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 rendere i loro servizi interoperabili con i servizi elettronici di recapito certificato qualificati prestati da altri prestatori di servizi fiduciari qualificati, al fine di trasferire facilmente dati elettronici registrati tra due o più prestatori di servizi fiduciari qualificati e di promuovere pratiche leali nel mercato interno.

(53) Nella maggior parte dei casi i cittadini e i residenti dell'Unione non sono in grado di scambiare, a livello transfrontaliero, in modo sicuro e con un livello elevato di protezione dei dati, informazioni digitali relative alla loro identità quali indirizzi, età, qualifiche professionali, patente di guida e altri permessi e dati di pagamento.

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

(55) Qualsiasi fornitore di servizi che rilasci attributi in forma elettronica quali diplomi, licenze, certificati di nascita oppure poteri e mandati per rappresentare persone fisiche o giuridiche o agire a loro nome dovrebbe essere considerato un prestatore di servizi fiduciari che fornisce attestati elettronici di attributi. Agli attestati elettronici di attributi non dovrebbero essere negati gli effetti giuridici a motivo della loro forma elettronica o perché non soddisfano i requisiti degli attestati elettronici qualificati di attributi. È opportuno stabilire requisiti generali per garantire che gli effetti giuridici degli attestati elettronici qualificati di attributi 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 qualificati di attributi, ove opportuno.

(56) L'ampia disponibilità e utilizzabilità dei portafogli europei di identità digitale dovrebbe accrescere l'accettazione e la fiducia nei loro confronti da parte dei privati e dei prestatori di servizi privati. Le parti private facenti affidamento sulla certificazione che prestano servizi ad esempio nei settori dei trasporti, dell'energia, delle banche e dei servizi finanziari, della sicurezza sociale, della sanità, dell'acqua potabile, dei servizi postali, dell'infrastruttura digitale, delle telecomunicazioni o dell'istruzione dovrebbero pertanto accettare l'uso dei portafogli europei di identità digitale per la prestazione di servizi per i quali il diritto dell'Unione o nazionale o gli obblighi contrattuali impongono un'autenticazione forte dell'utente per l'identificazione online. Eventuali richieste dalle parti facenti affidamento sulla certificazione di informazioni provenienti dall'utente di un portafoglio europeo di identità digitale dovrebbero essere necessarie e proporzionate all'uso previsto in un determinato caso, essere in linea con il principio della minimizzazione dei dati e garantire la trasparenza per quanto riguarda quali dati sono condivisi e a quali scopi. Per agevolare l'uso e l'accettazione dei portafogli europei di identità digitale, è opportuno tenere conto delle norme e delle specifiche del settore ampiamente accettate nella loro introduzione.

(57) Qualora le piattaforme online di dimensioni molto grandi ai sensi dell'articolo 33, paragrafo 1, del regolamento (UE) 2022/2065 del Parlamento europeo e del Consiglio[15] impongano agli utenti di essere autenticati 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 un portafoglio europeo di identità digitale per accedere ai servizi privati e il loro accesso ai servizi non dovrebbe essere limitato o ostacolato per il fatto che non utilizzano un portafoglio europeo di identità digitale. Tuttavia, qualora gli utenti desiderino usarlo, le piattaforme online di dimensioni molto grandi dovrebbero accettarne l'uso a tale scopo, nel rispetto del principio della minimizzazione dei dati e del diritto degli utenti di utilizzare pseudonimi liberamente scelti. L'obbligo di accettare portafogli europei di identità digitale è 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.

(58) È opportuno elaborare codici di condotta a livello dell'Unione per contribuire all'ampia disponibilità e utilizzabilità 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 facilitare un'ampia 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.

---

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

(59) 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 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. Per l'utente dovrebbe essere tecnicamente possibile divulgare selettivamente gli attributi, anche quando in origine sono parti di una serie di attestati elettronici distinti, e combinarli e presentarli senza soluzione di continuità alle parti facenti affidamento sulla certificazione. Tale caratteristica dovrebbe diventare una caratteristica di progettazione di base dei portafogli europei di identità digitale, rafforzando in tal modo la praticità e la tutela dei dati personali, compresa la minimizzazione dei dati.

(60) A meno che norme specifiche del diritto dell'Unione o nazionale impongano agli utenti di identificarsi, non dovrebbe essere proibito accedere ai servizi utilizzando uno pseudonimo.

(61) Gli attributi forniti dai prestatori di servizi fiduciari qualificati nell'ambito degli attestati qualificati di attributi 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 dell'Unione o nazionale, ai fini dello scambio sicuro di attributi 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 qualificati di attributi 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 possibili meccanismi appropriati dovrebbe figurare 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 intende favorire il rispetto, da parte dei prestatori di servizi fiduciari qualificati che forniscono attestati elettronici qualificati di attributi, degli obblighi loro imposti dal regolamento (UE) n. 910/2014. Un nuovo allegato di tale regolamento dovrebbe contenere un elenco di categorie di attributi per i quali gli Stati membri devono assicurare che siano adottate misure per consentire ai fornitori qualificati di attestati elettronici qualificati di attributi di verificare mediante mezzi elettronici, su richiesta dell'utente, la loro autenticità rispetto alla fonte autentica pertinente.

(62) 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 dei clienti e lo scambio degli attributi specifici necessari per rispettare, ad esempio, le prescrizioni in materia di adeguata verifica della clientela ai sensi di un futuro regolamento che istituisce l'Autorità antiriciclaggio 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 dell'avvio di transazioni nel settore dei servizi di pagamento.

(63) Gli effetti giuridici di una firma elettronica non possono essere contestati in ragione della sua forma elettronica o del fatto che non soddisfa i requisiti della firma elettronica qualificata. Tuttavia, gli effetti giuridici delle firme elettroniche devono essere stabiliti dal diritto nazionale, salvo per i requisiti previsti dal presente regolamento a norma dei quali gli effetti giuridici di una firma elettronica qualificata devono essere considerati equivalenti a quelli di una firma autografa. Nel determinare gli effetti giuridici delle firme elettroniche gli Stati membri dovrebbero tenere conto del principio di proporzionalità tra il valore giuridico di un documento da firmare e il livello di sicurezza e di costo richiesto da una firma elettronica. Per aumentare l'accessibilità e l'uso delle firme elettroniche, gli Stati membri sono incoraggiati a valutare l'uso di firme elettroniche avanzate nelle transazioni quotidiane, per le quali essi forniscono un livello sufficiente di sicurezza e affidabilità.

(64) Per garantire la coerenza delle pratiche di certificazione in tutta l'Unione, 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 organismi pubblici o privati che dispongono di dispositivi qualificati per la creazione di una firma elettronica certificati di ricertificare temporaneamente tali dispositivi per un breve periodo di certificazione, sulla base dei risultati del processo di certificazione precedente, qualora tale ricertificazione non possa essere effettuata entro il termine stabilito per legge per un motivo diverso da una violazione della sicurezza o da un incidente di sicurezza, fatto salvo l'obbligo di condurre una valutazione delle vulnerabilità e fatta salva la pratica di certificazione applicabile.

(65) Il rilascio di certificati per l'autenticazione dei siti web è intesa ad offrire agli utenti una garanzia con un elevato livello di affidabilità riguardo all'identità delle entità dietro ai siti web, indipendentemente dalla piattaforma utilizzata per la visualizzazione di tale identità. Tali certificati dovrebbero contribuire a diffondere sicurezza e fiducia nelle transazioni commerciali online, in quanto gli utenti si fiderebbero di un sito web che è stato autenticato. L'uso di tali certificati da parte di siti web dovrebbe essere volontario. 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 stabilisce un quadro fiduciario comprendente obblighi minimi in materia di sicurezza e responsabilità per i fornitori di certificati qualificati di autenticazione dei siti web e requisiti per il rilascio di tali certificati. Gli elenchi nazionali di fiducia dovrebbero confermare la qualifica dei servizi di autenticazione di siti web e dei loro prestatori di servizi fiduciari, compresa la loro piena conformità ai requisiti del presente regolamento per quanto riguarda il rilascio di certificati qualificati di autenticazione di siti web. Il riconoscimento dei certificati qualificati di autenticazione di siti web comporta che i fornitori di browser web non dovrebbero negare l'autenticità dei certificati qualificati di autenticazione di siti web al solo scopo di attestare il collegamento tra il nome di dominio del sito web e la persona fisica o giuridica a cui è rilasciato il certificato o di confermare l'identità di tale persona. I fornitori di browser web dovrebbero far sì che l'utente finale visualizzi i dati di identità certificati e gli altri attributi in modo facilmente consultabile nell'ambiente del browser, tramite mezzi tecnici di loro scelta. A tal fine i fornitori di browser web dovrebbero garantire il supporto dei certificati qualificati di autenticazione di siti web emessi nel pieno rispetto del presente regolamento e l'interoperabilità con gli stessi.

L'obbligo di riconoscimento, interoperabilità e supporto dei certificati qualificati di autenticazione di siti web non pregiudica la libertà dei fornitori di browser web di garantire la sicurezza del web, l'autenticazione del dominio e la cifratura del traffico web con le modalità e tramite la tecnologia che ritengono più appropriate. Al fine di contribuire alla sicurezza online degli utenti finali, i fornitori di browser web dovrebbero, in circostanze eccezionali, poter adottare misure precauzionali tanto necessarie quanto proporzionate in risposta a preoccupazioni fondate riguardanti violazioni della sicurezza o la perdita di integrità di un certificato o di un insieme di certificati identificati. Qualora adottino tali misure precauzionali, i fornitori di browser web dovrebbero notificare senza indebito ritardo alla Commissione, all'organismo nazionale di vigilanza, al soggetto al quale è stato rilasciato il certificato e al prestatore di servizi fiduciari qualificato che ha rilasciato tale certificato o insieme di certificati, eventuali preoccupazioni in merito a tale violazione della sicurezza o perdita di integrità, nonché le misure adottate in relazione al singolo certificato o a un insieme di certificati. Tali misure non dovrebbero pregiudicare l'obbligo dei fornitori di browser web di riconoscere i certificati qualificati di autenticazione di siti web conformemente agli elenchi nazionali di fiducia. 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 e i residenti dell'Unione. Le misure previste dal presente regolamento volte ad accrescere la coerenza tra gli approcci e le prassi divergenti degli Stati membri in materia di procedure di vigilanza sono intese a contribuire a migliorare la fiducia nella sicurezza, nella qualità e nella disponibilità dei certificati qualificati di autenticazione di siti web.

(66) Molti Stati membri hanno introdotto requisiti nazionali per i servizi che forniscono un'archiviazione elettronica sicura e affidabile al fine di consentire la conservazione a lungo termine di dati elettronici e documenti elettronici, nonché per i servizi fiduciari associati. Al fine di garantire la certezza giuridica, 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. Il quadro giuridico per i servizi di archiviazione elettronica qualificati 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 dati elettronici e ai documenti elettronici creati in forma elettronica e ai documenti cartacei che sono stati scannerizzati e digitalizzati. Ove necessario, tali disposizioni dovrebbero consentire che i dati elettronici e i documenti elettronici conservati siano trasferiti su supporti o formati diversi al fine di estenderne la durabilità e la leggibilità oltre il periodo di validità tecnologica, evitando nel contempo, nella misura del possibile, le perdite e le alterazioni. Quando i dati elettronici e i documenti elettronici trasmessi al servizio di archiviazione elettronica 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 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 qualificati. In relazione ai servizi di archiviazione elettronica non armonizzati dal presente regolamento, gli Stati membri dovrebbero poter mantenere o introdurre disposizioni nazionali, in conformità del diritto dell'Unione, relative a tali servizi, quali disposizioni specifiche per i servizi integrati in un'organizzazione e utilizzati esclusivamente per gli archivi interni di tale organizzazione. Il presente regolamento non dovrebbe distinguere tra dati elettronici e i documenti elettronici creati in forma elettronica e documenti fisici che sono stati digitalizzati.

(67) Le attività degli archivi nazionali e delle istituzioni della memoria, in qualità di organizzazioni preposte alla conservazione del patrimonio documentario nell'interesse pubblico, sono generalmente disciplinate dal diritto nazionale e non forniscono necessariamente servizi fiduciari ai sensi del presente regolamento. Nella misura in cui tali istituzioni non forniscono tali servizi fiduciari, il presente regolamento non ne pregiudica il funzionamento.

(68) I registri elettronici sono una sequenza di registrazioni di dati elettronici che dovrebbero garantirne l'integrità e l'accuratezza dell'ordine cronologico. I registri elettronici dovrebbero stabilire una sequenza cronologica delle registrazioni di dati. Congiuntamente ad altre tecnologie, dovrebbero 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 e la registrazione delle proprietà immobiliari nei registri catastali decentrati. I registri elettronici qualificati dovrebbero stabilire una presunzione legale per l'ordine cronologico sequenziale univoco e accurato e l'integrità della registrazione dei dati nel registro. In ragione delle loro specificità, ad esempio l'ordine cronologico sequenziale delle registrazioni di dati, i registri elettronici dovrebbero essere distinti da altri servizi fiduciari quali le validazioni temporali elettroniche e i servizi elettronici di recapito certificato. Per garantire la certezza giuridica e promuovere l'innovazione, è opportuno istituire un quadro giuridico a livello dell'Unione che disponga il riconoscimento transfrontaliero dei servizi fiduciari per la registrazione dei dati nei registri elettronici. Ciò dovrebbe impedire in misura sufficiente che lo stesso bene digitale sia copiato e venduto più di una volta a diverse parti. Il processo di creazione e aggiornamento di un registro elettronico dipende dal tipo di registro utilizzato, ossia se è centralizzato o distribuito. Il presente regolamento dovrebbe garantire la neutralità tecnologica, vale a dire non favorire né discriminare alcuna tecnologia utilizzata per attuare il nuovo servizio fiduciario per i registri elettronici. Inoltre, nell'elaborazione degli atti di esecuzione che specificano i requisiti per i registri elettronici qualificati, la Commissione dovrebbe tenere conto degli indicatori di sostenibilità relativi a eventuali effetti negativi sul clima o altri effetti negativi connessi all'ambiente, utilizzando metodologie adeguate.

(69) Il ruolo dei prestatori di servizi fiduciari per i registri elettronici dovrebbe essere quello di verificare la registrazione sequenziale dei dati nel registro. Il presente regolamento lascia impregiudicati gli obblighi giuridici degli utenti dei registri elettronici ai sensi del diritto dell'Unione o nazionale. Ad esempio, i casi d'uso che comportano il trattamento di dati personali dovrebbero rispettare il regolamento (UE) 2016/679 e i casi d'uso relativi ai servizi finanziari dovrebbero essere conformi al pertinente diritto dell'Unione in materia di servizi finanziari.

(70) Al fine di evitare la frammentazione del mercato interno e gli ostacoli all'interno di quest'ultimo dovuti a norme divergenti e restrizioni tecniche e di garantire un processo coordinato per non compromettere l'attuazione del quadro europeo relativo a un'identità digitale, è necessario un processo per una cooperazione ravvicinata e strutturata tra la Commissione, gli Stati membri, la società civile, il mondo accademico e il settore privato. Per conseguire tale obiettivo gli Stati membri e la Commissione dovrebbero cooperare nell'ambito del quadro istituito dalla raccomandazione (UE) 2021/946 della Commissione[16] al fine di individuare un pacchetto di strumenti comune dell'Unione per un quadro europeo relativo a un'identità digitale. In tale contesto, gli Stati membri dovrebbero concordare un'architettura tecnica e un quadro di riferimento completi, un insieme comune di norme e di riferimenti tecnici, tra cui norme vigenti riconosciute, e una serie di orientamenti e descrizioni di migliori prassi che contemplino almeno tutte le funzionalità e l'interoperabilità dei portafogli europei di identità digitale, comprese le firme elettroniche, e dei prestatori di servizi fiduciari qualificati per gli attestati elettronici di attributi di cui al presente regolamento. In tale contesto, gli Stati membri dovrebbero anche concordare gli elementi comuni per quanto concerne un modello di business e una struttura tariffaria per i portafogli europei di identità digitale al fine di agevolarne l'adozione, in particolare da parte delle PMI, 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 europeo relativo a un'identità digitale e rispecchiare tali risultati.

---

16 Raccomandazione (UE) 2021/946 della Commissione, del 3 giugno 2021, relativa a un pacchetto di strumenti comuni dell'Unione per un approccio coordinato verso un quadro europeo relativo a un'identità digitale (GU L 210 del 14.6.2021, pag. 51).

(71) Il presente regolamento prevede 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 in un paese terzo, qualora quest'ultimo fornisca sufficienti garanzie, assicurando che le attività di vigilanza e le verifiche possano essere eseguite come se fossero effettuate nell'Unione. Ove la conformità al presente 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.

(72) Per garantire la certezza giuridica della validità delle firme elettroniche avanzate basate su certificati qualificati, è essenziale specificare la valutazione della parte facente affidamento sulla certificazione che effettua la convalida di tale firma elettronica avanzata basata su certificati qualificati.

(73) I prestatori di servizi fiduciari dovrebbero utilizzare metodi 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.

(74) Il presente regolamento stabilisce 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 o l'attestato elettronico di attributi qualificato sulla base di vari metodi armonizzati in tutta l'Unione. Per garantire che i certificati qualificati e gli attestati elettronici qualificati di attributi siano rilasciati alla persona cui appartengono e che attestino l'insieme corretto e unico di dati che rappresenta l'identità di tale persona, i prestatori di servizi fiduciari qualificati che rilasciano certificati qualificati o attestati elettronici qualificati di attributi dovrebbero, al momento del rilascio di tali certificati e attestati, garantire con assoluta certezza l'identificazione di tale persona. Inoltre, oltre alla verifica obbligatoria dell'identità della persona, se applicabile per il rilascio di certificati qualificati e al momento del rilascio di un attestato elettronico di attributi qualificato, i prestatori di servizi fiduciari qualificati dovrebbero garantire con assoluta certezza la correttezza e l'accuratezza degli attributi della persona cui è rilasciato il certificato qualificato o l'attestato elettronico di attributi qualificato. Tali obblighi di risultato e di assoluta certezza nella verifica dei dati attestati dovrebbero essere sostenuti con mezzi adeguati, anche utilizzando un metodo o, se necessario, una combinazione di metodi specifici previsti dal presente regolamento. Dovrebbe essere possibile combinare tali metodi per fornire una base adeguata ai fini della verifica dell'identità della persona cui è rilasciato il certificato qualificato o l'attestato elettronico di attributi qualificato. Tale combinazione dovrebbe poter includere il ricorso a mezzi di identificazione elettronica che soddisfano i requisiti del livello di garanzia significativo in combinazione con altri mezzi di verifica dell'identità che consentirebbero di soddisfare i requisiti armonizzati di cui al presente regolamento per quanto riguarda il livello di garanzia elevato nell'ambito di ulteriori procedure armonizzate a distanza, garantendo l'identificazione con un elevato livello di affidabilità. Tali metodi dovrebbero includere la possibilità per il prestatore di servizi fiduciari qualificato che rilascia un attestato elettronico di attributi qualificato di verificare gli elementi da attestare mediante mezzi elettronici, su richiesta dell'utente, conformemente al diritto dell'Unione o nazionale, anche rispetto alle fonti autentiche.

(75) Per mantenere il presente regolamento in linea con gli sviluppi globali e seguire le migliori 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.

(76) Poiché gli obiettivi del presente regolamento, vale a dire lo sviluppo del quadro europeo relativo a un'identità digitale e di un quadro per i servizi fiduciari a livello dell'Unione, non possono essere conseguiti in misura sufficiente dagli Stati membri ma, a motivo della loro portata e dei loro effetti, possono essere conseguiti meglio a livello di Unione, quest'ultima può intervenire in base al principio di sussidiarietà sancito dall'articolo 5 del trattato sull'Unione europea. Il presente regolamento si limita a quanto è necessario per conseguire tali obiettivi in ottemperanza al principio di proporzionalità enunciato nello stesso articolo.

(77) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725, il Garante europeo della protezione dei dati è stato consultato.

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

HANNO ADOTTATO IL PRESENTE REGOLAMENTO:

Articolo 1

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

1) l'articolo 1 è sostituito dal seguente:

"*Articolo 1*
Oggetto

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

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

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

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

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 notificati da uno Stato membro, ai portafogli europei di identità digitale forniti da uno Stato membro e ai prestatori di servizi fiduciari stabiliti nell'Unione.";

b) il paragrafo 3 è sostituito dal seguente:

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

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

---

* 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).";

3) l'articolo 3 è così modificato:

a) i punti da 1) a 5) sono sostituiti dai seguenti:

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

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

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

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

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

b) è inserito il punto seguente:

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

c) il punto 6 è sostituito dal seguente:

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

d) il punto 16 è sostituito dal seguente:

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

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

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

c) la creazione di firme elettroniche o sigilli elettronici;

d) la convalida di firme elettroniche o sigilli elettronici;

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

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

g) il rilascio di attestati elettronici di attributi;

h) la convalida di attestati elettronici di attributi;

i) la creazione di validazioni temporali elettroniche;

j) la convalida di validazioni temporali elettroniche;

k) la prestazione di servizi elettronici di recapito certificato;

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

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

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

e) il punto 18 è sostituito dal seguente:

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

f) il punto 21 è sostituito dal seguente:

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

g) sono inseriti i punti seguenti:

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

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

h) il punto 38 è sostituito dal seguente:

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

i) il punto 41 è sostituito dal seguente:

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

j) sono inseriti i punti seguenti:

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

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

44) "attestato elettronico di attributi ", un attestato in forma elettronica che consente l’autenticazione di attributi;

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

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

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

48) "archiviazione elettronica", un servizio che consente la ricezione, la conservazione, la consultazione e la cancellazione di dati elettronici e documenti elettronici al fine di garantirne la durabilità e leggibilità nonché di preservarne l'integrità, la riservatezza e la prova dell'origine per tutto il periodo di conservazione;

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

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

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

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

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

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

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

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

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

4) l'articolo 5 è sostituito dal seguente:

"*Articolo 5*
Pseudonimi nelle transazioni elettroniche

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

5) al capo II è inserita la sezione seguente:

"SEZIONE 1
PORTAFOGLIO EUROPEO DI IDENTITÀ DIGITALE

Articolo 5 bis
Portafogli europei di identità digitale

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

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

a) direttamente da uno Stato membro;

b) su incarico di uno Stato membro;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

a) sostengono protocolli e interfacce comuni:

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

   a) su esplicita richiesta dell'utente;

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

23. Entro … [6 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai requisiti di cui ai paragrafi 4, 5, 8 e 18 del presente articolo relativamente all'attuazione del portafoglio europeo di identità digitale. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

24. La Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure per facilitare l'onboarding degli utenti nel portafoglio europeo di identità digitale tramite mezzi di identificazione elettronica conformi al livello di garanzia elevato o mezzi di identificazione elettronica conformi al livello di garanzia significativo unitamente a ulteriori procedure di onboarding a distanza che, insieme, soddisfano i requisiti del livello di garanzia elevato. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 5 ter
Parti facenti affidamento sulla certificazione dei portafogli europei di identità digitale

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

11. Entro ... [6 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione relativi all'attuazione dei portafogli europei di identità digitale di cui all'articolo 6 bis, paragrafo 23, stabilisce specifiche e procedure tecniche per i requisiti di cui ai paragrafi 2, 5 e da 6a 9 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 5 quater
Certificazione dei portafogli europei di identità digitale

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

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

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

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

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

6. Entro ... [6 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili alla certificazione dei portafogli europei di identità digitale di cui ai paragrafi 1, 2 e 3 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

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

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

Articolo 5 quinquies
Pubblicazione di un elenco dei portafogli europei di identità digitale certificati

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

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

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

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

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

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

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

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

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

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

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

7. Entro ... [6 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione relativo all'attuazione dei portafogli europei di identità digitale di cui all'articolo 5 bis, paragrafo 23, stabilisce i formati e le procedure applicabili ai fini dei paragrafi 1, 4 e 5 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 5 sexies

Violazione della sicurezza dei portafogli europei di identità digitale

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

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

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

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

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

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

5. Entro … [6 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili alle misure di cui ai paragrafi 1, 2 e 3 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 5 septies

Ricorso transfrontaliero ai portafogli europei di identità digitale

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

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

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

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

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

---

* 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).

** 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).

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

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

6) prima dell'articolo 6 è inserito il titolo seguente:

"SEZIONE 2
REGIMI DI IDENTIFICAZIONE ELETTRONICA";

7) all'articolo 7, la lettera g) è sostituita dalla seguente:

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

8) all'articolo 8, paragrafo 3, il primo comma è sostituito dal seguente:

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

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

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

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

10) all'articolo 10, il titolo è sostituito dal seguente:

"Violazione della sicurezza dei regimi di identificazione elettronica";

11) è inserito l'articolo seguente:

"*Articolo 11 bis*
Corrispondenza dell'identità a livello transfrontaliero

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

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

3. Entro … [6 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai requisiti di cui al paragrafo 1 del presente articolo mediante atti di esecuzione. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

12) l’articolo 12 è così modificato:

a) il titolo è sostituito dal seguente:

"Interoperabilità";

b) il paragrafo 3 è così modificato:

i) la lettera c) è sostituita dalla seguente:

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

ii) la lettera d) è soppressa;

c) 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 una persona fisica o giuridica, una persona fisica che rappresenta un'altra persona fisica o una persona giuridica disponibile nell'ambito dei regimi di identificazione elettronica;"

d) i paragrafi 5 e 6 sono sostituiti dai seguenti:

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

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

e) il paragrafo 7 è soppresso;

f) il paragrafo 8 è sostituito dal seguente:

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

13) al capo II sono inseriti gli articoli seguente:

"*Articolo 12 bis*

Certificazione dei regimi di identificazione elettronica

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

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

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

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

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

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

Articolo 12 ter

Accesso a componenti hardware e software

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

---

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

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

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

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

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

15) gli articoli 14, 15 e 16 sono sostituiti dai seguenti:

"Articolo 14
Aspetti internazionali

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

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

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

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

Articolo 15
Accessibilità per le persone con disabilità ed esigenze particolari

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

Articolo 16
Sanzioni

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

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

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

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

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

---

* Direttiva (UE) 2022/2555 del Parlamento europeo e del Consiglio, del 14 dicembre 2022, relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, recante modifica del regolamento (UE) n. 910/2014 e della direttiva (UE) 2018/1972 e che abroga la direttiva (UE) 2016/1148 (direttiva NIS 2) (GU L 333 del 27.12.2022, pag. 80).";

16) al capo III, sezione 2, il titolo è sostituito dal seguente:

"Servizi fiduciari non qualificati";

17) gli articoli 17 e 18 sono soppressi;

18) al capo III, sezione 2, è inserito l'articolo 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 tipo, sia diretti che indiretti, per la prestazione del servizio fiduciario non qualificato, le quali, fatto salvo l'articolo 21 della direttiva (UE) 2022/2555, comprendono almeno misure relative:

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

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

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

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

2. Entro … [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili al paragrafo 1, lettera a), del presente articolo. Si presume che i requisiti di cui al presente articolo siano stati rispettati, ove siano rispettate tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

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

b) sono inseriti i paragrafi seguente:

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

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

c) i paragrafi 2, 3 e 4’ sono sostituiti dai seguenti:

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

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

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

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

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

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

"4. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure riguardo a quanto segue:

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

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

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

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

20) l'articolo 21 è così modificato:

a) i paragrafi 1 e 2 sono sostituiti dai seguenti:

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

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

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

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

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

b) il paragrafo 4 è sostituito dal seguente:

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

21) 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 deve essere rilasciato il certificato qualificato o l'attestato elettronico di attributi qualificato.

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

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

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

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

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

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

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

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

c) mediante un attestato elettronico di attributi qualificato;

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

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

1 quater. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure per la verifica dell'identità e degli attributi conformemente ai paragrafi 1, 1 bis e 1 ter. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2 ";

b) il paragrafo 2 è così modificato:

i) la lettera a) è sostituita dalla seguente:

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

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

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

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

iii) sono inserite le lettere seguenti:

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

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

ii) controlli procedurali o amministrativi;

iii) gestione e attuazione dei servizi;

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

iv) le lettere g), h) e i) 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 giudiziari e per assicurare la continuità del servizio. Tali registrazioni possono essere elettroniche;

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

v) la lettera j) è soppressa;

vi) è aggiunto il comma seguente:

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

c) il paragrafo 5 è sostituito dai seguenti:

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

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

5. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo], la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure riguardo ai requisiti di cui al paragrafo 2, del presente articolo. Si presume che i requisiti di cui al presente paragrafo siano stati rispettati ove siano rispettate tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

22) al capo III, sezione 3, è inserito l'articolo seguente:

"*Articolo 24 bis*

Riconoscimento dei servizi fiduciari qualificati

1. Le firme elettroniche qualificate basate su un certificato qualificato rilasciato in uno Stato membro e i sigilli elettronici qualificati basati su un certificato qualificato rilasciato in uno Stato membro sono riconosciuti rispettivamente quali firme elettroniche qualificate e sigilli elettronici qualificati in tutti gli altri Stati membri.

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

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

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

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

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

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

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

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

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

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

23) all'articolo 25, il paragrafo 3 è soppresso;

24) l'articolo 26 è così modificato:

a) il comma unico diventa paragrafo 1;

b) è aggiunto il paragrafo seguente:

"2. Entro ... [24 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione valuta la necessità di adottare atti di esecuzione per stabilire un elenco di norme di riferimento e, se necessario, stabilire specifiche e procedure applicabili alle firme elettroniche avanzate. Sulla base di tale valutazione, la Commissione può adottare tali atti di esecuzione. Si presume che i requisiti delle firme elettroniche avanzate siano stati rispettati ove una firma elettronica avanzata sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

25) all'articolo 27, il paragrafo 4 è soppresso;

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

"6. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai certificati qualificati di firma elettronica. Si presume che i requisiti di cui all'allegato I siano stati rispettati ove un certificato qualificato di firma elettronica sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo2.";

27) all'articolo 29 è inserito il paragrafo seguente:

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

28) è inserito l'articolo seguente:

"*Articolo 29 bis*
Requisiti relativi ai servizi qualificati per la gestione di
dispositivi qualificati per la creazione di una firma elettronica a distanza

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

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

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

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

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

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

2. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, specifiche e procedure ai fini del paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

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

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

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

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

31) l'articolo 32 è così modificato:

a) al paragrafo 1 è aggiunto il comma seguente:

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

b) il paragrafo 3 è sostituito dal seguente:

"3. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili alla convalida delle firme elettroniche qualificate. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

32) è inserito l'articolo 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 a condizione che:

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

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

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

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

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

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

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

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

3. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili alla convalida delle firme elettroniche avanzate basate su certificati qualificati. Si presume che i requisiti di cui al paragrafo 1 del presente articolo siano stati rispettati ove la convalida di una firma elettronica avanzata su certificati qualificati sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

33) all'articolo 33, il paragrafo 2 è sostituito dal seguente:

"2. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili al servizio di convalida qualificato di cui al paragrafo 1 del presente articolo. Si presume che i requisiti di cui al paragrafo 1 del presente articolo siano stati rispettati ove il servizio di convalida qualificato delle firme elettroniche qualificate sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

34) l'articolo 34 è così modificato:

a) è inserito il paragrafo seguente:

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

b) il paragrafo 2 è sostituito dal seguente:

"2. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili al servizio di conservazione qualificato delle firme elettroniche qualificate. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

35) all'articolo 35, il paragrafo 3 è soppresso;

36) l'articolo 36 è così modificato:

a) il comma unico diventa paragrafo 1;

b) è aggiunto il paragrafo seguente:

"2. Entro ... [24 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione valuta la necessità di adottare atti di esecuzione per stabilire un elenco di norme di riferimento e, se necessario, stabilire specifiche e procedure applicabili ai sigilli elettronici avanzati. Sulla base di tale valutazione, la Commissione può adottare tali atti di esecuzione. Si presume che i requisiti dei sigilli elettronici avanzati siano stati rispettati ove un sigillo elettronico avanzato sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

37) all'articolo 37, il paragrafo 4 è soppresso;

38) all'articolo 38, il paragrafo 6 è sostituito dal seguente:

"6. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai certificati qualificati dei sigilli elettronici. Si presume che i requisiti di cui all'allegato III siano stati rispettati ove un certificato qualificato di sigillo elettronico sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

39) è inserito l'articolo seguente:

"*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.";

40) al capo III, sezione 5, è inserito l'articolo seguente:

"*Articolo 40 bis*
Requisiti per la convalida dei sigilli elettronici avanzati basati su certificati qualificati

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

41) all'articolo 41, il paragrafo 3 è soppresso;

42) l'articolo 42 è così modificato:

a) è inserito il paragrafo seguente:

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

b) il paragrafo 2 è sostituito dal seguente:

"2. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili sia al collegamento della data e dell'ora ai dati sia alla determinazione dell'accuratezza delle fonti di misurazione del tempo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

43) l'articolo 44 è così modificato:

a) è inserito il paragrafo seguente:

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

b) il paragrafo 2 è sostituito dal seguente:

"2. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai processi di invio e ricezione dei dati. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

c) sono inseriti i paragrafi seguenti:

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

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

44) 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 di tali requisiti è effettuata conformemente alle norme, alle specifiche e alle procedure di cui al paragrafo 2 del presente articolo.

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

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

2. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai certificati qualificati di autenticazione di siti web, di cui al paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

45) è inserito l'articolo seguente:

"*Articolo 45 bis*
Misure precauzionali in materia di cibersicurezza

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

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

3. Qualora adotti misure precauzionali a norma del paragrafo 2, il fornitore di browser web notifica per iscritto, senza indebito ritardo, le sue preoccupazioni, unitamente a una descrizione delle misure adottate per attenuare tali preoccupazioni, alla Commissione, all'organismo di vigilanza competente, al soggetto al quale è stato rilasciato il certificato e al prestatore di servizi fiduciari qualificato che ha rilasciato tale certificato o insieme di certificati. Al ricevimento di tale notifica, l'organismo di vigilanza competente rilascia un avviso di ricevimento al fornitore di browser web in questione.

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

46) al capo III sono aggiunte le sezioni seguenti:

"SEZIONE 9
ATTESTATI ELETTRONICI DI ATTRIBUTI

Articolo 45 ter
Effetti giuridici degli attestati elettronici di attributi

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

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

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

Articolo 45 quater

Attestati elettronici di attributi nei servizi pubblici

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

Articolo 45 quinquies

Requisiti per gli attestati elettronici qualificati di attributi

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

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

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

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

5. Entro ... [6 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili agli attestati elettronici qualificati di attributi. Tali atti di esecuzione sono coerenti con gli atti di esecuzione di cui all'articolo 5 bis, paragrafo 23, relativi all'attuazione del portafoglio europeo di identità digitale. Essi sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 45 sexies

Verifica degli attributi rispetto a fonti autentiche

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

2. Entro ... [6 mesi dalla data di entrata in vigore del presente regolamento modificativo], tenendo conto delle pertinenti norme internazionali, la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili al catalogo di attributi, nonché i regimi per gli attestati di attributi e le procedure di verifica degli attestati elettronici qualificati di attributi ai fini del paragrafo 1 del presente articolo. Tali atti di esecuzione sono coerenti con gli atti di esecuzione di cui all'articolo 5 bis, paragrafo 23, relativi all'attuazione del portafoglio europeo di identità digitale. Sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 45 septies

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

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

   a) i requisiti di cui all'allegato VII;

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

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

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

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

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

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

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

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

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

7. Entro … [6 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai fini del paragrafo 3 del presente articolo. Tali atti di esecuzione sono coerenti con gli atti di esecuzione di cui all'articolo 5 bis, paragrafo 23, relativi all'attuazione del portafoglio europeo di identità digitale. Essi sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

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

Articolo 45 octies

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

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

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

Articolo 45 nonies

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

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

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

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

SEZIONE 10

SERVIZI DI ARCHIVIAZIONE ELETTRONICA

Articolo 45 decies

Effetti giuridici dei servizi di archiviazione elettronica

1. Ai dati elettronici e ai documenti elettronici conservati mediante un servizio di archiviazione elettronica non vengono negati gli effetti giuridici né l'ammissibilità come prova in procedimenti giudiziari per il solo motivo della loro forma elettronica o perché non sono conservati mediante un servizio di archiviazione elettronica qualificato.

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

Articolo 45 undecies

Requisiti per i servizi di archiviazione elettronica qualificati

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

   a) sono forniti da prestatori di servizi fiduciari qualificati;

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

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

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

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

2. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai servizi di archiviazione elettronica qualificati. Si presume che i requisiti dei servizi di archiviazione elettronica qualificati siano rispettati ove un servizio di archiviazione elettronica qualificato sia conforme a tali norme, specifiche e procedure. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

SEZIONE 11
REGISTRI ELETTRONICI

Articolo 45 duodecies
Effetti giuridici dei registri elettronici

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

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

Articolo 45 terdecies
Requisiti per i registri elettronici qualificati

1. I registri elettronici qualificati soddisfano i requisiti seguenti:

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

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

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

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

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

3. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce un elenco di norme di riferimento e, se necessario, stabilisce specifiche e procedure applicabili ai requisiti di cui al paragrafo 1 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

47) è inserito il capo seguente:

"CAPO IV bis
QUADRO DI GOVERNANCE

Articolo 46 bis
Vigilanza sul quadro relativo al portafoglio europeo di identità digitale

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

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

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

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

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

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

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

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

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

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

d) effettuare ispezioni in loco e supervisione a distanza;

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

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

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

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

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

7. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo], la Commissione, mediante atti di esecuzione, stabilisce i formati e le procedure applicabili alla relazione di cui al paragrafo 6 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 46 ter

Vigilanza dei servizi fiduciari

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo], la Commissione adotta orientamenti sull'esercizio, da parte degli organismi di vigilanza designati a norma del paragrafo 1 del presente articolo, dei compiti di cui al paragrafo 4 del presente articolo e, mediante atti di esecuzione, stabilisce i formati e le procedure applicabili alla relazione di cui al paragrafo 6 del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.

Articolo 46 quater
Punti di contatto unici

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

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

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

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

Articolo 46 quinquies
Assistenza reciproca

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

2. L'assistenza reciproca implica almeno quanto segue:

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

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

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

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

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

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

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

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

4. Entro ... [12 mesi dalla data di entrata in vigore del presente regolamento modificativo], e successivamente ogni due anni, il gruppo di cooperazione istituito a norma dell'articolo 46 sexies, paragrafo 1, emana orientamenti sugli aspetti organizzativi e sulle procedure relativi all'assistenza reciproca di cui ai paragrafi 1 e 2 del presente articolo.

Articolo 46 sexies
Gruppo di cooperazione per l'identità digitale europea

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

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

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

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

5. Il gruppo di cooperazione svolge i compiti seguenti:

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

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

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

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

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

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

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

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

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

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

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

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

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

7. Entro il ... [12 mesi dall'entrata in vigore del presente regolamento modificativo] la Commissione, mediante atti di esecuzione, stabilisce le modalità procedurali necessarie per facilitare la cooperazione tra gli Stati membri di cui al paragrafo 5, lettera d), del presente articolo. Tali atti di esecuzione sono adottati secondo la procedura d'esame di cui all'articolo 48, paragrafo 2.";

48) l'articolo 47 è così modificato:

a) i paragrafi 2 e 3 sono sostituiti dai seguenti:

"2. Il potere di adottare gli atti delegati di cui all'articolo 5 quater, paragrafo 7, all'articolo 24, paragrafo 4 ter, e all'articolo 30, paragrafo 4, è conferito alla Commissione per un periodo indeterminato a decorrere dal 17 settembre 2014.

3. La delega di potere di cui all'articolo 5 quater, paragrafo 7, all'articolo 24, paragrafo 4 ter, e all'articolo 30, paragrafo 4, può essere revocata in qualsiasi momento dal Parlamento europeo o dal Consiglio. La decisione di revoca pone fine alla delega di potere ivi specificata. Gli effetti della decisione decorrono dal giorno successivo alla pubblicazione della decisione nella *Gazzetta ufficiale dell'Unione europea* o da una data successiva ivi specificata. Essa non pregiudica la validità degli atti delegati già in vigore.";

b) il paragrafo 5 è sostituito dal seguente:

"5. L'atto delegato adottato ai sensi dell'articolo 5 quater, paragrafo 7, dell'articolo 24, paragrafo 4 ter, o dell'articolo 30, paragrafo 4, entra in vigore solo se né il Parlamento europeo né il Consiglio hanno sollevato obiezioni entro il termine di due mesi dalla data in cui esso è stato loro notificato o se, prima della scadenza di tale termine, sia il Parlamento europeo che il Consiglio hanno informato la Commissione che non intendono sollevare obiezioni. Tale termine è prorogato di due mesi su iniziativa del Parlamento europeo o del Consiglio.";

49) al capo VI è inserito l'articolo seguente:

"*Articolo 48 bis*
Obblighi di comunicazione

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

2. Le statistiche raccolte conformemente al paragrafo 1 comprendono:

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

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

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

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

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

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

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

50) l'articolo 49 è sostituito dal seguente:

"*Articolo 49*
Riesame

1. La Commissione riesamina l'applicazione del presente regolamento e presenta, entro ... [24 mesi dalla data di entrata in vigore del regolamento modificativo], una relazione in proposito al Parlamento europeo e al Consiglio. In tale relazione, in particolare, la Commissione valuta se sia opportuno modificare l'ambito di applicazione del presente regolamento o sue disposizioni specifiche, comprese, segnatamente, le disposizioni di cui all'articolo 5 quater, paragrafo 5, tenendo conto dell'esperienza acquisita nell'applicazione del regolamento stesso e dei progressi tecnologici, dell'evoluzione del mercato e degli sviluppi giuridici. Se necessario, tale relazione è corredata di una proposta di modifica del presente regolamento.

2. La relazione di cui al paragrafo 1 comprende una valutazione della disponibilità, della sicurezza e dell'utilizzabilità dei mezzi di identificazione elettronica notificati e dei passaporti europei di identità digitale che rientrano nell'ambito di applicazione del presente regolamento, ed esamina se sia necessario imporre a tutti i prestatori di servizi privati online che fanno affidamento su servizi di identificazione elettronica di terzi per l'autenticazione degli utenti di accettare l'utilizzo di mezzi di identificazione elettronica notificati e del portafoglio europeo di identità digitale.

3. Entro … [sei anni dalla data di entrata in vigore del regolamento modificativo], e successivamente ogni quattro anni, la Commissione presenta al Parlamento europeo e al Consiglio una relazione sui progressi compiuti nella realizzazione degli obiettivi del presente regolamento.";

51) l'articolo 51 è sostituito dal seguente:

"*Articolo 51*
Misure transitorie

1. I dispositivi per la creazione di una firma sicura la cui conformità sia stata determinata conformemente all'articolo 3, paragrafo 4, della direttiva 1999/93/CE continuano a essere considerati dispositivi qualificati per la creazione di una firma elettronica a norma del presente regolamento fino al ... [36 mesi dopo l'entrata in vigore del presente regolamento modificativo].

2. I certificati qualificati rilasciati a persone fisiche a norma della direttiva 1999/93/CE continuano a essere considerati certificati qualificati di firme elettroniche a norma del presente regolamento fino al ... [24 mesi dopo l'entrata in vigore del presente regolamento modificativo].

3. La gestione di dispositivi qualificati per la creazione di una firma elettronica e di sigilli elettronici a distanza da parte di prestatori di servizi fiduciari qualificati diversi dai prestatori di servizi fiduciari qualificati che forniscono servizi fiduciari qualificati per la gestione di dispositivi qualificati per la creazione di una firma e di un sigillo elettronici a distanza conformemente agli articoli 29 bis e 39 bis può essere effettuata senza la necessità di ottenere la qualifica per la prestazione di tali servizi di gestione fino al .... [24 mesi dopo l'entrata in vigore del presente regolamento modificativo].

4. 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 presente regolamento modificativo] presentano all'organismo di vigilanza una relazione di valutazione della conformità che attesti il rispetto dell'articolo 24, paragrafi 1, 1 bis e 1 ter, quanto prima e comunque entro il ... [24 mesi dall'entrata in vigore del presente regolamento modificativo].

52) gli allegati da I a IV sono modificati, rispettivamente, secondo gli allegati da I a IV del presente regolamento;

53) sono aggiunti i nuovi allegati V, VI e VII che figurano negli allegati V, VI e VII del presente regolamento.

Articolo 2

Entrata in vigore

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,

Per il Parlamento europeo	*Per il Consiglio*
La presidente	*Il presidente*

ALLEGATO I

Nell'allegato I del regolamento (UE) n. 910/2014, 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

Nell'allegato II del regolamento (UE) n. 910/2014, i punti 3 e 4 sono soppressi.

ALLEGATO III

Nell'allegato III del regolamento (UE) n. 910/2014, 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

L'allegato IV del regolamento (UE) n. 910/2014 è così modificato:

1) la lettera c) è sostituita dalla seguente:

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

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

2) 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

"ALLEGATO V

REQUISITI PER GLI ATTESTATI ELETTRONICI QUALIFICATI DI ATTRIBUTI

Gli attestati elettronici qualificati di attributi contengono:

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

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

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

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

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

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

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

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

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

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

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

ALLEGATO VI

"ALLEGATO VI

ELENCO MINIMO DI ATTRIBUTI

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

1. indirizzo;

2. età;

3. genere;

4. stato civile;

5. composizione del nucleo familiare;

6. nazionalità o cittadinanza;

7. titoli e licenze di studio;

8. qualifiche e licenze professionali;

9. poteri e mandati di rappresentanza di persone fisiche o giuridiche

10. permessi e licenze pubblici;

11. per le persone giuridiche, i dati societari e finanziari.".

ALLEGATO VII

"ALLEGATO VII

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

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

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

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

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

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

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

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

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

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

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