II

(Atti non legislativi)

DECISIONI

DECISIONE DI ESECUZIONE (UE) 2020/1023 DELLA COMMISSIONE

del 15 luglio 2020

che modifica la decisione di esecuzione (UE) 2019/1765 per quanto riguarda lo scambio transfrontaliero di dati tra applicazioni mobili nazionali di tracciamento dei contatti e di allerta nell'ambito della lotta alla pandemia di COVID-19

(Testo rilevante ai fini del SEE)

LA COMMISSIONE EUROPEA,

visto il trattato sul funzionamento dell'Unione europea,

vista la direttiva 2011/24/UE del Parlamento europeo e del Consiglio, del 9 marzo 2011, concernente l'applicazione dei diritti dei pazienti relativi all'assistenza sanitaria transfrontaliera ([1]), in particolare l'articolo 14, paragrafo 3,

considerando quanto segue:

(1) L'articolo 14 della direttiva 2011/24/UE attribuisce all'Unione il compito di sostenere e facilitare la cooperazione e lo scambio di informazioni tra gli Stati membri operanti nell'ambito di una rete volontaria che collega le autorità nazionali responsabili dell'assistenza sanitaria online designate dagli Stati membri (la «rete eHealth»).

(2) La decisione di esecuzione (UE) 2019/1765 della Commissione ([2]) stabilisce le norme per l'istituzione, la gestione e il funzionamento della rete di autorità nazionali responsabili dell'assistenza sanitaria online. L'articolo 4 della decisione conferisce alla rete eHealth il compito di 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.

(3) A seguito della crisi sanitaria pubblica causata dalla pandemia di COVID-19, diversi Stati membri hanno sviluppato applicazioni mobili che sostengono il tracciamento dei contatti e permettono di allertare gli utenti affinché adottino misure adeguate, quali l'esecuzione di test o l'autoisolamento, qualora siano stati potenzialmente esposti al virus a causa della prossimità con un altro utente di tali applicazioni che è risultato positivo. Queste applicazioni si avvalgono della tecnologia Bluetooth per rilevare la prossimità tra i dispositivi. Con la revoca delle restrizioni ai viaggi tra gli Stati membri a partire da giugno 2020, è opportuno migliorare l'interoperabilità dei sistemi nazionali delle tecnologie di informazione e di comunicazione tra gli Stati membri partecipanti alla rete eHealth, attuando un'infrastruttura digitale che renda possibile l'interoperabilità tra le applicazioni mobili nazionali a sostegno delle attività di tracciamento dei contatti e di allerta.

([1]) GU L 88 del 4.4.2011, pag. 45.

([2]) 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 (GU L 270 del 24.10.2019, pag. 83).

(4) La Commissione sostiene gli Stati membri in relazione alle applicazioni mobili summenzionate. L'8 aprile 2020 la Commissione ha adottato una raccomandazione relativa a un pacchetto di strumenti comuni dell'Unione per l'uso della tecnologia e dei dati al fine di contrastare la crisi COVID-19 e uscirne, in particolare per quanto riguarda le applicazioni mobili e l'uso di dati anonimizzati sulla mobilità (la «raccomandazione della Commissione») ([3]). Gli Stati membri che partecipano alla rete eHealth hanno adottato, con il supporto della Commissione, un pacchetto di strumenti comuni dell'UE per gli Stati membri sulle applicazioni mobili a sostegno del tracciamento dei contatti ([4]), nonché orientamenti sull'interoperabilità per le applicazioni mobili di tracciamento dei contatti autorizzate nell'UE ([5]). Il pacchetto di strumenti illustra i requisiti nazionali per le applicazioni mobili nazionali di tracciamento dei contatti e di allerta, che in particolare dovrebbero essere utilizzate su base volontaria, essere approvate dalle rispettive autorità sanitarie nazionali, tutelare la vita privata ed essere prontamente rimosse quando non più necessarie. A seguito degli sviluppi più recenti della crisi COVID-19, la Commissione ([6]) e il comitato europeo per la protezione dei dati (EDPB) ([7]) hanno entrambi pubblicato orientamenti sulle applicazioni mobili e sugli strumenti di tracciamento dei contatti relativamente alla protezione dei dati. La progettazione delle applicazioni mobili degli Stati membri e dell'infrastruttura digitale che ne consente l'interoperabilità si basa sul pacchetto di strumenti comuni dell'UE, sugli orientamenti summenzionati e sulle specifiche tecniche concordate nell'ambito della rete eHealth.

(5) Al fine di facilitare l'interoperabilità delle applicazioni mobili nazionali di tracciamento dei contatti e di allerta, gli Stati membri partecipanti alla rete eHealth che hanno deciso di far progredire la loro collaborazione in questo settore su base volontaria hanno sviluppato, con il sostegno della Commissione, un'infrastruttura digitale quale strumento informatico per lo scambio di dati. Tale infrastruttura digitale è denominata «gateway federativo».

(6) La presente decisione stabilisce disposizioni relative al ruolo degli Stati membri partecipanti e della Commissione per il funzionamento del gateway federativo ai fini dell'interoperabilità transfrontaliera delle applicazioni mobili nazionali di tracciamento dei contatti e di allerta.

(7) Il trattamento dei dati personali degli utenti delle applicazioni mobili di tracciamento dei contatti e di allerta, effettuato sotto la responsabilità degli Stati membri o di altre organizzazioni o organismi ufficiali pubblici degli Stati membri, dovrebbe essere realizzato conformemente al regolamento (UE) 2016/679 del Parlamento europeo e del Consiglio ([8]) («il regolamento generale sulla protezione dei dati») e alla direttiva 2002/58/CE del Parlamento europeo e del Consiglio ([9]). Il trattamento dei dati personali effettuato sotto la responsabilità della Commissione allo scopo di gestire e garantire la sicurezza del gateway federativo dovrebbe ottemperare alle disposizioni del regolamento (UE) 2018/1725 del Parlamento europeo e del Consiglio ([10]).

(8) Il gateway federativo dovrebbe consistere in un'infrastruttura informatica sicura che fornisca un'interfaccia comune in cui le autorità nazionali o gli organismi ufficiali designati possano scambiare un insieme minimo di dati in riferimento ai contatti con persone infette da SARS-CoV-2, al fine di informare altri soggetti della potenziale esposizione all'infezione, e che promuova una cooperazione efficace nel campo dell'assistenza sanitaria tra gli Stati membri facilitando lo scambio di informazioni rilevanti.

(9) La presente decisione dovrebbe pertanto stabilire le modalità per lo scambio transfrontaliero di dati tramite il gateway federativo all'interno dell'UE tra le autorità nazionali o gli organismi ufficiali designati.

([3]) Raccomandazione (UE) 2020/518 della Commissione, dell'8 aprile 2020, relativa a un pacchetto di strumenti comuni dell'Unione per l'uso della tecnologia e dei dati al fine di contrastare la crisi Covid-19 e uscirne, in particolare per quanto riguarda le applicazioni mobili e l'uso di dati anonimizzati sulla mobilità (GU L 114 del 14.4.2020, pag. 7).

([4]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/covid-19_apps_en.pdf.

([5]) https://ec.europa.eu/health/sites/health/files/ehealth/docs/contacttracing_mobileapps_guidelines_en.pdf.

([6]) Comunicazione della Commissione - Orientamenti sulle app a sostegno della lotta alla pandemia di Covid-19 relativamente alla protezione dei dati (GU C 124I del 17.4.2020, pag. 1).

([7]) Linee-guida 04/2020 sull'uso dei dati di localizzazione e degli strumenti per il tracciamento dei contatti nel contesto dell'emergenza legata al COVID-19 e dichiarazione del 16 giugno 2020 relativa all'impatto sulla protezione dei dati derivante dall'interoperabilità delle applicazioni di tracciamento dei contatti; entrambi i documenti sono reperibili alla pagina: https://edpb.europa.eu/edpb_it.

([8]) 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).

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

([10]) 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).

(10) Gli Stati membri partecipanti, rappresentati dalle autorità nazionali o dagli organismi ufficiali designati, determinano congiuntamente le finalità e i mezzi del trattamento dei dati personali tramite il gateway federativo e sono pertanto contitolari del trattamento. L'articolo 26 del regolamento generale sulla protezione dei dati 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. Ciascun titolare del trattamento dovrebbe assicurarsi di disporre di una base giuridica a livello nazionale per il trattamento nel gateway federativo.

(11) La Commissione, in quanto fornitrice di soluzioni tecniche e organizzative per il gateway federativo, procede al trattamento dei dati personali pseudonimizzati per conto degli Stati membri partecipanti al gateway federativo quali contitolari del trattamento ed è pertanto responsabile del trattamento. A norma dell'articolo 28 del regolamento generale sulla protezione dei dati e dell'articolo 29 del regolamento (UE) 2018/1725, i trattamenti da parte di un responsabile del trattamento sono disciplinati da un contratto o da un atto giuridico a norma del diritto dell'Unione o degli Stati membri che vincola il responsabile del trattamento al titolare del trattamento e che specifica i trattamenti. La presente decisione stabilisce norme relative ai trattamenti da parte della Commissione in qualità di responsabile del trattamento.

(12) Nell'effettuare il trattamento dei dati personali nel quadro del gateway federativo, la Commissione è vincolata dalla sua decisione (UE, Euratom) 2017/46 della Commissione ([11]).

(13) Considerando che le finalità per cui i titolari del trattamento trattano i dati personali nelle applicazioni mobili nazionali di tracciamento dei contatti e di allerta non richiedono necessariamente l'identificazione dell'interessato, i titolari del trattamento possono non essere sempre in grado di garantire l'applicazione dei diritti degli interessati. I diritti di cui agli articoli da 15 a 20 del regolamento generale sulla protezione dei dati possono pertanto non applicarsi quando sono soddisfatte le condizioni di cui all'articolo 11 di tale regolamento.

(14) A seguito dell'aggiunta di due nuovi allegati occorre numerare l'allegato attuale della decisione di esecuzione (UE) 2019/1765.

(15) È pertanto opportuno modificare di conseguenza la decisione di esecuzione (UE) 2019/1765.

(16) Tenuto conto della situazione di emergenza causata dalla pandemia di COVID-19, è opportuno che la presente decisione si applichi a decorrere dal giorno successivo alla pubblicazione nella *Gazzetta ufficiale dell'Unione europea*.

(17) Il Garante europeo della protezione dei dati è stato consultato a norma dell'articolo 42, paragrafo 1, del regolamento (UE) 2018/1725 e ha espresso un parere il 9 luglio 2020.

(18) Le misure di cui alla presente decisione sono conformi al parere del comitato istituito a norma dell'articolo 16 della direttiva 2011/24/UE,

HA ADOTTATO LA PRESENTE DECISIONE:

Articolo 1

La decisione di esecuzione (UE) 2019/1765 è così modificata:

1) all'articolo 2, paragrafo 1, sono aggiunte le seguenti lettere g), h), i), j), k), l), m), n) e o):

«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 (*);

([11]) Decisione (UE, Euratom) 2017/46 della Commissione, del 10 gennaio 2017, sulla sicurezza dei sistemi di comunicazione e informazione della Commissione europea (GU L 6 dell'11.1.2017, pag. 40). 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.

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;

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.»;

(*) 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).

2) all'articolo 4, paragrafo 1, è aggiunta la seguente lettera h):

«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.»;

3) all'articolo 6, paragrafo 1, sono aggiunte le seguenti lettere f) e g):

«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.»;

4) l'articolo 7 è così modificato:

a) il titolo è sostituito da «Protezione dei dati personali trattati tramite l'infrastruttura di servizi digitali di eHealth»;

b) al paragrafo 2, il termine «allegato» è sostituito dal termine «allegato I»;

5) è inserito il seguente articolo 7 *bis*:

«*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.

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.»;

6) l'allegato diventa l'allegato I;

7) sono aggiunti gli allegati II e III, il cui testo figura nell'allegato della presente decisione.

Articolo 2

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

Fatto a Bruxelles, il 15 luglio 2020

Per la Commissione
La presidente
Ursula VON DER LEYEN

ALLEGATO

Nella decisione di esecuzione (UE) 2019/1765 sono aggiunti i seguenti allegati II e III:

«*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 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.

([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.

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

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:

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 ([2]);

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

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:

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.

(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.»