DECISIONE DI ESECUZIONE (UE) 2022/483 DELLA COMMISSIONE

del 21 marzo 2022

che modifica la decisione di esecuzione (UE) 2021/1073 che stabilisce specifiche tecniche e norme per l'attuazione del quadro di fiducia per il certificato COVID digitale dell'UE istituito dal regolamento (UE) 2021/953 del Parlamento europeo e del Consiglio

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

visto il regolamento (UE) 2021/953 del Parlamento europeo e del Consiglio, del 14 giugno 2021, su un quadro per il rilascio, la verifica e l'accettazione di certificati interoperabili di vaccinazione, di test e di guarigione in relazione alla COVID-19 (certificato COVID digitale dell'UE) per agevolare la libera circolazione delle persone durante la pandemia di COVID-19 ([1]), in particolare l'articolo 9, paragrafo 1,

considerando quanto segue:

(1) Il regolamento (UE) 2021/953 stabilisce il certificato COVID digitale dell'UE, il quale comprova che il titolare ha ricevuto un vaccino anti COVID-19, un risultato negativo a un test o è guarito dall'infezione, con lo scopo di agevolare l'esercizio del diritto di libera circolazione durante la pandemia di COVID-19 da parte dei loro titolari.

(2) Il regolamento (UE) 2021/954 del Parlamento europeo e del Consiglio ([2]) dispone che gli Stati membri applichino le norme stabilite nel regolamento (UE) 2021/953 ai cittadini di paesi terzi che non rientrano nell'ambito di applicazione di tale regolamento ma che soggiornano regolarmente o risiedono nel loro territorio e che sono autorizzati a spostarsi in altri Stati membri ai sensi del diritto dell'Unione.

(3) A norma della raccomandazione (UE) 2022/290 del Consiglio che modifica la raccomandazione (UE) 2020/912 relativa alla restrizione temporanea dei viaggi non essenziali verso l'UE e all'eventuale revoca di tale restrizione ([3]), i cittadini di paesi terzi che intendono effettuare un viaggio non essenziale da un paese terzo verso l'Unione dovrebbero essere in possesso di una prova valida della vaccinazione o della guarigione, come un certificato COVID digitale dell'UE o un certificato COVID-19 rilasciato da un paese terzo contemplato da un atto di esecuzione adottato a norma dell'articolo 8, paragrafo 2, del regolamento (UE) 2021/953.

(4) Affinché il certificato COVID digitale dell'UE sia operativo in tutta l'Unione, la Commissione ha adottato la decisione di esecuzione (UE) 2021/1073 ([4]), che stabilisce specifiche tecniche e norme per compilare, rilasciare in modo sicuro e verificare i certificati COVID digitali dell'UE, garantire la protezione dei dati personali, stabilire la struttura comune dell'identificativo univoco del certificato e creare un codice a barre valido, sicuro e interoperabile.

(5) Conformemente all'articolo 4 del regolamento (UE) 2021/953, la Commissione e gli Stati membri dovevano istituire e mantenere un quadro di fiducia per il certificato COVID digitale dell'UE. Tale quadro di fiducia è in grado di sostenere lo scambio bilaterale degli elenchi dei certificati revocati contenenti gli identificativi univoci dei certificati revocati.

([1]) GU L 211 del 15.6.2021, pag. 1.

([2]) Regolamento (UE) 2021/954 del Parlamento europeo e del Consiglio, del 14 giugno 2021, su un quadro per il rilascio, la verifica e l'accettazione di certificati interoperabili di vaccinazione, di test e di guarigione in relazione alla COVID-19 (certificato COVID digitale dell'UE) per i cittadini di paesi terzi regolarmente soggiornanti o residenti nel territorio degli Stati membri durante la pandemia di COVID-19 (GU L 211 del 15.6.2021, pag. 24).

([3]) Raccomandazione (UE) 2022/290 del Consiglio, del 22 febbraio 2022, che modifica la raccomandazione (UE) 2020/912 del Consiglio relativa alla restrizione temporanea dei viaggi non essenziali verso l'UE e all'eventuale revoca di tale restrizione (GU L 43 del 24.2.2022, pag. 79).

([4]) Decisione di esecuzione (UE) 2021/1073 della Commissione, del 28 giugno 2021, che stabilisce specifiche tecniche e norme per l'attuazione del quadro di fiducia per il certificato COVID digitale dell'UE istituito dal regolamento (UE) 2021/953 del Parlamento europeo e del Consiglio (GU L 230 del 30.6.2021, pag. 32).

(6) Il 1º luglio 2021 è diventato operativo il gateway per i certificati COVID digitali dell'UE (il «gateway»), che costituisce la parte centrale del quadro di fiducia e consente lo scambio sicuro e affidabile tra gli Stati membri delle chiavi pubbliche utilizzate per la verifica dei certificati COVID digitali dell'UE.

(7) In seguito al successo della loro introduzione su larga scala, i certificati COVID digitali dell'UE sono diventati un bersaglio per i truffatori che cercano modi per rilasciare certificati fraudolenti. Tali certificati fraudolenti devono pertanto essere revocati. Inoltre alcuni certificati COVID digitali dell'UE possono essere revocati dagli Stati membri a livello nazionale per motivi medici e di salute pubblica, ad esempio perché una partita di vaccini somministrati è successivamente risultata difettosa.

(8) Mentre il sistema del certificato COVID digitale dell'UE è in grado di smascherare immediatamente i certificati falsificati, i certificati autentici rilasciati illecitamente sulla base di documenti falsi, a seguito di un accesso non autorizzato o con intento fraudolento non possono essere individuati negli altri Stati membri a meno che gli elenchi dei certificati revocati generati a livello nazionale non siano scambiati tra gli Stati membri. Lo stesso vale per i certificati che sono stati revocati per motivi medici e di salute pubblica. Il mancato rilevamento, da parte delle applicazioni di verifica degli Stati membri, dei certificati revocati da altri Stati membri costituisce una minaccia per la salute pubblica e indebolisce la fiducia dei cittadini nel sistema del certificato COVID digitale dell'UE.

(9) Come indicato al considerando 19 del regolamento (UE) 2021/953, per motivi medici e di salute pubblica e in caso di certificati rilasciati o ottenuti fraudolentemente, è opportuno che gli Stati membri possano stilare e scambiare con altri Stati membri, ai fini di tale regolamento, elenchi di revoca dei certificati per casi limitati, in particolare per quanto riguarda i certificati rilasciati erroneamente, come conseguenza di una frode o a seguito della sospensione di una partita di vaccino anti COVID-19 risultata difettosa. Gli Stati membri non dovrebbero poter revocare i certificati rilasciati dagli altri Stati membri. Gli elenchi di revoca dei certificati scambiati non dovrebbero contenere dati personali diversi da quelli identificativi unici dei certificati. In particolare non dovrebbero includere il motivo per cui un certificato è stato revocato.

(10) Oltre alle informazioni generali sulla possibilità di revoca dei certificati e sui possibili motivi di tale misura, i titolari dei certificati revocati dovrebbero essere tempestivamente informati della revoca dei loro certificati e dei motivi della revoca dall'autorità di rilascio responsabile. In alcune circostanze, in particolare nel caso dei certificati COVID digitali dell'UE rilasciati in formato cartaceo, rintracciare il titolare e informarlo della revoca potrebbe tuttavia risultare impossibile o comportare uno sforzo sproporzionato. Gli Stati membri non dovrebbero raccogliere dati personali aggiuntivi non necessari per il processo di rilascio solo per poter informare i titolari in caso di revoca dei loro certificati.

(11) È pertanto necessario rafforzare il quadro di fiducia per il certificato COVID digitale dell'UE sostenendo lo scambio bilaterale tra gli Stati membri degli elenchi dei certificati revocati.

(12) La presente decisione non riguarda la sospensione temporanea dei certificati per casi di uso nazionale che esulano dall'ambito di applicazione del regolamento sul certificato COVID digitale dell'UE, ad esempio perché il titolare di un certificato di vaccinazione è risultato positivo al SARS-CoV-2. Essa non pregiudica le procedure stabilite per verificare le regole operative per la validità dei certificati.

(13) Sebbene siano tecnicamente possibili diverse architetture per lo scambio degli elenchi dei certificati revocati, la più appropriata consiste nello scambiarli tramite il gateway, in quanto limita gli scambi di dati al quadro di fiducia già istituito e, rispetto a un sistema alternativo peer-to-peer, riduce al minimo il numero dei possibili punti di vulnerabilità come pure degli scambi tra Stati membri.

(14) Il gateway per i certificati COVID digitali dell'UE dovrebbe di conseguenza essere rafforzato per sostenere lo scambio sicuro dei certificati COVID digitali dell'UE revocati ai fini della loro verifica sicura tramite il gateway. A tale riguardo dovrebbero essere attuate misure di sicurezza adeguate per proteggere i dati personali trattati nel gateway. Per garantire un livello elevato di protezione, gli Stati membri dovrebbero pseudonimizzare gli attributi dei certificati mediante un hash irreversibile da includere negli elenchi dei certificati revocati. L'identificativo univoco dovrebbe quindi essere considerato un dato pseudonimizzato per i trattamenti effettuati nel quadro del gateway.

(15) È inoltre opportuno stabilire disposizioni sul ruolo degli Stati membri e della Commissione per quanto riguarda lo scambio degli elenchi dei certificati revocati.

(16) Il trattamento dei dati personali dei titolari dei certificati, effettuato sotto la responsabilità degli Stati membri o di altre organizzazioni pubbliche o organismi ufficiali degli Stati membri, dovrebbe essere realizzato conformemente al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([5]). Il trattamento dei dati personali effettuato sotto la responsabilità della Commissione allo scopo di gestire e garantire la sicurezza del gateway per i certificati COVID digitali dell'UE dovrebbe ottemperare alle disposizioni del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([6]).

(17) Gli Stati membri, rappresentati dalle autorità nazionali o dagli organismi ufficiali designati, determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali tramite il gateway per i certificati COVID digitali dell'UE e sono pertanto contitolari del trattamento. L'articolo 26 del regolamento (UE) 2016/679 prevede l'obbligo per i contitolari del trattamento dei dati personali di determinare in modo trasparente le rispettive responsabilità in merito all'osservanza degli obblighi derivanti da detto regolamento. Esso prevede inoltre la possibilità che tali responsabilità siano determinate dal diritto dell'Unione o dello Stato membro cui i titolari del trattamento sono soggetti. L'accordo di cui all'articolo 26 dovrebbe essere incluso nell'allegato III della presente decisione.

(18) Il regolamento (UE) 2021/953 attribuisce alla Commissione il compito di sostenere tali scambi. Il modo più appropriato per adempiere tale mandato consiste nel raccogliere per conto degli Stati membri gli elenchi dei certificati revocati presentati. Alla Commissione dovrebbe pertanto essere assegnato un ruolo di responsabile del trattamento per sostenere tali scambi agevolando lo scambio degli elenchi tramite il gateway per i certificati COVID digitali dell'UE per conto degli Stati membri.

(19) La Commissione, in quanto fornitrice di soluzioni tecniche e organizzative per il gateway per i certificati COVID digitali dell'UE, procede al trattamento dei dati personali contenuti negli elenchi dei certificati revocati nel gateway per conto degli Stati membri quali contitolari del trattamento. Agisce pertanto in qualità di responsabile del trattamento. A norma dell'articolo 28 del regolamento (UE) 2016/679 e dell'articolo 29 del regolamento (UE) 2018/1725, i trattamenti da parte di un responsabile del trattamento devono essere disciplinati da un contratto o da un atto giuridico, a norma del diritto dell'Unione o di uno Stato membro, che vincoli il responsabile del trattamento al titolare del trattamento e che specifichi i trattamenti. È pertanto necessario stabilire norme relative ai trattamenti da parte della Commissione in qualità di responsabile del trattamento.

(20) Il compito di sostegno della Commissione non comporta la costituzione di una banca dati centralizzata di cui al considerando 52 del regolamento (UE) 2021/953. Tale divieto è inteso a evitare la creazione di un archivio centrale di tutti i certificati COVID digitali dell'UE rilasciati e non impedisce agli Stati membri di scambiare gli elenchi dei certificati revocati, possibilità espressamente prevista all'articolo 4, paragrafo 2, del regolamento (UE) 2021/953.

(21) Nell'effettuare il trattamento dei dati personali nel quadro del gateway per i certificati COVID digitali dell'UE, la Commissione è vincolata dalla sua decisione (UE, Euratom) 2017/46 ([7]).

(22) L'articolo 3, paragrafo 10, del regolamento (UE) 2021/953 consente alla Commissione di adottare atti di esecuzione che stabiliscono che i certificati COVID-19 rilasciati da un paese terzo con il quale l'Unione e gli Stati membri hanno concluso un accordo sulla libera circolazione delle persone che consente alle parti contraenti di limitare in modo non discriminatorio la libera circolazione per motivi di sanità pubblica e che non contiene un meccanismo di incorporazione degli atti giuridici dell'Unione sono equivalenti a quelli rilasciati in conformità di tale regolamento. Su tale base l'8 luglio 2021 la Commissione ha adottato la decisione di esecuzione (UE) 2021/1126 ([8]) che stabilisce l'equivalenza dei certificati COVID-19 rilasciati dalla Svizzera.

([5]) Regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio, del 27 aprile 2016, relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali, nonché alla libera circolazione di tali dati e che abroga la direttiva 95/46/CE (regolamento generale sulla protezione dei dati) (GU L 119 del 4.5.2016, pag. 1).

([6]) 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).

([7]) La Commissione pubblica ulteriori informazioni sulle norme di sicurezza valide per tutti i sistemi informatici della Commissione europea alla pagina: https://ec.europa.eu/info/publications/security-standards-applying-all-european-commission-information-systems_it.

([8]) Decisione di esecuzione (UE) 2021/1126 della Commissione, dell'8 luglio 2021, che stabilisce l'equivalenza dei certificati COVID-19 rilasciati dalla Svizzera ai certificati rilasciati a norma del regolamento (UE) 2021/953 del Parlamento europeo e del Consiglio (GU L 243 del 9.7.2021, pag. 49).

(23) L'articolo 8, paragrafo 2, del regolamento (UE) 2021/953 consente alla Commissione di adottare atti di esecuzione che stabiliscono che i certificati COVID-19 rilasciati da un paese terzo secondo norme e sistemi tecnologici che sono interoperabili con il quadro di fiducia per il certificato COVID digitale dell'UE, che consentono la verifica dell'autenticità, della validità e dell'integrità del certificato e che contengono i dati di cui all'allegato del regolamento, devono essere considerati equivalenti ai certificati COVID digitali dell'UE, al fine di agevolare l'esercizio del diritto di libera circolazione all'interno dell'Unione da parte dei loro titolari. Come indicato al considerando 28 del regolamento (UE) 2021/953, l'articolo 8, paragrafo 2, di tale regolamento riguarda l'accettazione dei certificati rilasciati da paesi terzi ai cittadini dell'Unione e ai loro familiari. La Commissione ha già adottato diversi atti di esecuzione di questo tipo.

(24) Onde evitare lacune nell'individuazione dei certificati revocati contemplati da tali atti di esecuzione, i paesi terzi i cui certificati COVID-19 sono stati considerati equivalenti a norma dell'articolo 3, paragrafo 10, e dell'articolo 8, paragrafo 2, del regolamento (UE) 2021/953 dovrebbero anche poter presentare i pertinenti elenchi dei certificati revocati al gateway per i certificati COVID digitali dell'UE.

(25) Alcuni cittadini di paesi terzi titolari di certificati COVID-19 revocati rilasciati da un paese terzo i cui certificati COVID-19 sono stati considerati equivalenti a norma del regolamento (UE) 2021/953 possono non rientrare nell'ambito di applicazione di tale regolamento o del regolamento (UE) 2021/954 nel momento in cui un elenco dei certificati revocati comprendente i loro certificati è generato dal paese terzo in questione. Nel momento in cui un elenco dei certificati revocati è generato da un determinato paese terzo non è tuttavia possibile sapere se tutti i cittadini di paesi terzi titolari dei certificati revocati rientrino nell'ambito di applicazione di uno dei suddetti regolamenti. Non è quindi possibile escludere le persone che non rientrano nell'ambito di applicazione di uno dei due regolamenti nel momento in cui sono generati gli elenchi dei certificati revocati di tali paesi e qualsiasi tentativo in tal senso comporterebbe per gli Stati membri l'impossibilità di individuare i certificati revocati detenuti da cittadini di paesi terzi che viaggiano verso l'Unione per la prima volta. Nondimeno anche i certificati revocati di tali cittadini di paesi terzi verrebbero verificati dagli Stati membri quando i loro titolari effettuano un viaggio verso l'Unione e, successivamente, quando viaggiano all'interno dell'Unione. I paesi terzi i cui certificati sono stati considerati equivalenti a norma del regolamento (UE) 2021/953 non partecipano alla governance del gateway e pertanto non si qualificano come contitolari del trattamento.

(26) Il certificato COVID digitale dell'UE si è inoltre dimostrato l'unico sistema di certificato COVID-19 operativo a livello internazionale su larga scala. Ha pertanto assunto un'importanza crescente nel mondo e ha contribuito ad affrontare la pandemia a livello internazionale, facilitando e rendendo sicuri gli spostamenti tra un paese e l'altro e favorendo la ripresa globale. Nel processo di adozione di altri atti di esecuzione a norma dell'articolo 8, paragrafo 2, del regolamento (UE) 2021/953 emergono nuove esigenze relative alla compilazione del certificato COVID digitale dell'UE. In base alle norme di cui alla decisione di esecuzione (UE) 2021/1073, il cognome è un campo obbligatorio nei contenuti tecnici del certificato. È necessario modificare tale requisito per promuovere l'inclusione e l'interoperabilità con altri sistemi, dato che in alcuni paesi terzi vi sono persone prive di cognome. Nei casi in cui non possa essere suddiviso in due parti, il nome del titolare del certificato dovrebbe essere inserito nello stesso campo (cognome o nome) del certificato COVID digitale dell'UE in cui sarebbe indicato nel documento di viaggio o d'identità del titolare. Tale modifica consentirebbe inoltre un migliore allineamento dei contenuti tecnici dei certificati alle specifiche attualmente in vigore sui documenti di viaggio a lettura ottica pubblicate dall'Organizzazione per l'aviazione civile internazionale.

(27) È pertanto opportuno modificare di conseguenza la decisione di esecuzione (UE) 2021/1073.

(28) Conformemente all'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725, il Garante europeo della protezione dei dati è stato consultato e ha formulato il suo parere l'11 marzo 2022.

(29) Al fine di concedere agli Stati membri e alla Commissione tempo sufficiente per attuare le modifiche necessarie a consentire lo scambio degli elenchi dei certificati revocati tramite il gateway per i certificati COVID digitali dell'UE, la presente decisione dovrebbe iniziare ad applicarsi quattro settimane dopo l'entrata in vigore.

(30) Le misure previste dalla presente decisione sono conformi al parere del comitato istituito a norma dell'articolo 14 del regolamento (UE) 2021/953,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

La decisione di esecuzione (UE) 2021/1073 è così modificata:

1) sono inseriti gli articoli 5 bis, 5 ter e 5 quater seguenti:

«*Articolo 5 bis*

Scambio degli elenchi dei certificati revocati

1. Il quadro di fiducia per il certificato COVID digitale dell'UE consente lo scambio degli elenchi dei certificati revocati tramite il gateway centrale per i certificati COVID digitali dell'UE (il «gateway»), conformemente alle specifiche tecniche di cui all'allegato I.

2. Qualora revochino certificati COVID digitali dell'UE, gli Stati membri possono presentare al gateway gli elenchi dei certificati revocati.

3. Qualora gli Stati membri presentino elenchi dei certificati revocati, le autorità di rilascio tengono un elenco dei certificati revocati.

4. Qualora siano scambiati dati personali tramite il gateway, il trattamento è limitato alla finalità di sostenere lo scambio di informazioni sulla revoca. Tali dati personali sono utilizzati unicamente al fine di verificare lo stato di revoca dei certificati COVID digitali dell'UE rilasciati nell'ambito del regolamento (UE) 2021/953.

5. Le informazioni presentate al gateway comprendono i seguenti dati, conformemente alle specifiche tecniche di cui all'allegato I:

a) gli identificativi univoci pseudonimizzati dei certificati revocati;

b) una data di scadenza per l'elenco dei certificati revocati presentato.

6. Qualora revochi certificati COVID digitali dell'UE da essa rilasciati a norma del regolamento (UE) 2021/953 o del regolamento (UE) 2021/954 e intenda scambiare le pertinenti informazioni tramite il gateway, un'autorità di rilascio trasmette al gateway, in un formato sicuro, le informazioni di cui al paragrafo 5 sotto forma di elenchi dei certificati revocati, conformemente alle specifiche tecniche di cui all'allegato I.

7. Le autorità di rilascio forniscono, nella misura del possibile, una soluzione per informare i titolari dei certificati revocati in merito allo stato di revoca dei loro certificati e al motivo della revoca al momento della revoca stessa.

8. Il gateway raccoglie gli elenchi dei certificati revocati ricevuti. Esso fornisce strumenti per la distribuzione degli elenchi agli Stati membri. Cancella automaticamente gli elenchi in base alle date di scadenza indicate per ciascun elenco dall'autorità che lo ha presentato.

9. Le autorità nazionali o gli organismi ufficiali designati degli Stati membri che effettuano il trattamento dei dati personali nel gateway sono contitolari del trattamento dei dati. Le rispettive responsabilità dei contitolari del trattamento sono ripartite conformemente all'allegato VI.

10. La Commissione è responsabile del trattamento dei dati personali trattati all'interno del gateway. In qualità di responsabile del trattamento per conto degli Stati membri, la Commissione garantisce la sicurezza della trasmissione e dell'hosting dei dati personali all'interno del gateway e rispetta gli obblighi incombenti al responsabile del trattamento di cui all'allegato VII.

11. L'efficacia delle misure tecniche e organizzative volte a garantire la sicurezza del trattamento dei dati personali all'interno del gateway è periodicamente verificata, esaminata e valutata dalla Commissione e dai contitolari del trattamento.

Articolo 5 ter

Presentazione degli elenchi dei certificati revocati da parte di paesi terzi

I paesi terzi che rilasciano certificati COVID-19 per i quali la Commissione ha adottato un atto di esecuzione a norma dell'articolo 3, paragrafo 10, o dell'articolo 8, paragrafo 2, del regolamento (UE) 2021/953 possono presentare elenchi dei certificati COVID-19 revocati contemplati da tale atto di esecuzione, affinché siano trattati dalla Commissione per conto dei contitolari del trattamento nel gateway di cui all'articolo 5 *bis*, conformemente alle specifiche tecniche di cui all'allegato I.

Articolo 5 quater

Governance del trattamento dei dati personali nel gateway centrale per i certificati COVID digitali dell'UE

1. Il processo decisionale dei contitolari del trattamento è gestito da un gruppo di lavoro istituito nell'ambito del comitato di cui all'articolo 14 del regolamento (UE) 2021/953.

2. Le autorità nazionali o gli organismi ufficiali designati degli Stati membri che effettuano il trattamento dei dati personali nel gateway in qualità di contitolari del trattamento designano i rappresentanti presso tale gruppo.»;

2) l'allegato I è modificato conformemente all'allegato I della presente decisione;

3) l'allegato V è modificato conformemente all'allegato II della presente decisione;

4) il testo che figura nell'allegato III della presente decisione è aggiunto quale allegato VI;

5) il testo che figura nell'allegato IV della presente decisione è aggiunto quale allegato VII.

Articolo 2

La presente decisione entra in vigore il terzo giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

Essa si applica a decorrere da quattro settimane dopo l'entrata in vigore.

Fatto a Bruxelles, il 21 marzo 2022

Per la Commissione
La presidente
Ursula VON DER LEYEN

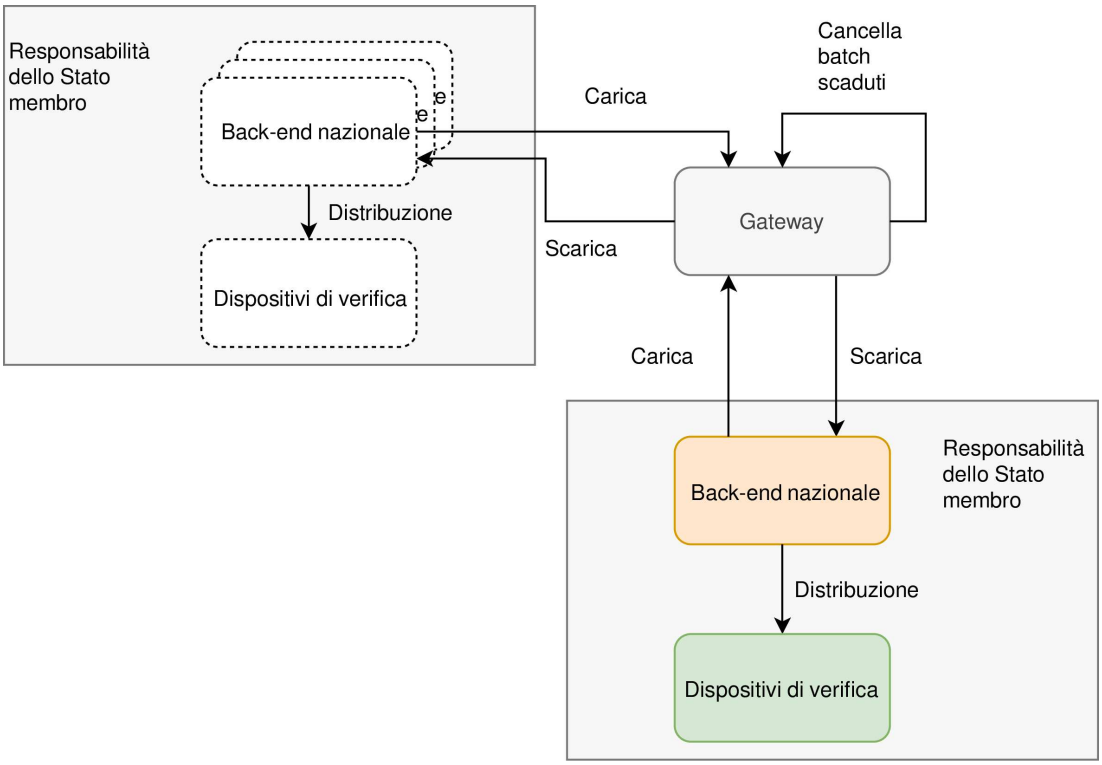
ALLEGATO I

Nell'allegato I della decisione di esecuzione (UE) 2021/1073 è aggiunta la seguente sezione 9:

«9. **SOLUZIONE DI REVOCA**

9.1. **Fornitura dell'elenco dei certificati COVID digitali revocati (DRL — *DCC Revocation List*)**

Il gateway fornisce le funzionalità e gli endpoint per conservare e gestire gli elenchi dei certificati revocati:



9.2. **Modello di fiducia**

Tutte le connessioni sono stabilite dal modello di fiducia standard del DCCG mediante i certificati NB_{TLS} e NB_{UP} (cfr. governance dei certificati). Tutte le informazioni sono suddivise in pacchetti e caricate mediante messaggi CMS per garantirne l'integrità.

9.3. **Costruzione dei batch (lotti)**

9.3.1. *Batch*

Ogni elenco dei certificati revocati contiene una o più voci ed è raggruppato in batch contenenti una serie di hash e i relativi metadati. Un batch è immutabile e definisce una data di scadenza che indica quando il batch può essere cancellato. La data di scadenza di tutti gli elementi del batch deve essere esattamente la stessa, il che significa che i batch devono essere raggruppati per data di scadenza e per DSC di firma. Ciascun batch contiene al massimo 1 000 voci. Se l'elenco dei certificati revocati comprende più di 1 000 voci, si creano più batch. Una voce può essere presente in al massimo un batch. Il batch è suddiviso in pacchetti in una struttura CMS e firmato dal certificato NB_{up} del paese che lo carica.

9.3.2. *Indice dei batch*

Al momento della sua creazione il batch è automaticamente aggiunto all'indice e il gateway gli attribuisce un ID unico. L'indice dei batch è ordinato in base alla data di modifica, in ordine cronologico ascendente.

9.3.3. *Comportamento del gateway*

Il gateway tratta i batch di revoca senza modificarli: non può aggiornare, né rimuovere, né aggiungere informazioni ai batch. I batch sono inoltrati a tutti i paesi autorizzati (cfr. capo 9.6).

Il gateway osserva attivamente le date di scadenza dei batch ed elimina i batch scaduti. Dopo la cancellazione del batch, il gateway invia una risposta «HTTP 410 Gone» per l'URL del batch cancellato. Pertanto il batch figura nell'indice dei batch come «deleted» («cancellato»).

9.4. **Tipi di hash**

L'elenco dei certificati revocati contiene hash che possono rappresentare diversi tipi/attributi di revoca. Tali tipi o attributi sono indicati al momento della fornitura degli elenchi dei certificati revocati. I tipi attuali sono:

Tipo	Attributo	Calcolo dell'hash
SIGNATURE	DCC Signature	SHA256 of DCC Signature
UCI	UCI (Unique Certificate Identifier)	SHA256 of UCI
COUNTRYCODEUCI	Issuing Country Code + UCI	SHA256 of Issuing CountryCode + UCI

Solo i primi 128 bit degli hash codificati come stringhe in base64 sono inseriti nei batch e utilizzati per identificare il DCC revocato ([1]).

9.4.1. *Tipo di hash: SHA256(DCC Signature)*

In questo caso l'hash è calcolato sui byte della firma COSE_SIGN1 dal CWT. Per le firme RSA l'intera firma sarà usata come input. La formula per i certificati firmati con EC-DSA utilizza il valore r come input:

SHA256(r)

[necessario per tutte le nuove implementazioni]

9.4.2. *Tipo di hash: SHA256(UCI)*

In questo caso l'hash è calcolato sulla stringa UCI codificata in UTF-8 e convertita in un array di byte.

[deprecato ([2]), ma supportato per motivi di retrocompatibilità]

9.4.3. *Tipo di hash: SHA256(Issuing CountryCode+UCI)*

In questo caso il CountryCode codificato come stringa UTF-8 è concatenato con l'UCI codificato con una stringa UTF-8. Esso è quindi convertito in array di byte e utilizzato come input della funzione di hash.

[deprecato[2], ma supportato per motivi di retrocompatibilità]

9.5. **Struttura API**

9.5.1. *API per la fornitura delle voci di revoca*

9.5.1.1. Finalità

Le voci dell'elenco dei certificati revocati sono fornite dall'API in batch comprendenti un indice dei batch.

9.5.1.2. Endpoint

([1]) Cfr. anche il punto 9.5.1.2 per le descrizioni dettagliate dell'API.
([2]) Deprecato significa che questa caratteristica non è presa in considerazione per le nuove implementazioni, ma è supportata per le quelle esistenti per un periodo di tempo ben definito.

9.5.1.2.1. Endpoint di scaricamento dell'elenco dei batch

Gli endpoint sono di semplice concezione e restituiscono un elenco di batch insieme a un piccolo wrapper che fornisce i metadati. I batch sono ordinati per data in ordine (cronologico) ascendente:

/revocation-list

Verb: GET

Content-Type: application/json

Response: JSON Array

```
{
    'more':true|false,
    'batches':
        [{
            'batchId': '{uuid}',
            'country': 'XY',
            'date': '2021-11-01T00:00:00Z'
            'deleted': true | false
        }, ..
        ]
}
```

Nota: Il risultato è limitato a 1 000 per impostazione predefinita. Se il flag «more» è impostato su «true», la risposta indica che sono disponibili più batch per lo scaricamento. Per scaricare più elementi, il client deve impostare nell'intestazione (header) If-Modified-Since una data non anteriore all'ultima voce ricevuta.

La risposta contiene un array JSON con la seguente struttura:

Campo	Definizione
more	Flag booleano che indica che vi sono più batch.
batches	Array con i batch esistenti.
batchId	https://en.wikipedia.org/wiki/Universally_unique_identifier
country	Codice paese ISO 3166
date	Data UTC ISO 8601. Data in cui il batch è stato aggiunto o cancellato.
deleted	booleano. «True» se cancellato. Quando viene impostato il flag «deleted», la voce può essere rimossa definitivamente dai risultati dell'interrogazione dopo 7 giorni.

9.5.1.2.1.1. Codici di risposta

Codice	Descrizione
200	Tutto ok.
204	Nessun contenuto, se il contenuto dell'intestazione «If-Modified-Since» non restituisce alcuna corrispondenza.

Intestazione della richiesta

Intestazione	Obbligatoria	Descrizione
If-Modified-Since	Sì	Questa intestazione contiene l'ultima data scaricata al fine di ottenere solo i risultati più recenti. Nella chiamata iniziale l'intestazione dovrebbe essere impostata su «2021-06-01 T00:00:00Z»

9.5.1.2.2. Endpoint di scaricamento dei batch

I batch contengono un elenco degli identificativi dei certificati:

/revocation-list/{batchId}

Verb: GET

Accepts: application/cms

Response:CMS with Content

{

'country': 'XY',

'expires': '2022-11-01T00:00:00Z',

'kid':'23S+33f=',

'hashType':'SIGNATURE',

'entries':[{

'hash':'e2e2e2e2e2e2e2e2'

}, ..]

}

La risposta contiene un CMS che comprende una firma che deve corrispondere al certificato NB_{UP} del paese. Tutti gli elementi nell'array JSON presentano la seguente struttura:

Campo	Obbligatorio	Tipo	Definizione
expires	Sì	String	Data in cui l'elemento può essere rimosso. Data/ora UTC ISO 8601
country	Sì	String	Codice paese ISO 3166
hashType	Sì	String	Tipo di hash delle voci fornite (cfr. Tipi di hash)
entries	Sì	JSON Object Array	Cfr. tabella Voci
kid	Sì	String	kid del DSC codificato in base64 utilizzato per firmare il DCC. Se il kid è sconosciuto è possibile utilizzare la stringa «UNKNOWN_KID» (escludendo le»).

Note:

— I batch sono raggruppati per data di scadenza e DSC: tutti gli elementi scadono contemporaneamente e sono stati firmati con la stessa chiave.

— Il termine di scadenza è espresso da data/ora UTC perché l'EU-DCC è un sistema globale e non devono esserci ambiguità temporali.

— La data di scadenza di un DCC revocato in via permanente è fissata alla data di scadenza del corrispondente DSC utilizzato per firmare il DCC o al Termine di scadenza del DCC revocato (nel qual caso si considera che gli orari indicati in NumericDate/epoch siano nel fuso orario UTC).

— Il back-end nazionale (NB) elimina gli elementi dall'elenco dei certificati revocati una volta raggiunta la data di **scadenza**.

— L'NB può rimuovere elementi dall'elenco dei certificati revocati nel caso in cui il **kid** usato per firmare il DCC sia revocato.

9.5.1.2.2.1. Voci

Campo	Obbligatorio	Tipo	Definizione
hash	Sì	String	Primi 128 bit dell'hash SHA256 codificati come stringa in base64

Nota: l'oggetto delle voci contiene attualmente solo un hash, ma per essere compatibile con le modifiche future è stato scelto un oggetto invece di un array json.

9.5.1.2.2.2. Codici di risposta

Codice	Descrizione
200	Tutto ok.
410	batch non più presente. Il batch può essere cancellato nel back-end nazionale.

9.5.1.2.2.3. Intestazioni della risposta

Intestazione	Descrizione
ETag	ID del batch

9.5.1.2.3. Endpoint di caricamento dei batch

Il caricamento è effettuato sullo stesso endpoint tramite una richiesta POST:

/revocation-list

Verb: POST

Accepts: application/cms

Request: CMS with Content

ContentType: application/cms

Content:

{

'country': 'XY',

'expires': '2022-11-01T00:00:00Z',

'kid':'23S+33f=',

'hashType':'SIGNATURE',

'entries':[{

'hash':'e2e2e2e2e2e2e2e2'

}, ..]

}

Il batch viene firmato utilizzando il certificato NB_{UP}. Il gateway verifica che la firma sia stata impostata dall'NB_{UP} per il *paese* in questione. Se il controllo della firma non dà esito positivo, il caricamento non va a buon fine.

NOTA: ogni batch è immutabile e non può essere modificato dopo il caricamento. Esso può tuttavia essere cancellato. Viene memorizzato l'ID di ogni batch cancellato e viene rifiutato il caricamento di un nuovo batch con lo stesso identificativo.

9.5.1.2.4. Endpoint di cancellazione dei batch

Un batch può essere cancellato sullo stesso endpoint tramite richiesta DELETE:

/revocation-list

Verb: DELETE

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

oppure, per motivi di compatibilità, al seguente endpoint con richiesta POST:

/revocation-list/delete

Verb: POST

Accepts: application/cms

ContentType: application/cms

Request: CMS with Content

Content:

{

'batchId': '...'

}

9.6. **Protezione API/GDPR**

La presente sezione specifica le misure di attuazione per conformarsi alle disposizioni del regolamento 2021/953 per quanto riguarda il trattamento dei dati personali.

9.6.1. *Autenticazione esistente*

Attualmente il gateway utilizza il certificato NB_{TLS} per autenticare i paesi collegati al gateway. Tale autenticazione può essere utilizzata per determinare l'identità del paese collegato al gateway. Tale identità può quindi essere utilizzata per implementare il controllo degli accessi.

9.6.2. *Controllo degli accessi*

Per poter trattare i dati personali lecitamente, il gateway implementa un meccanismo di controllo degli accessi.

Il gateway implementa un elenco di controllo degli accessi combinato con la sicurezza basata sui ruoli. Tale schema prevede il mantenimento di due tabelle: una tabella descrive quali Ruoli possono applicare quali Operazioni a quali Risorse, mentre un'altra tabella descrive quali Ruoli sono assegnati a quali Utenti.

Al fine di implementare i controlli richiesti dal presente documento, sono necessari tre Ruoli, ossia:

RevocationListReader

RevocationUploader

RevocationDeleter

I seguenti endpoint verificano se l'Utente (*User*) ha il Ruolo (*Role*) RevocationListReader; se sì, l'accesso viene concesso, in caso contrario viene restituita una risposta HTTP 403 Forbidden:

GET/revocation-list/

GET/revocation-list/{batchId}

I seguenti endpoint verificano se l'Utente ha il Ruolo RevocationUploader; se sì, l'accesso viene concesso, in caso contrario viene restituita una risposta HTTP 403 Forbidden:

POST/revocation-list

I seguenti endpoint verificano se l'Utente ha il Ruolo RevocationDeleter; se sì, l'accesso viene concesso, in caso contrario viene restituita una risposta HTTP 403 Forbidden:

DELETE/revocation-list

POST/revocation-list/delete

Il gateway fornisce inoltre un metodo affidabile mediante il quale gli amministratori possono gestire i Ruoli collegati agli Utenti in modo da ridurre la probabilità di errori umani senza gravare sugli amministratori funzionali.».

ALLEGATO II

La sezione 3 dell'allegato V della decisione di esecuzione 2021/1073 è sostituita dalla seguente:

«3. ***Strutture comuni e requisiti generali***

Un certificato COVID digitale dell'UE non può essere rilasciato se, a causa di informazioni mancanti, non è possibile compilare correttamente tutti i campi di dati conformemente alla presente specifica. **Ciò non va inteso in modo da pregiudicare l'obbligo degli Stati membri di rilasciare certificati COVID digitali dell'UE.**

In tutti i campi le informazioni possono essere fornite utilizzando l'insieme completo di caratteri UNICODE 13.0 codificati utilizzando l'UTF-8, a meno che i caratteri non siano specificamente limitati a serie di valori o a insiemi di caratteri più ristretti.

La struttura comune è la seguente:

"JSON":{

"ver":<informazioni sulla versione>,

"nam":{

<informazioni sul nome della persona>

},

"dob":<data di nascita>,

"v" o "t" o "r":[

{<informazioni sulla dose di vaccinazione, sul test o sulla guarigione, una voce>}

]

}

Nelle sezioni successive sono fornite informazioni dettagliate sui singoli gruppi e campi.

Se le regole indicano che un campo deve essere tralasciato, ciò significa che deve essere vuoto e che nel contenuto non sono ammessi né il nome né il valore del campo.

3.1. ***Versione***

Devono essere fornite informazioni sulla versione. Le versioni seguono il versionamento semantico ("Semantic Versioning" semver: https://semver.org). In fase di produzione la versione deve corrispondere a una delle versioni prodotte ufficialmente (attuale o precedenti). Per maggiori dettagli cfr. sezione relativa alla posizione dello schema JSON.

ID del campo	Nome del campo	Istruzioni
ver	Versione dello schema	Deve corrispondere all'identificativo della versione dello schema utilizzata per generare l'EUDCC. Esempio: "ver":"1.3.0"

3.2. ***Nome e data di nascita della persona***

Il nome della persona è il nome ufficiale completo, corrispondente al nome indicato nei documenti di viaggio. L'identificativo della struttura è *nam*. Deve essere indicato esattamente 1 (un) nome della persona.

ID del campo	Nome del campo	Istruzioni
nam/fn	Cognome/i	Cognome/i del titolare. Se il titolare non ha cognomi e ha un nome, il campo deve essere tralasciato. In tutti gli altri casi deve essere fornito esattamente 1 (un) campo non vuoto, che include tutti i cognomi. In caso di più cognomi, questi devono essere separati da uno spazio. I nomi composti che comprendono trattini o caratteri simili devono tuttavia rimanere invariati.

		Esempi: "fn":"Musterfrau-Gößinger" "fn":"Musterfrau-Gößinger Müller"
nam/fnt	Cognome/i standardizzato/i	Cognome/i del titolare traslitterato utilizzando la stessa convenzione utilizzata nei documenti di viaggio a lettura ottica del titolare (come le norme definite nel documento ICAO 9303, parte 3). Se il titolare non ha cognomi e ha un nome, il campo deve essere tralasciato. In tutti gli altri casi, deve essere fornito esattamente 1 (un) campo non vuoto, che include solo i caratteri A-Z e <. Lunghezza massima: 80 caratteri (come da specifica ICAO 9303). Esempi: "fnt":"MUSTERFRAU<GOESSINGER" "fnt":"MUSTERFRAU<GOESSINGER<MUELLER"
nam/gn	Nome/i	Nome/i del titolare. Se il titolare non ha nomi e ha un cognome, il campo deve essere tralasciato. In tutti gli altri casi, deve essere fornito esattamente 1 (un) campo non vuoto, che include tutti i nomi. In caso di più nomi, questi devono essere separati da uno spazio. Esempio: "gn":"Isolde Erika"
nam/gnt	Nome/i standardizzato/i	Nome/i del titolare traslitterato utilizzando la stessa convenzione utilizzata nei documenti di viaggio a lettura ottica del titolare (come le norme definite nel documento ICAO 9303, parte 3). Se il titolare non ha nomi e ha un cognome, il campo deve essere tralasciato. In tutti gli altri casi, deve essere fornito esattamente 1 (un) campo non vuoto, che include solo i caratteri A-Z e <. Lunghezza massima: 80 caratteri. Esempio: "gnt":"ISOLDE<ERIKA"
dob	Data di nascita	Data di nascita del titolare del DCC. Data completa o parziale senza ora, limitata all'intervallo da 1900-01-01 a 2099-12-31. Se la data di nascita completa o parziale è nota, deve essere fornito esattamente 1 (un) campo non vuoto. Se la data di nascita non è nota, neanche parzialmente, il campo deve contenere una stringa vuota "". Il contenuto del campo dovrebbe corrispondere alle informazioni riportate sui documenti di viaggio. Se sono disponibili informazioni sulla data di nascita, deve essere utilizzato uno dei seguenti formati ISO 8601. Altre opzioni non sono supportate. AAAA-MM-GG AAAA-MM AAAA (L'app di verifica può indicare le parti mancanti della data di nascita utilizzando la stessa convenzione XX utilizzata nei documenti di viaggio a lettura ottica, ad esempio 1990-XX-XX.) Esempi: "dob":"1979-04-14" "dob":"1901-08" "dob":"1939" "dob":""

3.3. ***Gruppi per informazioni specifiche relative al tipo di certificato***

Lo schema JSON supporta tre gruppi di voci comprendenti informazioni specifiche relative al tipo di certificato. Ciascun EUDCC deve contenere esattamente 1 (un) gruppo. Non sono ammessi gruppi vuoti.

Identificativo del gruppo	**Nome del gruppo**	**Voci**
v	Gruppo Vaccinazione	Se presente, deve contenere esattamente 1 (una) voce che descriva esattamente 1 (una) dose di vaccinazione (una dose).
t	Gruppo Test	Se presente, deve contenere esattamente 1 (una) voce che descriva esattamente 1 (un) risultato del test.
r	Gruppo Guarigione	Se presente, deve contenere esattamente 1 (una) voce che descriva 1 (una) dichiarazione di guarigione.».

ALLEGATO III

«ALLEGATO VI

RESPONSABILITÀ DEGLI STATI MEMBRI IN QUALITÀ DI CONTITOLARI DEL TRATTAMENTO PER IL GATEWAY PER I CERTIFICATI COVID DIGITALI DELL'UE AI FINI DELLO SCAMBIO DEGLI ELENCHI DEI CERTIFICATI COVID DIGITALI DELL'UE REVOCATI

SEZIONE 1

Sottosezione 1

Ripartizione delle responsabilità

1) I contitolari del trattamento trattano i dati personali tramite il gateway del quadro di fiducia conformemente alle specifiche tecniche di cui all'allegato I.

2) Le autorità di rilascio degli Stati membri sono gli unici titolari del trattamento responsabili della raccolta, dell'uso, della comunicazione e di qualsiasi altro trattamento delle informazioni sulla revoca al di fuori del gateway, anche per quanto riguarda la procedura che conduce alla revoca di un certificato.

3) Ogni titolare del trattamento è responsabile del trattamento dei dati personali nel gateway del quadro di fiducia conformemente agli articoli 5, 24 e 26 del regolamento generale sulla protezione dei dati.

4) Ogni titolare del trattamento istituisce un punto di contatto con una casella di posta elettronica funzionale da utilizzare per la comunicazione tra i contitolari del trattamento stessi e tra questi ultimi e il responsabile del trattamento.

5) Un gruppo di lavoro istituito dal comitato di cui all'articolo 14 del regolamento (UE) 2021/953 è incaricato di decidere in merito a eventuali problematiche derivanti dallo scambio degli elenchi dei certificati revocati nonché dalla contitolarità del relativo trattamento dei dati personali e di agevolare la fornitura di istruzioni coordinate alla Commissione in qualità di responsabile del trattamento. Il processo decisionale dei contitolari del trattamento è disciplinato da tale gruppo di lavoro e dal regolamento interno che esso è chiamato ad adottare. Come norma di base, la non partecipazione di qualsiasi contitolare del trattamento a una riunione del suddetto gruppo di lavoro, che sia stata annunciata per iscritto almeno sette (7) giorni prima della convocazione, è considerata quale tacito accordo con gli esiti di tale riunione del gruppo di lavoro. Qualsiasi contitolare del trattamento può convocare una riunione di tale gruppo di lavoro.

6) Le istruzioni al responsabile del trattamento sono inviate dai punti di contatto di qualsiasi contitolare del trattamento, d'intesa con gli altri contitolari del trattamento, come da processo decisionale del gruppo di lavoro di cui al precedente punto 5. Il contitolare del trattamento che fornisce le istruzioni dovrebbe trasmetterle al responsabile del trattamento per iscritto e informarne tutti gli altri contitolari del trattamento. Se la questione in esame è così urgente da non consentire una riunione del gruppo di lavoro di cui al precedente punto 5, è comunque possibile fornire istruzioni, ma esse possono essere revocate dal gruppo di lavoro. Tali istruzioni dovrebbero essere fornite per iscritto e tutti gli altri contitolari del trattamento dovrebbero esserne informati all'atto della fornitura delle istruzioni.

7) Il gruppo di lavoro istituito in base al precedente punto 5 non osta alla competenza individuale di qualsiasi contitolare del trattamento di informare la rispettiva autorità di controllo competente conformemente agli articoli 33 e 24 del regolamento generale sulla protezione dei dati. Tale notifica non richiede il consenso degli altri contitolari del trattamento.

8) Nell'ambito del gateway del quadro di fiducia solo le persone autorizzate dalle autorità nazionali o dagli organismi ufficiali designati possono accedere ai dati personali scambiati.

9) Ogni autorità di rilascio tiene, sotto la propria responsabilità, un registro delle attività di trattamento. La contitolarità del trattamento può essere indicata nel registro.

Sottosezione 2

Responsabilità e ruoli per la gestione delle richieste degli interessati e la loro informazione

1) Ogni titolare del trattamento, nel suo ruolo di autorità di rilascio, fornisce alle persone fisiche i cui certificati sono stati da esso revocati (gli «interessati») informazioni su tali revoche e sul trattamento dei loro dati personali nel gateway per i certificati COVID digitali dell'UE al fine di sostenere lo scambio degli elenchi dei certificati revocati, conformemente all'articolo 14 del regolamento generale sulla protezione dei dati, salvo che ciò non si riveli impossibile o implichi uno sforzo sproporzionato.

2) Ogni titolare del trattamento funge da punto di contatto per le persone fisiche i cui certificati sono stati da esso revocati e gestisce le richieste presentate dagli interessati o dai loro rappresentanti nell'esercizio dei loro diritti a norma del regolamento generale sulla protezione dei dati personali. Se un contitolare del trattamento riceve da un interessato una richiesta relativa a un certificato rilasciato da un altro contitolare del trattamento, esso informa l'interessato dell'identità e dei dati di contatto di tale contitolare del trattamento competente. Se richiesto da un altro contitolare del trattamento, i contitolari del trattamento si forniscono assistenza reciproca nella gestione delle richieste degli interessati e si rispondono reciprocamente senza indebito ritardo e al più tardi entro un mese dalla ricezione di una richiesta di assistenza. Se una richiesta riguarda dati presentati da un paese terzo, il titolare del trattamento che riceve la richiesta la gestisce e informa l'interessato dell'identità e dei dati di contatto dell'autorità di rilascio del paese terzo.

3) Ogni titolare del trattamento mette a disposizione degli interessati il contenuto del presente allegato, comprese le disposizioni di cui ai punti 1 e 2.

SEZIONE 2

Gestione degli incidenti di sicurezza, comprese le violazioni dei dati personali

1) I contitolari del trattamento si forniscono assistenza reciproca nell'identificazione e nella gestione di eventuali incidenti di sicurezza connessi al trattamento nel gateway per i certificati COVID digitali dell'UE, comprese le violazioni dei dati personali.

2) I contitolari del trattamento, in particolare, si informano reciprocamente:

   a) di eventuali rischi potenziali o effettivi per la disponibilità, la riservatezza e/o l'integrità dei dati personali oggetto di trattamento nel gateway del quadro di fiducia;

   b) di eventuali violazioni dei dati personali, delle probabili conseguenze delle violazioni dei dati personali e della valutazione del rischio per i diritti e le libertà delle persone fisiche, nonché delle misure adottate per porre rimedio alla violazione dei dati personali e per attenuare il rischio per i diritti e le libertà delle persone fisiche;

   c) di eventuali violazioni delle garanzie tecniche e/o organizzative del trattamento nel gateway del quadro di fiducia.

3) I contitolari del trattamento comunicano alla Commissione, alle competenti autorità di controllo e, ove prescritto, agli interessati, eventuali violazioni dei dati personali in relazione al trattamento nel gateway del quadro di fiducia in conformità agli articoli 33 e 34 del regolamento generale sulla protezione dei dati o a seguito della notifica da parte della Commissione.

4) Ogni autorità di rilascio applica adeguate misure tecniche e organizzative, intese a:

   a) garantire e proteggere la disponibilità, l'integrità e la riservatezza dei dati personali oggetto di trattamento congiunto;

   b) proteggere i dati personali in suo possesso da trattamenti, perdite, usi, comunicazioni, acquisizioni o accessi non autorizzati o illeciti;

   c) garantire che l'accesso ai dati personali non sia esteso o consentito a soggetti diversi dai destinatari o dai responsabili del trattamento.

SEZIONE 3

Valutazione d'impatto sulla protezione dei dati

1) Se un titolare del trattamento, per rispettare gli obblighi di cui agli articoli 35 e 36 del regolamento (UE) 2016/679, ha bisogno di informazioni da un altro titolare del trattamento, invia una richiesta specifica alla casella di posta elettronica funzionale di cui alla sezione 1, sottosezione 1, punto 4. Quest'ultimo titolare del trattamento si adopera al meglio per fornire tali informazioni.».

ALLEGATO IV

«*ALLEGATO VII*

RESPONSABILITÀ DELLA COMMISSIONE IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO DEI DATI PER IL GATEWAY PER I CERTIFICATI COVID DIGITALI DELL'UE A SOSTEGNO DELLO SCAMBIO DEGLI ELENCHI DEI CERTIFICATI COVID DIGITALI DELL'UE REVOCATI

La Commissione:

1) Istituisce, per conto degli Stati membri, un'infrastruttura di comunicazione sicura e affidabile che sostenga lo scambio degli elenchi dei certificati revocati presentati al gateway per i certificati COVID digitali dell'UE.

2) Per adempiere i propri obblighi in qualità di responsabile del trattamento dei dati del gateway del quadro di fiducia per gli Stati membri, la Commissione può ricorrere a terzi come sotto-responsabili del trattamento; la Commissione informa i contitolari del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri sotto-responsabili del trattamento, offrendo in tal modo ai titolari del trattamento l'opportunità di opporsi congiuntamente a tali modifiche. La Commissione si assicura che a detti sotto-responsabili si applichino gli stessi obblighi in materia di protezione dei dati di cui alla presente decisione.

3) Tratta i dati personali soltanto su istruzione documentata dei titolari del trattamento, a meno che il trattamento non sia richiesto dal diritto dell'Unione o dello Stato membro; in tal caso, la Commissione informa i contitolari del trattamento in merito a tale obbligo giuridico prima di svolgere l'attività di trattamento, a meno che il diritto vieti la fornitura di tale informazione per importanti motivi di interesse pubblico.

   Il trattamento della Commissione comprende i seguenti elementi:

   a) l'autenticazione dei server back-end nazionali, sulla base dei certificati dei server back-end nazionali;

   b) la ricezione dei dati di cui all'articolo 5 *bis*, paragrafo 3, della decisione caricati dai server back-end nazionali, mediante la fornitura di un'interfaccia di programmazione di un'applicazione (API) che consenta ai server back-end nazionali di caricare i dati pertinenti;

   c) la conservazione dei dati nel gateway per i certificati COVID digitali dell'UE;

   d) la messa a disposizione dei dati affinché i server back-end nazionali possano scaricarli;

   e) la cancellazione dei dati alla data di scadenza o dietro istruzione del titolare del trattamento che li ha presentati;

   f) la cancellazione di tutti i dati rimanenti dopo che è terminata la prestazione del servizio, salvo che il diritto dell'Unione o degli Stati membri preveda la conservazione dei dati personali.

4) Adotta tutte le misure di sicurezza fisiche, logiche e organizzative all'avanguardia per mantenere efficiente il gateway per i certificati COVID digitali dell'UE. A tal fine la Commissione:

   a) designa un responsabile per la gestione della sicurezza a livello del gateway per i certificati COVID digitali dell'UE, ne comunica i dati di contatto ai contitolari del trattamento e garantisce la sua disponibilità a reagire alle minacce alla sicurezza;

   b) si assume la responsabilità della sicurezza del gateway per i certificati COVID digitali dell'UE, anche effettuando periodicamente prove, valutazioni e analisi delle misure di sicurezza;

   c) si assicura che tutte le persone cui è consentito l'accesso al gateway per i certificati COVID digitali dell'UE siano assoggettate per contratto, professionalmente o per legge all'obbligo di riservatezza.

5) Adotta tutte le misure di sicurezza necessarie per evitare di compromettere il regolare funzionamento operativo dei server back-end nazionali. A tal fine la Commissione istituisce procedure specifiche relative alla connessione dai server back-end al gateway per i certificati COVID digitali dell'UE. Queste comprendono:

   a) una procedura di valutazione del rischio finalizzata a individuare e stimare potenziali minacce al sistema;

   b) una procedura di audit e revisione finalizzata a:

      i. verificare la corrispondenza tra le misure di sicurezza applicate e la politica di sicurezza applicabile;

      ii. controllare periodicamente l'integrità dei file di sistema, dei parametri di sicurezza e delle autorizzazioni concesse;

iii. effettuare controlli allo scopo di rilevare violazioni della sicurezza e intrusioni;

iv. apportare modifiche per ridurre le lacune esistenti in materia di sicurezza;

v. definire le condizioni alle quali autorizzare, anche su richiesta dei titolari del trattamento, audit indipendenti, comprese ispezioni, e revisioni delle misure di sicurezza e contribuire all'esecuzione di tali audit e revisioni, fatto salvo il rispetto il protocollo (n. 7) del TFUE sui privilegi e sulle immunità dell'Unione europea;

c) la modifica della procedura di controllo finalizzata a documentare e misurare l'impatto di una modifica prima della sua realizzazione e a tenere informati i contitolari del trattamento in merito a eventuali modifiche in grado di avere effetti sulla comunicazione con le loro infrastrutture e/o sulla sicurezza di queste ultime;

d) l'elaborazione di una procedura per la manutenzione e la riparazione finalizzata a specificare le norme e le condizioni da rispettare in caso di manutenzione e/o riparazione delle attrezzature;

e) l'elaborazione di una procedura per gli incidenti di sicurezza finalizzata a definire il sistema di segnalazione e successione, informare senza indugio i titolari del trattamento interessati, informare senza indugio i titolari del trattamento affinché possano notificare le autorità nazionali di controllo della protezione dei dati in merito a qualsiasi violazione dei dati personali, e definire un processo disciplinare per affrontare le violazioni della sicurezza.

6) Adotta misure di sicurezza fisiche e/o logiche all'avanguardia per le strutture che ospitano le attrezzature del gateway per i certificati COVID digitali dell'UE e per i controlli relativi all'accesso alla sicurezza e ai dati logici. A tal fine la Commissione:

a) garantisce il rispetto della sicurezza fisica per stabilire specifici perimetri di sicurezza e consentire l'individuazione di violazioni;

b) controlla l'accesso alle strutture e tiene un registro dei visitatori a fini di tracciabilità;

c) si assicura che le persone esterne a cui è consentito l'accesso ai locali siano scortate da personale debitamente autorizzato;

d) provvede affinché non possano essere aggiunte, sostituite o rimosse attrezzature senza la preventiva autorizzazione degli organismi responsabili designati;

e) controlla l'accesso ai server back-end nazionali e da questi al gateway del quadro di fiducia;

f) provvede affinché le persone che accedono al gateway per i certificati COVID digitali dell'UE siano identificate e la loro identità sia accertata;

g) riesamina i diritti di autorizzazione relativi all'accesso al gateway per i certificati COVID digitali dell'UE in caso di violazione della sicurezza riguardante tale infrastruttura;

h) salvaguarda l'integrità delle informazioni trasmesse attraverso il gateway per i certificati COVID digitali dell'UE;

i) applica misure tecniche e organizzative di sicurezza per impedire l'accesso non autorizzato ai dati personali;

j) applica, ove necessario, misure per bloccare l'accesso non autorizzato al gateway per i certificati COVID digitali dell'UE dal dominio delle autorità di rilascio (ossia blocco di un indirizzo IP/di localizzazione).

7) Adotta misure per proteggere il suo dominio, compresa l'interruzione delle connessioni, in caso di scostamento sostanziale rispetto ai principi e ai concetti in materia di qualità o di sicurezza.

8) Prevede un piano di gestione dei rischi in relazione al suo settore di competenza.

9) Monitora – in tempo reale – l'efficienza di tutte le componenti dei suoi servizi del gateway del quadro di fiducia, produce statistiche periodiche e conserva le informazioni.

10) Fornisce (24 ore su 24 e sette giorni alla settimana) supporto in inglese per tutti i servizi del gateway del quadro di fiducia tramite telefono, posta elettronica o portale web e accetta le chiamate dai chiamanti autorizzati: coordinatori del gateway per i certificati COVID digitali dell'UE e rispettivi helpdesk, responsabili di progetto e persone designate dalla Commissione.

11) Assiste i contitolari del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile a norma dell'articolo 12 del regolamento (UE) 2018/1725, al fine di soddisfare l'obbligo del titolare del trattamento di dare seguito alle richieste per l'esercizio dei diritti dell'interessato di cui al capo III del regolamento generale sulla protezione dei dati.

12) Assiste i contitolari del trattamento fornendo informazioni relative al gateway per i certificati COVID digitali dell'UE al fine di adempiere gli obblighi di cui agli articoli 32, 33, 34, 35 e 36 del regolamento generale sulla protezione dei dati.

13) Garantisce che i dati trattati all'interno del gateway per i certificati COVID digitali dell'UE siano incomprensibili a chiunque non sia autorizzato ad accedervi.

14) Adotta tutte le misure necessarie per evitare che gli operatori del gateway per i certificati COVID digitali dell'UE abbiano accesso non autorizzato ai dati trasmessi.

15) Adotta misure volte a facilitare l'interoperabilità e la comunicazione tra i titolari del trattamento designati del gateway per i certificati COVID digitali dell'UE.

16) Tiene un registro delle attività di trattamento svolte per conto dei contitolari del trattamento in conformità all'articolo 31, paragrafo 2, del regolamento (UE) 2018/1725.».