►**B**

DECISIONE DI ESECUZIONE (UE) 2019/1765 DELLA COMMISSIONE

del 22 ottobre 2019

che stabilisce le norme per l'istituzione, la gestione e il funzionamento della rete di autorità nazionali responsabili dell'assistenza sanitaria online e che abroga la decisione di esecuzione 2011/890/UE

[notificata con il numero C(2019) 7460]

(Testo rilevante ai fini del SEE)

(GU L 270 del 24.10.2019, pag. 83)

Modificata da:

		Gazzetta ufficiale		
		n.	pag.	data
►**M1**	Decisione di esecuzione (UE) 2020/1023 della Commissione del 15 luglio 2020	L 227 I	1	16.7.2020

▼B

DECISIONE DI ESECUZIONE (UE) 2019/1765 DELLA COMMISSIONE

del 22 ottobre 2019

che stabilisce le norme per l'istituzione, la gestione e il funzionamento della rete di autorità nazionali responsabili dell'assistenza sanitaria online e che abroga la decisione di esecuzione 2011/890/UE

[notificata con il numero C(2019) 7460]

(Testo rilevante ai fini del SEE)

Articolo 1

Oggetto

La presente decisione stabilisce le norme necessarie per l'istituzione, la gestione e il funzionamento della rete eHealth di autorità nazionali responsabili dell'assistenza sanitaria online prevista dall'articolo 14 della direttiva 2011/24/UE.

Articolo 2

Definizioni

1. Ai fini della presente decisione si applicano le seguenti definizioni:

a) «rete eHealth»: la rete volontaria che collega le autorità nazionali responsabili dell'assistenza sanitaria online designate dagli Stati membri e che persegue gli obiettivi di cui all'articolo 14 della direttiva 2011/24/UE;

b) «punti di contatto nazionali per l'eHealth»: i portali tecnici e organizzativi per la prestazione di servizi informativi transfrontalieri per l'assistenza sanitaria online sotto la responsabilità degli Stati membri;

c) «servizi informativi transfrontalieri per l'assistenza sanitaria online»: i servizi esistenti che sono trattati tramite i punti di contatto nazionali per l'eHealth e una piattaforma di servizi digitali chiave sviluppata dalla Commissione ai fini dell'assistenza sanitaria transfrontaliera;

d) «infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online»: l'infrastruttura che consente la prestazione di servizi informativi transfrontalieri per l'assistenza sanitaria online tramite i punti di contatto nazionali per l'eHealth e la piattaforma europea di servizi digitali chiave. Tale infrastruttura comprende sia i servizi generici, quali definiti all'articolo 2, paragrafo 2, lettera e), del regolamento (UE) n. 283/2014, sviluppati dagli Stati membri, sia una piattaforma di servizi digitali chiave, quale definita all'articolo 2, paragrafo 2, lettera d), dello stesso regolamento, sviluppata dalla Commissione;

e) «altri servizi europei di eHealth condivisi»: i servizi digitali che possono essere sviluppati nel quadro della rete eHealth e condivisi tra gli Stati membri;

▼B

f) «modello di governance»: una serie di norme relative alla designazione degli organismi che partecipano ai processi decisionali relativi all'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online o ad altri servizi europei di eHealth condivisi sviluppati nel quadro della rete eHealth, nonché la descrizione di tali processi;

▼M1

g) «utente dell'applicazione»: una persona in possesso di un dispositivo intelligente che ha scaricato e utilizza un'applicazione mobile di tracciamento dei contatti e di allerta approvata;

h) «tracciamento dei contatti»: le misure attuate al fine di tracciare le persone che sono state esposte a una fonte di una grave minaccia per la salute a carattere transfrontaliero ai sensi dell'articolo 3, lettera c), della decisione n. 1082/2013/UE del Parlamento europeo e del Consiglio ([1]);

i) «applicazione mobile nazionale di tracciamento dei contatti e di allerta»: un'applicazione software approvata a livello nazionale che funziona su dispositivi intelligenti, in particolare smartphone, di norma progettata per un'interazione ampia e mirata con risorse web, e che elabora dati di prossimità e altre informazioni contestuali raccolte da molti sensori presenti nei dispositivi intelligenti allo scopo di tracciare i contatti con le persone infette da SARS-CoV-2 e di allertare le persone che potrebbero essere state esposte a SARS-CoV-2; queste applicazioni mobili sono in grado di rilevare la presenza di altri dispositivi che utilizzano il Bluetooth e di scambiare informazioni con server back-end avvalendosi di Internet;

j) «gateway federativo»: un gateway di rete gestito dalla Commissione mediante uno strumento informatico sicuro che riceve, conserva e mette a disposizione un insieme minimo di dati personali tra i server back-end degli Stati membri allo scopo di garantire l'interoperabilità delle applicazioni mobili nazionali di tracciamento dei contatti e di allerta;

k) «chiave»: un identificativo temporaneo unico relativo a un utente dell'applicazione che segnala di essere stato contagiato da SARS-CoV-2 o che potrebbe essere stato esposto a SARS-CoV-2;

l) «verifica dell'infezione»: il metodo applicato per confermare un'infezione da SARS-CoV-2, che indica in particolare se l'infezione è stata segnalata dall'utente dell'applicazione o se risulta dalla conferma di un'autorità sanitaria nazionale o mediante test di laboratorio;

m) «paesi di interesse»: lo Stato membro o gli Stati membri in cui un utente dell'applicazione ha soggiornato durante i 14 giorni precedenti la data di caricamento delle chiavi e in cui ha scaricato l'applicazione mobile nazionale di tracciamento dei contatti e di allerta approvata e/o ha viaggiato;

([1]) Decisione n. 1082/2013/UE del Parlamento europeo e del Consiglio, del 22 ottobre 2013, relativa alle gravi minacce per la salute a carattere transfrontaliero e che abroga la decisione n. 2119/98/CE (GU L 293 del 5.11.2013, pag. 1).

▼M1

n) «paese di origine delle chiavi»: lo Stato membro in cui è situato il server back-end che ha caricato le chiavi nel gateway federativo;

o) «dati di log»: una registrazione automatica di un'attività in relazione allo scambio di dati trattati tramite il gateway federativo e all'accesso agli stessi, che indica in particolare il tipo di attività di trattamento, la data e l'ora dell'attività di trattamento e l'identificativo della persona che effettua il trattamento dei dati.

▼B

2. Le definizioni di cui ai punti 1), 2), 7) e 8) dell'articolo 4 del regolamento (UE) 2016/679 si applicano di conseguenza.

Articolo 3

Membri della rete eHealth

1. I membri della rete eHealth sono le autorità degli Stati membri responsabili dell'assistenza sanitaria online, designate dagli Stati membri che partecipano alla rete eHealth.

2. Gli Stati membri che intendono partecipare alla rete eHealth notificano per iscritto alla Commissione:

a) la decisione di partecipare alla rete eHealth;

b) l'autorità nazionale responsabile dell'assistenza sanitaria online che diventerà membro della rete eHealth, nonché il nome del rappresentante e quello del suo supplente.

3. I membri notificano per iscritto alla Commissione:

a) la loro decisione di recedere dalla rete eHealth;

b) qualsiasi modifica delle informazioni di cui al paragrafo 2, lettera b).

4. La Commissione mette a disposizione del pubblico l'elenco dei membri che partecipano alla rete eHealth.

Articolo 4

Attività della rete eHealth

1. Nel perseguire l'obiettivo di cui all'articolo 14, paragrafo 2, lettera a), della direttiva 2011/24/UE, la rete eHealth può, in particolare:

a) facilitare una maggiore interoperabilità dei sistemi nazionali delle tecnologie di informazione e di comunicazione e la trasferibilità transfrontaliera dei dati sanitari elettronici nell'assistenza sanitaria transfrontaliera;

b) fornire orientamenti agli Stati membri, in collaborazione con altre autorità di vigilanza competenti, per quanto riguarda la condivisione dei dati sanitari tra gli Stati membri e la possibilità per i cittadini di avere accesso ai propri dati sanitari e di condividerli;

▼B

c) fornire orientamenti agli Stati membri e facilitare lo scambio di buone pratiche in merito allo sviluppo di servizi sanitari digitali differenti, come la telemedicina, la sanità mobile o le nuove tecnologie nel settore dei megadati e dell'intelligenza artificiale, tenendo conto delle azioni in corso a livello dell'UE;

d) fornire orientamenti agli Stati membri per quanto riguarda il sostegno alla promozione della salute, alla prevenzione delle malattie e al miglioramento della prestazione dell'assistenza sanitaria grazie un uso migliore dei dati sanitari e l'accrescimento delle competenze digitali dei pazienti e degli operatori sanitari;

e) fornire orientamenti agli Stati membri e facilitare lo scambio volontario di migliori pratiche sugli investimenti in infrastrutture digitali;

f) fornire agli Stati membri, in collaborazione con altri organismi e soggetti interessati, orientamenti sui necessari casi d'uso per l'interoperabilità clinica e gli strumenti per realizzarla;

g) fornire ai membri orientamenti sulla sicurezza dell'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online o di altri servizi europei di eHealth condivisi sviluppati nel quadro della rete eHealth, tenendo conto della legislazione e dei documenti elaborati a livello dell'Unione, in particolare nel settore della sicurezza, nonché delle raccomandazioni nel settore della cibersicurezza, operando in stretta collaborazione con il gruppo di cooperazione in materia di sicurezza delle reti e dei sistemi informativi e con l'Agenzia dell'Unione europea per la cibersicurezza nonché con le autorità nazionali, se del caso;

▼M1

h) fornire orientamenti agli Stati membri sullo scambio transfrontaliero di dati personali tramite il gateway federativo tra applicazioni mobili nazionali di tracciamento dei contatti e di allerta.

▼B

2. Nell'elaborazione di orientamenti in merito a metodi efficaci per consentire l'uso di informazioni mediche per la sanità pubblica e la ricerca di cui all'articolo 14, paragrafo 2, lettera b), punto ii), della direttiva 2011/24/UE, la rete eHealth tiene conto degli orientamenti adottati dal comitato europeo per la protezione dei dati e, se del caso, lo consulta. Tali orientamenti possono anche riguardare le informazioni scambiate tramite l'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online o altri servizi europei di eHealth condivisi.

Articolo 5

Funzionamento della rete eHealth

1. La rete eHealth adotta il suo regolamento interno a maggioranza semplice dei suoi membri.

2. La rete eHealth adotta un programma di lavoro pluriennale e uno strumento di valutazione dell'attuazione dello stesso.

▼B

3. Per assolvere i suoi compiti la rete eHealth può costituire sottogruppi permanenti in relazione a compiti specifici, in particolare per quanto riguarda l'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online o gli altri servizi europei di eHealth condivisi sviluppati nel quadro della rete eHealth.

4. La rete eHealth può anche costituire sottogruppi temporanei, anche con esperti, per esaminare questioni specifiche sulla base di un mandato definito dalla stessa rete eHealth. Tali sottogruppi si sciolgono non appena espletato il loro mandato.

5. Allorché decidono di far progredire la loro collaborazione in alcuni settori che rientrano nei compiti della rete, i membri della rete eHealth dovrebbero concordare le regole della cooperazione avanzata e impegnarsi a rispettarle.

6. Nel perseguire i suoi obiettivi, la rete eHealth opera in stretta collaborazione con le azioni comuni che sostengono le attività della rete eHealth, ove tali azioni comuni esistono, con le parti interessate o altri organismi o meccanismi di sostegno interessati, e tiene conto dei risultati ottenuti nel quadro di tali attività.

7. La rete eHealth elabora, insieme alla Commissione, i modelli di governance dell'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online e partecipa a tale governance:

i) concordando le priorità dell'infrastruttura di servizi digitali di eHealth e controllandone il funzionamento;

ii) elaborando orientamenti e requisiti per il funzionamento, compresa la selezione delle norme utilizzate per l'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online;

iii) decidendo se i membri della rete eHealth debbano essere autorizzati ad avviare e proseguire lo scambio di dati sanitari elettronici attraverso l'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online, tramite i rispettivi punti di contatto nazionali per l'eHealth, sulla base della loro rispondenza ai requisiti stabiliti dalla rete eHealth valutata in base ai test eseguiti e agli audit condotti dalla Commissione;

iv) approvando il piano di lavoro annuale per l'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online.

8. La rete eHealth può elaborare, insieme alla Commissione, i modelli di governance di altri servizi europei di eHealth condivisi sviluppati nel quadro della rete eHealth e partecipare alla loro governance. La rete può inoltre stabilire le priorità, d'intesa con la Commissione, ed elaborare orientamenti per il funzionamento di tali servizi europei di eHealth condivisi.

▼B

9. Il regolamento interno può prevedere che altri paesi, diversi dagli Stati membri, che applicano la direttiva 2011/24/UE possano partecipare alle riunioni della rete eHealth in qualità di osservatori.

10. I membri della rete eHealth e i loro rappresentanti, nonché gli esperti e gli osservatori invitati, sono tenuti al rispetto degli obblighi del segreto professionale stabiliti dall'articolo 339 del trattato, nonché delle disposizioni della Commissione in materia di sicurezza riguardanti la protezione delle informazioni classificate UE, riportate nella decisione (UE, Euratom) 2015/444 della Commissione ([1]). In caso di mancato rispetto di tali obblighi il presidente della rete eHealth può adottare tutte le misure appropriate conformemente al regolamento interno.

Articolo 6

Relazione tra la rete eHealth e la Commissione

1. La Commissione:

a) partecipa alle riunioni della rete eHealth e le copresiede con il rappresentante dei membri;

b) collabora con la rete eHealth e le fornisce sostegno in relazione alle sue attività;

c) assicura i servizi di segreteria per la rete eHealth;

d) sviluppa, applica e mantiene misure tecniche e organizzative adeguate relative ai servizi chiave dell'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online;

e) sostiene la rete eHealth nella verifica della conformità tecnica e organizzativa dei punti di contatto nazionali per l'eHealth ai requisiti per lo scambio transfrontaliero di dati sanitari eseguendo i test e conducendo gli audit necessari. Esperti degli Stati membri possono assistere i controllori della Commissione;

▼M1

f) sviluppa, applica e mantiene misure tecniche e organizzative adeguate relative alla sicurezza della trasmissione e dell'hosting dei dati personali nel gateway federativo allo scopo di garantire l'interoperabilità delle applicazioni mobili nazionali di tracciamento dei contatti e di allerta;

g) sostiene la rete eHealth nella verifica della conformità tecnica e organizzativa delle autorità nazionali ai requisiti per lo scambio transfrontaliero di dati personali nel gateway federativo eseguendo i test e conducendo gli audit necessari. Esperti degli Stati membri possono assistere gli auditor della Commissione.

▼B

2. La Commissione può partecipare alle riunioni dei sottogruppi della rete eHealth.

3. La Commissione può consultare la rete eHealth su questioni relative all'assistenza sanitaria online a livello dell'Unione e allo scambio di migliori pratiche in materia di assistenza sanitaria online.

([1]) Decisione (UE, Euratom) 2015/444 della Commissione, del 13 marzo 2015, sulle norme di sicurezza per proteggere le informazioni classificate UE (GU L 72 del 17.3.2015, pag. 53).

▼B

4. La Commissione mette a disposizione del pubblico informazioni sulle attività svolte dalla rete eHealth.

Articolo 7

▼M1

Protezione dei dati personali trattati tramite l'infrastruttura di servizi digitali di eHealth

▼B

1. Gli Stati membri, rappresentati dalle competenti autorità nazionali o da altri organismi designati, sono considerati titolari del trattamento dei dati personali da essi elaborati tramite l'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online e attribuiscono in modo chiaro e trasparente le responsabilità tra i titolari del trattamento.

2. La Commissione è considerata responsabile del trattamento dei dati personali dei pazienti elaborati tramite l'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online. In qualità di responsabile del trattamento, la Commissione gestisce i servizi chiave dell'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online e rispetta gli obblighi in capo a un responsabile del trattamento di cui all' ►M1 allegato I ◄ della presente decisione. La Commissione non ha accesso ai dati personali dei pazienti trattati tramite l'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online.

3. La Commissione è considerata titolare del trattamento dei dati personali necessari per concedere e gestire i diritti di accesso ai servizi chiave dell'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online. Tali dati sono i recapiti degli utenti, compresi nome, cognome e indirizzo di posta elettronica, e la loro affiliazione.

▼M1

Articolo 7 bis

Scambio transfrontaliero di dati tramite il gateway federativo tra applicazioni mobili nazionali di tracciamento dei contatti e di allerta

1. Laddove sono scambiati dati personali tramite il gateway federativo, il trattamento è limitato alla finalità di facilitare l'interoperabilità delle applicazioni mobili nazionali di tracciamento dei contatti e di allerta all'interno del gateway federativo e la continuità del tracciamento dei contatti in un contesto transfrontaliero.

2. I dati personali di cui al paragrafo 3 sono trasmessi al gateway federativo in forma pseudonimizzata.

▼M1

3. I dati personali pseudonimizzati scambiati tramite il gateway federativo e trattati al suo interno comprendono soltanto le seguenti informazioni:

a) le chiavi trasmesse dalle applicazioni mobili nazionali di tracciamento dei contatti e di allerta fino a 14 giorni prima della data di caricamento delle chiavi;

b) i dati di log associati alle chiavi in linea con il protocollo di specifiche tecniche utilizzato nel paese di origine delle chiavi;

c) la verifica dell'infezione;

d) i paesi di interesse e il paese di origine delle chiavi.

4. Le autorità nazionali o gli organismi ufficiali designati che effettuano il trattamento dei dati personali nel gateway federativo sono contitolari del trattamento dei dati elaborati nel gateway federativo. Le rispettive responsabilità dei contitolari del trattamento sono attribuite in conformità dell'allegato II. Gli Stati membri che desiderano partecipare allo scambio transfrontaliero di dati tra applicazioni mobili nazionali di tracciamento dei contatti e di allerta notificano alla Commissione la propria intenzione prima di aderirvi, indicando l'autorità nazionale o l'organismo ufficiale che è stato designato come titolare del trattamento competente.

5. La Commissione è responsabile del trattamento dei dati personali elaborati all'interno del gateway federativo. In qualità di responsabile del trattamento, la Commissione garantisce la sicurezza del trattamento dei dati personali all'interno del gateway federativo, ivi compresi trasmissione e hosting, e rispetta gli obblighi incombenti al responsabile del trattamento di cui all'allegato III.

6. L'efficacia delle misure tecniche e organizzative volte a garantire la sicurezza del trattamento dei dati personali all'interno del gateway federativo è periodicamente verificata, esaminata e valutata dalla Commissione e dalle autorità nazionali autorizzate ad accedere al gateway federativo.

7. Fatta salva la decisione dei contitolari del trattamento di terminare il trattamento nel gateway federativo, il funzionamento del gateway federativo è disattivato al più tardi 14 giorni dopo che tutte le applicazioni mobili nazionali di tracciamento dei contatti e di allerta connesse hanno cessato di trasmettere chiavi tramite il gateway federativo.

▼B

Articolo 8

Spese

1. I partecipanti alle attività della rete eHealth non sono retribuiti dalla Commissione per i servizi resi.

▼B

2. Le spese di viaggio e di soggiorno sostenute dai partecipanti alle attività della rete eHealth sono rimborsate dalla Commissione conformemente alle disposizioni in vigore in seno alla Commissione in materia di rimborso delle spese sostenute da persone estranee alla Commissione invitate a partecipare a riunioni in veste di esperti. Tali spese sono rimborsate nei limiti degli stanziamenti disponibili assegnati nel quadro della procedura annuale di assegnazione delle risorse.

Articolo 9

Abrogazione

La decisione di esecuzione 2011/890/UE è abrogata. I riferimenti alla decisione abrogata si intendono fatti alla presente decisione.

Articolo 10

Destinatari

Gli Stati membri sono destinatari della presente decisione.

▼M1

ALLEGATO I

▼B

RESPONSABILITÀ DELLA COMMISSIONE IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO DEI DATI PER L'INFRASTRUTTURA DI SERVIZI DIGITALI DI EHEALTH PER I SERVIZI INFORMATIVI TRANSFRONTALIERI PER L'ASSISTENZA SANITARIA ONLINE

La Commissione:

1. Istituisce un'infrastruttura di comunicazione sicura e affidabile che interconnette le reti dei membri della rete eHealth che partecipano all'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online («infrastruttura di comunicazione sicura centrale») e ne assicura il funzionamento. Per adempiere ai suoi obblighi, la Commissione può ricorrere a terzi. La Commissione si assicura che a detti terzi si applichino gli stessi obblighi in materia di protezione dei dati di cui alla presente decisione.

2. Configura una parte dell'infrastruttura di comunicazione sicura centrale in modo che i punti di contatto nazionali per l'eHealth possano scambiarsi informazioni in maniera sicura, affidabile ed efficiente.

3. Tratta i dati personali su istruzione documentata dei titolari del trattamento.

4. Adotta tutte le misure di sicurezza fisiche, logiche e organizzative per mantenere efficiente l'infrastruttura di comunicazione sicura centrale. A tal fine la Commissione:

   a) designa un responsabile per la gestione della sicurezza a livello dell'infrastruttura di comunicazione sicura centrale, ne comunica i dati di contatto ai titolari del trattamento e garantisce la sua disponibilità a reagire alle minacce alla sicurezza;

   b) si assume la responsabilità della sicurezza dell'infrastruttura di comunicazione sicura centrale;

   c) si assicura che tutte le persone cui è consentito l'accesso all'infrastruttura di comunicazione sicura centrale siano assoggettati per contratto, professionalmente o per legge all'obbligo di riservatezza;

   d) si assicura che il personale che ha accesso alle informazioni classificate soddisfi i relativi criteri in materia di nulla osta e riservatezza.

5. Adotta tutte le misure di sicurezza necessarie per evitare di compromettere il regolare funzionamento operativo del dominio dell'altro. A tal fine la Commissione istituisce le procedure specifiche relative alla connessione all'infrastruttura di comunicazione sicura centrale. Tali informazioni 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 attuata;

      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 colmare le lacune esistenti in materia di sicurezza;

▼B

v) definire le condizioni alle quali autorizzare, anche su richiesta dei titolari del trattamento, audit indipendenti, comprese ispezioni, e contribuire all'esecuzione di tali audit e di revisioni delle misure di sicurezza;

c) una procedura di controllo delle modifiche finalizzata a documentare e misurare l'impatto di una modifica prima della sua realizzazione e a tenere informati i punti di contatto nazionali per l'eHealth in merito a eventuali modifiche in grado di avere effetti sulla comunicazione con le altre infrastrutture nazionali e/o sulla sicurezza di queste;

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

e) una procedura per gli incidenti alla sicurezza finalizzata a definire il sistema di segnalazione e successione, informare senza indugio l'amministrazione nazionale responsabile e il garante europeo della protezione dei dati in merito a qualsiasi violazione della sicurezza e definire un processo disciplinare per affrontare le violazioni della sicurezza.

6. Adotta misure di sicurezza fisiche e/o logiche per le strutture che ospitano le attrezzature per l'infrastruttura di comunicazione sicura centrale e 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 della rispettiva organizzazione;

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

e) controlla l'accesso da e verso un'altra rete o altre reti interconnesse con l'infrastruttura di comunicazione sicura centrale;

f) provvede affinché le persone che accedono all'infrastruttura di comunicazione sicura centrale siano identificate e la loro identità sia accertata;

g) riesamina i diritti di autorizzazione relativi all'accesso all'infrastruttura di comunicazione sicura centrale in caso di violazione della sicurezza riguardante tale infrastruttura;

h) salvaguarda l'integrità delle informazioni trasmesse attraverso l'infrastruttura di comunicazione sicura centrale;

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 all'infrastruttura di comunicazione sicura centrale dal dominio dei punti di contatto nazionali per l'eHealth (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.

▼B

9. Monitora — in tempo reale — l'efficienza di tutte le componenti dei suoi servizi dell'infrastruttura di comunicazione sicura centrale, 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 dell'infrastruttura di comunicazione sicura centrale tramite telefono, posta elettronica o portale web e accetta le chiamate dai chiamanti autorizzati: coordinatori dell'infrastruttura di comunicazione sicura centrale e rispettivi helpdesk, responsabili di progetto e persone designate dalla Commissione.

11. Assiste i titolari del trattamento fornendo informazioni relative all'infrastruttura di comunicazione sicura centrale dell'infrastruttura di servizi digitali di eHealth per i servizi informativi transfrontalieri per l'assistenza sanitaria online, ai fini dell'adempimento degli obblighi di cui agli articoli 35 e 36 del regolamento (UE) 2016/679.

12. Si assicura che i dati trasportati all'interno dell'infrastruttura di comunicazione sicura centrale siano criptati.

13. Adotta tutte le misure necessarie per evitare che gli operatori dell'infrastruttura di comunicazione sicura centrale abbiano accesso non autorizzato ai dati trasportati.

14. Adotta misure volte a facilitare l'interoperabilità e la comunicazione tra le amministrazioni nazionali competenti designate dell'infrastruttura di comunicazione sicura centrale.

▼M1

ALLEGATO II

RESPONSABILITÀ DEGLI STATI MEMBRI PARTECIPANTI IN QUALITÀ DI CONTITOLARI DEL TRATTAMENTO PER IL GATEWAY FEDERATIVO PER IL TRATTAMENTO TRANSFRONTALIERO TRA APPLICAZIONI MOBILI NAZIONALI DI TRACCIAMENTO DEI CONTATTI E DI ALLERTA

SEZIONE 1

Sottosezione 1

Ripartizione delle responsabilità

1. I contitolari del trattamento trattano i dati personali tramite il gateway federativo conformemente alle specifiche tecniche stabilite dalla rete eHealth ([1]).

2. Ogni titolare del trattamento è competente per il trattamento dei dati personali nel gateway federativo conformemente al regolamento generale sulla protezione dei dati e alla direttiva 2002/58/CE.

3. 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 e tra questi ultimi e il responsabile del trattamento.

(4) Un sottogruppo temporaneo costituito dalla rete eHealth in conformità all'articolo 5, paragrafo 4, è incaricato di esaminare eventuali problematiche derivanti dall'interoperabilità delle applicazioni mobili nazionali di tracciamento dei contatti e di allerta 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. Nell'ambito del sottogruppo temporaneo i titolari del trattamento possono, tra l'altro, lavorare a un approccio comune in materia di conservazione dei dati nei loro server back-end nazionali, tenendo conto del periodo di conservazione stabilito per il gateway federativo.

(5) Le istruzioni al responsabile del trattamento sono inviate da qualsiasi punto di contatto dei contitolari del trattamento, d'intesa con gli altri contitolari del trattamento nel sottogruppo summenzionato.

(6) Solo le persone autorizzate dalle autorità nazionali o dagli organismi ufficiali designati possono accedere ai dati personali degli utenti scambiati nel gateway federativo.

(7) Ogni autorità nazionale o organismo ufficiale designato cessa di essere contitolare del trattamento dalla data del ritiro della sua partecipazione al gateway federativo. Rimane tuttavia competente per i trattamenti effettuati nel gateway federativo prima del suo ritiro.

Sottosezione 2

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

1. Ogni titolare del trattamento fornisce agli utenti della sua applicazione mobile nazionale di tracciamento dei contatti e di allerta («gli interessati») informazioni relative al trattamento dei loro dati personali nel gateway

([1]) In particolare le specifiche di interoperabilità per le catene di trasmissione transfrontaliere tra app approvate del 16 giugno 2020, disponibili alla pagina: https://ec.europa.eu/health/ehealth/key_documents_it#anchor0.

▼M1

federativo ai fini dell'interoperabilità transfrontaliera delle applicazioni mobili nazionali di tracciamento dei contatti e di allerta, a norma degli articoli 13 e14 del regolamento generale sulla protezione dei dati.

2. Ogni titolare del trattamento funge da punto di contatto per gli utenti della sua applicazione mobile nazionale di tracciamento dei contatti e di allerta e gestisce le richieste, presentate da tali utenti o dai loro rappresentanti, relative all'esercizio dei diritti degli interessati a norma del regolamento generale sulla protezione dei dati. Ogni titolare del trattamento designa uno specifico punto di contatto dedicato alle richieste ricevute dagli interessati. Se un contitolare del trattamento riceve da un interessato una richiesta che non rientra sotto la sua responsabilità, la inoltra prontamente al contitolare del trattamento competente. Se richiesto, 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 15 giorni dalla ricezione di una richiesta di assistenza.

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 alla sicurezza, comprese le violazioni dei dati personali

(1) I contitolari del trattamento si forniscono assistenza reciproca nell'identificazione e nella gestione di eventuali incidenti alla sicurezza connessi al trattamento nel gateway federativo, 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 federativo;

b) di eventuali incidenti alla sicurezza connessi al trattamento nel gateway federativo;

c) 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;

d) di eventuali violazioni delle garanzie tecniche e/o organizzative del trattamento nel gateway federativo.

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 federativo in conformità agli articoli 33 e 34 del regolamento (UE) 2016/679 o a seguito della notifica da parte della Commissione.

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 generale sulla protezione dei dati, 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 3. Quest'ultimo titolare del trattamento si adopera al meglio per fornire tali informazioni

▼M1

ALLEGATO III

RESPONSABILITÀ DELLA COMMISSIONE IN QUALITÀ DI RESPONSABILE DEL TRATTAMENTO DEI DATI PER IL GATEWAY FEDERATIVO PER IL TRATTAMENTO TRANSFRONTALIERO TRA APPLICAZIONI MOBILI NAZIONALI DI TRACCIAMENTO DEI CONTATTI E DI ALLERTA

La Commissione:

(1) Istituisce un'infrastruttura di comunicazione sicura e affidabile che interconnette le applicazioni mobili nazionali di tracciamento dei contatti e di allerta degli Stati membri che partecipano al gateway federativo e ne assicura il funzionamento. Per adempiere i propri obblighi in qualità di responsabile del trattamento dei dati del gateway federativo, la Commissione può ricorrere a terzi come sub-responsabili del trattamento; la Commissione informa i contitolari del trattamento di eventuali modifiche previste riguardanti l'aggiunta o la sostituzione di altri sub-responsabili del trattamento, offrendo in tal modo ai titolari del trattamento l'opportunità di opporsi congiuntamente a tali modifiche, come stabilito all'allegato II, sezione 1, sottosezione 1, punto 4. La Commissione si assicura che a detti sub-responsabili si applichino gli stessi obblighi in materia di protezione dei dati di cui alla presente decisione.

(2) Tratta i dati personali soltanto su istruzione documentata dei titolari del trattamento, salvo che lo richieda il diritto dell'Unione o dello Stato membro; in tal caso, la Commissione informa i titolari del trattamento in merito a tale obbligo giuridico prima del trattamento, a meno che il diritto vieti la fornitura di tale informazione per importanti motivi di interesse pubblico.

(3) Effettua il trattamento, che 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 7 *bis*, paragrafo 3, della decisione di esecuzione caricati dai server back-end nazionali, mediante la fornitura di un'interfaccia di programmazione di un'applicazione che consenta ai server back-end nazionali di caricare i dati pertinenti;

c) la conservazione dei dati nel gateway federativo, dopo averli ricevuti dai server back-end nazionali;

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

e) la cancellazione dei dati una volta che tutti i server back-end partecipanti li hanno scaricati o al più tardi 14 giorni dopo la loro ricezione;

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.

Il responsabile del trattamento adotta le misure necessarie a preservare l'integrità dei dati trattati.

(4) Adotta tutte le misure di sicurezza fisiche, logiche e organizzative all'avanguardia per mantenere efficiente il gateway federativo. A tal fine la Commissione:

▼M1

a) designa un responsabile per la gestione della sicurezza a livello del gateway federativo, ne comunica i dati di contatto ai titolari del trattamento e garantisce la sua disponibilità a reagire alle minacce alla sicurezza;

b) si assume la responsabilità della sicurezza del gateway federativo;

c) si assicura che tutte le persone cui è consentito l'accesso al gateway federativo 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 le procedure specifiche relative alla connessione dai server back-end al gateway federativo. 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) consentire, anche su richiesta dei titolari del trattamento, l'esecuzione di audit indipendenti, comprese ispezioni, e di revisioni delle misure di sicurezza, e contribuirvi, a condizioni che rispettino il protocollo (n. 7) del TFUE sui privilegi e sulle immunità dell'Unione europea ([1]);

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 titolari 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 alla sicurezza finalizzata a definire il sistema di segnalazione e successione, informare senza indugio i titolari del trattamento e il garante europeo 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 federativo e per i controlli relativi all'accesso alla sicurezza e ai dati logici. A tal fine la Commissione:

([1]) Protocollo (n. 7) sui privilegi e sulle immunità dell'Unione europea (GU C 326 del 26.10.2012, pag. 266).

▼**M1**

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 federativo;

f) provvede affinché le persone che accedono al gateway federativo siano identificate e la loro identità sia accertata;

g) riesamina i diritti di autorizzazione relativi all'accesso al gateway federativo in caso di violazione della sicurezza riguardante tale infrastruttura;

h) salvaguarda l'integrità delle informazioni trasmesse attraverso il gateway federativo;

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 federativo dal dominio delle autorità nazionali (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 federativo, 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 federativo tramite telefono, posta elettronica o portale web e accetta le chiamate dai chiamanti autorizzati: coordinatori del gateway federativo e rispettivi helpdesk, responsabili di progetto e persone designate dalla Commissione.

(11) Assiste i titolari del trattamento con misure tecniche e organizzative adeguate, nella misura in cui ciò sia possibile, 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.

▼**M1**

(12) Assiste i titolari del trattamento fornendo informazioni relative al gateway federativo, ai fini dell'adempimento degli obblighi di cui agli articoli 32, 35 e 36 del regolamento generale sulla protezione dei dati.

(13) Garantisce che i dati trattati all'interno del gateway federativo siano incomprensibili a chiunque non sia autorizzato ad accedere a quest'ultimo.

(14) Adotta tutte le misure necessarie per evitare che gli operatori del gateway federativo abbiano accesso non autorizzato ai dati trasmessi.

(15) Adotta misure volte a facilitare l'interoperabilità e la comunicazione tra i titolari del trattamento del gateway federativo designati.

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