Traduzione

0.818.104.136.1

Convenzione

tra il Dipartimento federale dell'interno della Confederazione Svizzera e il Robert Koch-Institut, istituto federale nel settore di attività del Ministero della salute della Repubblica federale tedesca, avente ad oggetto le app di tracciamento dei contatti con persone infette da coronavirus (scambio di chiavi mediante un server gateway di interoperabilità transfrontaliera gestito in territorio svizzero)

Conclusa il 19 marzo 2021
Entrata in vigore mediante scambio di note il 7 maggio 2021
(Stato 7 maggio 2021)

Il Robert Koch-Institut, istituto federale nel settore di attività del Ministero della salute della Repubblica federale tedesca e responsabile dell'app «Corona-Warn» ai sensi della normativa in materia di protezione dei dati, denominato in appresso **«RKI»**, e il Dipartimento federale dell'interno della Confederazione Svizzera, rappresentato dall'Ufficio federale della sanità pubblica, responsabile dell'app «SwissCovid» ai sensi della normativa in materia di protezione dei dati e denominato in appresso **«UFSP»**, denominati congiuntamente **«partner»**, stipulano la seguente Convenzione sullo scambio di chiavi tra le rispettive app di tracciamento dei contatti mediante un server gateway di interoperabilità transfrontaliera gestito in territorio svizzero.

§ 1 Campo di applicazione e scopo della Convenzione

1. La presente Convenzione riguarda esclusivamente il trattamento di dati personali, descritto al paragrafo 3, mediante il server gateway per consentire lo scambio transfrontaliero di segnalazioni tra utenti dell'app Corona-Warn del RKI e dell'app SwissCovid dell'UFSP risultati positivi al coronavirus. Le disposizioni che seguono sono applicabili nella misura in cui in virtù della legislazione in materia di protezione dei dati i partner sono contitolari del trattamento, secondo quanto previsto dall'articolo 26 del Regolamento generale sulla protezione dei dati (GDPR) o da normative nazionali equivalenti.

2. Il trattamento dei dati tramite il gateway ha lo scopo esclusivo di permettere da un punto di vista tecnico al RKI in quanto gestore dell'app Corona-Warn e all'UFSP in quanto gestore dell'app SwissCovid di avvertire efficacemente i rispettivi utenti entrati in contatto con un utente dell'altra app nazionale di tracciamento dei contatti in merito alla potenziale esposizione al SARS-CoV-2 in caso di una relativa segnalazione. Tale scopo include anche l'analisi statistica successiva dei dati di protocollo, intesa ad assicurare il funzionamento del gateway e a rilevare statisticamente il carico e l'utilizzo generale del server.

3. Lo scopo della presente Convenzione è di definire le finalità e i mezzi del trattamento congiunto dei dati e di disciplinare i relativi diritti e obblighi dei partner in qualità di contitolari. Ciascuno dei partner rimane il titolare unico delle attività di trattamento che esulano dal campo di applicazione della presente Convenzione, per le quali non vengono definiti congiuntamente finalità e mezzi del trattamento.

§ 2 Definizioni

1. Per «utente» si intende una persona che utilizza un'app di tracciamento dei contatti su un telefono cellulare.

2. Per «app di tracciamento dei contatti» si intendono le applicazioni informatiche per telefono cellulare (app) fornite dai partner sotto le denominazioni «Corona-Warn» e «SwissCovid» che tracciano la prossimità tra utenti e segnalano la potenziale esposizione al coronavirus SARS-CoV-2.

3. Per «server back-end» si intende un sistema di server gestito a livello nazionale che mette a disposizione dell'app nazionale (app di tracciamento dei contatti o equivalente) il proprio contenuto mediante procedura di richiamo. Tale contenuto consiste segnatamente di chiavi e metadati trasmessi dalle app di tracciamento dei contatti o scaricati dal gateway.

4. Per «gateway» si intende un sistema di server gestito dall'UFSP, al quale può essere collegato un server back-end tramite un'interfaccia per caricare le chiavi della propria app nazionale e scaricare le chiavi messe a disposizione da corrispondenti app estere.

5. Per «chiavi» si intendono i codici di identificazione univoci con un giorno di validità generati dal sistema operativo del telefono cellulare, nonché i relativi metadati, per un utente che mediante un'app di tracciamento dei contatti segnala di essere risultato positivo al SARS-CoV-2. Essi sono considerati dati sanitari ai sensi del GDPR.

6. Per «metadati» si intendono le informazioni collegate a una chiave o in essa contenute che possono contenere indicazioni riguardanti il giorno di validità, la verifica del contagio, il Paese di provenienza della chiave e altri dati rilevanti dal punto di vista epidemiologico e che vengono utilizzate da un'app di tracciamento dei contatti per valutare la contagiosità di un utente che mediante l'app in uso segnala di essere risultato positivo al SARS-CoV-2.

7. Per «verifica del contagio» si intendono i metodi di conferma di un contagio da SARS-CoV-2, vale a dire la conferma del contagio da parte di un'autorità sanitaria nazionale o mediante esame di laboratorio.

8. Per «dati di protocollo» si intende la registrazione automatica di un accesso connesso al trattamento di dati tramite il gateway, dalla quale risultano in particolare il tipo, la data e l'ora del trattamento.

9. Per «dati personali» si intendono tutte le informazioni che si riferiscono a una persona fisica identificata o identificabile («persona interessata») nel campo di applicazione della presente Convenzione.

§ 3 Scambio di dati transfrontaliero tra l'app Corona-Warn e l'app SwissCovid tramite il gateway

1. L'attività di trattamento congiunto dei partner sul gateway si limita alle seguenti fasi di processo:

a) autenticazione dei server back-end nazionali;

b) ricezione delle chiavi tramite un'interfaccia di programmazione dell'applicazione che consente ai server back-end nazionali di caricare questi dati;

c) memorizzazione sul gateway delle chiavi caricate dai server back-end nazionali;

d) approntamento sul gateway delle chiavi memorizzate provenienti dalla Repubblica federale tedesca per lo scaricamento tramite il server back-end svizzero;

e) approntamento sul gateway delle chiavi memorizzate provenienti dalla Confederazione Svizzera per lo scaricamento tramite il server back-end tedesco;

f) verifica della confidenzialità e dell'integrità delle chiavi al momento della ricezione e dell'approntamento;

g) cancellazione o distruzione definitiva delle chiavi memorizzate subito dopo essere state scaricate e verificate dal server back-end ricevente, oppure 14 giorni dopo la ricezione dal server back-end trasmittente; è determinante il primo di questi due momenti;

h) cancellazione o distruzione definitiva di tutti i dati personali rimanenti dopo la disattivazione del gateway o la sospensione unilaterale definitiva della trasmissione di chiavi al gateway da parte di un partner.

2. I server back-end nazionali possono trasmettere al gateway soltanto le chiavi della loro app nazionale di tracciamento dei contatti il cui giorno di validità al momento della trasmissione risale al massimo a 14 giorni prima.

3. La trasmissione di chiavi al gateway può essere effettuata soltanto se l'utente ha espressamente acconsentito al trattamento transfrontaliero dei propri dati ai fini della presente Convenzione.

4. In linea di principio, il trattamento è effettuato in base alle norme tecniche di interoperabilità accessibili al pubblico della rete europea eHealth, salvo diversa disposizione della presente Convenzione e nella misura di quanto possibile per i partner in virtù del diritto nazionale. Tali norme risultano in particolare dalle specifiche di interoperabilità del 16 giugno 2020[1] per le catene di trasmissione transfrontaliere tra app approvate.

5. Il trattamento è effettuato previa reciproca accettazione dei partner e soltanto a condizione che nel Paese dell'altro partner sia garantito un livello di protezione

[1] Consultabile in Internet al seguente indirizzo: https://ec.europa.eu/health/ehealth/key_documents_en#anchor0

equivalente nel trattamento dei dati personali, e che sia prevista una decisione di adeguatezza della Commissione europea secondo l'articolo 45 GDPR o siano previste garanzie adeguate secondo l'articolo 46 GDPR e le persone interessate dispongano di diritti azionabili e di rimedi giuridici efficaci.

§ 4 Competenze e obblighi dell'UFSP

1. La competenza per l'allestimento e la gestione del gateway spetta all'UFSP. In tale funzione, l'UFSP garantisce il trattamento sicuro e la protezione dei dati scambiati sul gateway, compresa la loro trasmissione e il loro approntamento, e assume i compiti definiti al capoverso 3. L'UFSP sostiene i costi che ne risultano, mentre quelli per l'adeguamento delle proprie app di tracciamento dei contatti sono a carico di ciascun partner.

2. L'UFSP, in collaborazione con il Centro nazionale per la cibersicurezza (NCSC) e l'Incaricato federale della protezione dei dati e della trasparenza (IFPDT), verifica, analizza e valuta regolarmente, almeno ogni sei mesi e a seconda delle circostanze, l'efficacia delle misure tecniche e organizzative volte a garantire il trattamento sicuro dei dati sul gateway. L'UFSP informa l'IFPDT in merito all'analisi e alla valutazione.

3. L'UFSP:

a) crea e garantisce un'infrastruttura di comunicazione sicura, che consenta ai server back-end dei partner di scambiare i dati menzionati al paragrafo 3 capoverso 2 conformemente a quanto disposto dalla presente Convenzione;

b) con il consenso del RKI, può coinvolgere un terzo in veste di responsabile del trattamento ai sensi dell'articolo 4 numero 8 GDPR. Gli accordi contrattuali con il responsabile del trattamento devono rispettare le esigenze di cui all'articolo 28 GDPR. In caso di ricorso a un responsabile per il trattamento di dati personali di utenti dell'app Corona-Warn, l'UFSP provvede affinché gli obblighi di protezione dei dati previsti dalla presente Convenzione si applichino anche al responsabile del trattamento e vengano da esso rispettati. In linea di principio, il responsabile ha la possibilità di designare un solo sotto-responsabile del trattamento e solo con il consenso del RKI. Il RKI ha il diritto di negare il proprio consenso alla designazione di un responsabile o di un sotto-responsabile per gravi motivi. Un grave motivo può sussistere in particolare se il sotto-responsabile pregiudica la posizione giuridica del RKI ai sensi della presente Convenzione, se il RKI ha una valida ragione di temere che il sotto-responsabile non rispetti gli obblighi contrattuali e/o legali di protezione dei dati e/o di sicurezza delle informazioni o se esistono seri indizi di comportamento non conforme da parte del sotto-responsabile, tali da compromettere la fiducia nella sua generale affidabilità;

c) se altri Paesi si allacciano al gateway, assicura che le chiavi trasmesse al gateway dal server back-end dell'app Corona-Warn continuino a essere scambiate ai fini della presente Convenzione soltanto con il server back-end dell'app SwissCovid, e in particolare che non vengano trasmesse ai sistemi degli altri Paesi;

d) adotta tutte le misure organizzative, fisiche e logiche di sicurezza necessarie in base alle direttive dell'Amministrazione federale della Confederazione Svizzera in materia di TIC (Protezione di base delle TIC nell'Amministrazione federale)[2] per garantire il funzionamento del gateway. A tal fine, l'UFSP:

   aa) designa un servizio competente per la gestione della sicurezza del gateway, comunica al RKI le coordinate di contatto del servizio designato e garantisce la sua prontezza a reagire a eventuali minacce per la sicurezza,

   bb) si assume la responsabilità della sicurezza del gateway,

   cc) assicura che tutte le persone autorizzate ad accedere al gateway sono sottoposte a obblighi contrattuali, professionali o legali di confidenzialità considerati sufficienti ai sensi del GDPR o di normative nazionali equivalenti, anche considerata la qualificazione delle chiavi come dati sanitari;

e) adotta tutte le misure di sicurezza necessarie per garantire che il regolare funzionamento dei server back-end dei partner non venga compromesso. A tal fine, predispone procedure particolari per la connessione dei server back-end al gateway, tra cui:

   aa) una procedura per l'analisi del rischio, che consenta di identificare e valutare le potenziali minacce per il sistema,

   bb) una procedura di audit e di verifica:

      i. per la verifica della conformità delle misure di sicurezza attuate con le pertinenti prescrizioni in materia di sicurezza applicabili al trattamento dei dati (il quale, per quanto riguarda le chiavi, comprende i dati sanitari) previste dalla direttiva Si001 – Protezione di base delle TIC nell'Amministrazione federale – e dalla legislazione svizzera in materia di protezione dei dati,

      ii. per il controllo regolare dell'integrità dei file di sistema, dei parametri di sicurezza e delle autorizzazioni rilasciate,

      iii. per la sorveglianza necessaria ad accertare eventuali violazioni della sicurezza e intrusioni non autorizzate,

      iv. per l'attuazione delle modifiche necessarie a eliminare eventuali lacune nella sicurezza, e

      v. per consentire – anche su richiesta del RKI – lo svolgimento e la partecipazione alla realizzazione di audit indipendenti, ispezioni comprese, nonché verifiche delle misure di sicurezza (p. es. protezione di base secondo l'Ufficio federale tedesco per la sicurezza informatica, BSI) e controlli da parte dell'autorità di controllo per

2 In particolare le direttive Si001 – Protezione di base delle TIC nell'Amministrazione federale – e Si003 – Sicurezza delle reti nell'Amministrazione federale – , consultabili in Internet sul sito: www.bk.admin.ch > Trasformazione digitale e governance delle TIC > Direttive TIC > Sicurezza

la protezione dei dati competente per il RKI ai fini dell'adempimento dei rispettivi compiti di legge,

cc) una procedura di controllo delle modifiche, che consenta di documentare e valutare le conseguenze di una modifica prima della sua implementazione e di tenere informati i titolari del trattamento in merito a tutte le modifiche che potrebbero avere un impatto sulla comunicazione con le loro infrastrutture e/o sulla loro sicurezza,

dd) una procedura di manutenzione e riparazione con regole e condizioni per la manutenzione e/o riparazione delle apparecchiature,

ee) una procedura per gli incidenti in materia di sicurezza (procedura di segnalazione e di escalation) atta a garantire che l'incaricato ufficiale della protezione dei dati del RKI riceva senza indugio informazioni in merito a ogni violazione di dati personali, con indicazione delle modalità, dell'estensione e delle circostanze nonché delle probabili conseguenze della violazione e delle misure adottate e previste per l'eliminazione della violazione e la mitigazione delle possibili conseguenze negative,

ff) se non esiste già, una procedura disciplinare per procedere contro le violazioni della sicurezza,

gg) un test di penetrazione effettuato da un organismo indipendente, compresa un'analisi del codice sorgente;

f) adotta misure di sicurezza fisiche e/o logiche conformi allo stato attuale della tecnica per le infrastrutture in cui sono alloggiate le apparecchiature per il gateway, per i controlli dei dati logici e per la sicurezza degli accessi. La direttiva sulla protezione di base delle TIC (cfr. par. 4 cpv. 3 lett. e bb i.) costituisce la base di riferimento; altre misure di sicurezza di natura tecnico-organizzativa devono essere documentate nel piano di sicurezza;

g) adotta misure per la protezione del proprio dominio di rete, compresa la separazione dei collegamenti;

h) tiene un piano di gestione dei rischi per quanto riguarda il gateway;

i) sorveglia – in tempo reale – la performance di tutte le componenti di servizio del gateway, allestisce statistiche periodiche e registra le attività del gateway;

j) fornisce assistenza telefonica e per posta elettronica a tutti i servizi del gateway e risponde alle telefonate dei chiamanti autorizzati;

k) adotta tutte le misure necessarie per garantire che il gestore tecnico del gateway non possa accedere senza autorizzazione ai dati trasmessi;

l) adotta le opportune misure per agevolare la comunicazione tra i partner;

m) conformemente all'articolo 30 capoverso 1 GDPR o a una normativa nazionale equivalente nonché alla presente Convenzione, tiene un registro di tutte le operazioni di trattamento eseguite;

n) a intervalli regolari, adotta le opportune misure atte a garantire che le misure di sicurezza fisiche e logiche siano sempre conformi allo stato della tecnica;

o) in accordo con l'Ufficio federale dell'informatica e della telecomunicazione (UFIT), consente al RKI o ai servizi da esso coinvolti, quali il BSI, di procedere ai propri controlli della sicurezza tecnica del gateway e di ripetere tali controlli o parte di essi in caso di modifiche fisiche o logiche del gateway.

4. L'UFSP comunica senza indugio al RKI tutti i fatti e le modifiche importanti che riguardano il gateway e che influiscono sul trattamento dei dati scambiati, in particolare:

a) i rischi potenziali o concreti per la disponibilità, la confidenzialità e/o l'integrità dei dati trattati sul gateway;

b) gli incidenti in materia di sicurezza;

c) ogni violazione di dati personali, le probabili conseguenze di tale violazione e la valutazione dei rischi per i diritti e le libertà delle persone fisiche, nonché tutte le misure adottate per rimediare alla violazione e ridurre i rischi per i diritti e le libertà delle persone fisiche;

d) ogni violazione dei provvedimenti tecnici e/o organizzativi adottati ai sensi della presente Convenzione per tutelare le operazioni di trattamento sul gateway;

e) ogni modifica fisica o logica del gateway con un impatto diretto o indiretto sulla disponibilità, confidenzialità e/o integrità dei dati trattati sul gateway.

5. Inoltre, in caso di incidenti in materia di sicurezza, l'UFSP informa direttamente e senza indugio anche l'incaricato ufficiale della protezione dei dati del RKI, per stabilire l'ulteriore modo di procedere. Se in seguito a un incidente in materia di sicurezza i partner sottostanno a obblighi di notifica o comunicazione in virtù degli articoli 33 e 34 GDPR, l'UFSP mette senza indugio a disposizione del RKI, e separatamente anche dell'incaricato ufficiale della protezione dei dati del RKI, tutte le informazioni necessarie per la verifica dell'eventuale sussistere di un obbligo di notifica o di comunicazione.

6. Se i partner sottostanno a obblighi di comunicazione ai sensi dell'articolo 34 GDPR, l'UFSP si assume il compito di comunicare con le persone interessate dalla violazione di dati personali in territorio svizzero, compresi gli utenti dell'app SwissCovid.

7. L'UFSP ha anche il compito di trattare ed evadere le domande/richieste degli utenti dell'app SwissCovid riguardanti l'esercizio dei diritti delle persone interessate conformemente al GDPR o a una normativa nazionale equivalente nonché alla presente Convenzione.

8. Conformemente agli articoli 13, 14 e 26 capoverso 2 secondo periodo GDPR, nell'ambito dell'informativa sulla protezione dei dati dell'app SwissCovid l'UFSP informa gli utenti dell'app in merito al trattamento dei loro dati personali in virtù della presente Convenzione ai fini delle segnalazioni transfrontaliere.

§ 5 Competenze e obblighi del RKI

1. Nei limiti delle sue possibilità, il RKI assiste l'UFSP nell'identificare e gestire gli incidenti in materia di sicurezza connessi al trattamento dei dati sul gateway, comprese le violazioni di dati personali.

2. In particolare, nei limiti delle proprie conoscenze e possibilità, il RKI comunica all'UFSP le seguenti informazioni:

a) i rischi potenziali o concreti per la disponibilità, la confidenzialità e/o l'integrità dei dati personali trattati sul gateway;

b) gli incidenti in materia di sicurezza connessi al trattamento dei dati sul gateway;

c) ogni violazione di dati personali, le probabili conseguenze di tale violazione e la valutazione dei rischi per i diritti e le libertà delle persone fisiche, nonché tutte le misure adottate per rimediare alla violazione e ridurre i rischi per i diritti e le libertà delle persone fisiche;

d) ogni violazione dei provvedimenti tecnici e/o organizzativi adottati per tutelare le operazioni di trattamento sul gateway.

3. Il RKI ha anche il compito di trattare ed evadere le domande/richieste degli utenti dell'app Corona-Warn riguardanti l'esercizio dei diritti delle persone interessate conformemente al GDPR o a una normativa nazionale equivalente nonché alla presente Convenzione.

4. Conformemente agli articoli 13, 14 e 26 capoverso 2 secondo periodo GDPR, nell'ambito dell'informativa sulla protezione dei dati dell'app Corona Warn il RKI informa gli utenti dell'app in merito al trattamento dei loro dati personali in virtù della presente Convenzione.

5. Il RKI assume la responsabilità in merito all'adempimento degli obblighi di notifica e di comunicazione che incombono ai partner in virtù degli articoli 33 e 34 GDPR. È responsabile di effettuare le notifiche e le comunicazioni nonché della comunicazione con l'autorità di controllo competente ai sensi degli articoli 33 e 34 GDPR.

6. Se i partner sottostanno a obblighi di comunicazione ai sensi dell'articolo 34 GDPR, il RKI si assume il compito di comunicare con le persone interessate dalla violazione di dati personali in territorio tedesco, compresi gli utenti dell'app Corona-Warn.

§ 6 Competenze e obblighi di entrambi i partner

1. Ciascuno dei partner istituisce un punto di contatto dotato di una casella di posta elettronica funzionale da utilizzare per la comunicazione tra i partner in relazione alla presente Convenzione. In linea di principio, i messaggi in arrivo dovrebbero essere letti e trattati in tempi molto brevi. Nei casi urgenti occorre contattare l'altro partner anche telefonicamente, per informarlo e concordare il da farsi. A tal fine, ciascuno dei partner designa un interlocutore diretto (posta elettronica, telefono).

2. Ciascuno dei partner riceve le domande/richieste riguardanti l'esercizio dei diritti delle persone interessate trasmessegli dagli utenti conformemente al GDPR o a una normativa nazionale equivalente nonché alla presente Convenzione. Ciascuno dei partner designa uno speciale punto di contatto per le domande/richieste degli utenti. Se uno dei partner riceve da un utente una domanda/richiesta riguardante l'esercizio dei diritti delle persone interessate che, secondo la presente Convenzione o la normativa ad esso applicabile, non è di sua competenza o responsabilità, trasmette senza indugio la domanda/richiesta in questione al partner competente. Su richiesta, i partner si assistono reciprocamente nel trattamento delle domande/richieste delle persone interessate riguardanti l'esercizio dei loro diritti e rispondono all'altro senza indugio, ma al più tardi entro 15 giorni dalla ricezione di una richiesta di assistenza reciproca.

3. Ciascuno dei partner pubblica la presente Convenzione sul proprio sito Internet.

4. Se uno dei partner ha bisogno di informazioni da parte dell'altro partner per adempiere i propri obblighi ai sensi degli articoli 35 e 36 GDPR o di una normativa nazionale equivalente nonché della presente Convenzione, trasmette una domanda particolare alla casella di posta elettronica funzionale dell'altro partner. Quest'ultimo fa tutto il possibile per fornire le informazioni richieste.

5. Ciascuno dei partner è tenuto a garantire la correttezza dei dati personali trasmessi al gateway. Se emerge che un partner ha trasmesso al gateway dati personali inesatti o dati personali che non avrebbero dovuto essere trasmessi, ne avvisa senza indugio l'altro partner.

6. I dati personali degli utenti di un'app di tracciamento dei contatti che vengono trasmessi dai partner al gateway possono essere trasmessi soltanto in forma anonimizzata o pseudonimizzata. Ciascuno dei partner certifica che allo stato attuale delle conoscenze non è in grado di:

a) risalire all'identità di utenti specifici per mezzo delle chiavi presenti sul proprio server back-end; né

b) risalire all'identità di utenti specifici per mezzo delle chiavi ricevute tramite il gateway dall'altro partner o di eventuali altri set di dati.

7. Se un partner non è in grado di trattare le domande/richieste di una persona interessata riguardanti l'esercizio dei propri diritti perché non può identificarla a causa di una deliberata disattivazione della tracciabilità, ne informa la persona in questione nella misura in cui i dati di contatto disponibili glielo permettono (p. es. indirizzo di posta elettronica, recapito postale). In tal caso, i diritti della persona interessata non possono essere esercitati, a meno che quest'ultima fornisca a tal fine informazioni complementari che consentono di identificarla.

8. Ciascuno dei partner provvede affinché l'altro partner o l'entità giuridica da cui dipende secondo il diritto nazionale risponda nei confronti delle persone illecitamente danneggiate dalla trasmissione di dati ai sensi della presente Convenzione. Si applicano le disposizioni di cui all'articolo 82 capoversi 4 e 5 GDPR o disposizioni equivalenti del diritto nazionale che prevedono la responsabilità solidale dei contito-

lari nei confronti di terzi e, internamente, la ripartizione della responsabilità in proporzione alla parte di responsabilità per l'evento dannoso imputabile a ciascuno dei partner.

§ 7 Composizione delle controversie

1. Le controversie tra i partner relative all'interpretazione o all'applicazione della presente Convenzione devono essere per quanto possibile risolte in via amichevole.

2. Se una controversia non può essere risolta in via amichevole, essa viene sottoposta, su richiesta di un partner, a un tribunale arbitrale.

3. Il tribunale arbitrale è costituito caso per caso; ciascuno dei partner nomina un membro e i due membri designano di comune accordo un terzo membro come presidente nominato da entrambi i partner. I membri sono nominati entro due settimane dal momento in cui un partner ha comunicato all'altro che intende sottoporre la controversia a un tribunale arbitrale.

4. Il tribunale arbitrale statuisce a maggioranza dei voti. Le sue decisioni sono vincolanti e definitive. Ciascuno dei partner assume le spese per il proprio membro e quelle di rappresentanza nella procedura davanti al tribunale arbitrale; le spese per il presidente e gli altri costi sono ripartiti, in misura uguale, tra i partner. Il tribunale arbitrale può stabilire un'altra ripartizione delle spese. Per il resto, disciplina autonomamente la procedura applicabile.

§ 8 Disposizioni finali

1. La presente Convenzione entra in vigore non appena i partner si sono notificati reciprocamente l'adempimento delle condizioni nazionali. Il gateway viene attivato non appena tutte le apparecchiature necessarie sono state predisposte.

2. La Convenzione può essere modificata, abrogata o prorogata in qualsiasi momento di comune accordo tra i partner.

3. Essa rimane in vigore per la durata dello scambio di chiavi tramite il gateway e fintanto che il gateway esiste, ma al più tardi fino al 30 giugno 2022.

4. Le disposizioni della presente Convenzione relative alla protezione dei dati personali rimangono applicabili ai dati già trasmessi anche dopo l'abrogazione, la denuncia o la scadenza della Convenzione.

5. Ciascuno dei partner può sospendere in qualsiasi momento la trasmissione al gateway delle chiavi degli utenti della propria app di tracciamento dei contatti. Per quanto esigibile, tale intenzione deve essere comunicata all'altro partner il prima possibile affinché quest'ultimo possa adottare tempestivamente le necessarie misure, come l'adeguamento delle informazioni sulla protezione dei dati destinate agli utenti della propria app.

6. La presente Convenzione può essere denunciata unilateralmente per iscritto da ciascuno dei partner. La denuncia ha effetto dopo un mese dalla sua ricezione da parte dell'altro partner.

Berna, 15 marzo 2021

Per il
Dipartimento federale dell'interno:

Anne Lévy

Berlino, 19 marzo 2021

Per il
Robert Koch-Institut:

Lars Schaade