Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale dell'interno DFI
Ufficio federale della sanità pubblica UFSP

Informativa sulla protezione dei dati dell'Ufficio federale della sanità pubblica UFSP in relazione all'utilizzo dell'«app SwissCovid»

Versione: 24. giugno 2020

Nella presente informativa sulla protezione dei dati l'Ufficio federale della sanità pubblica (UFSP) spiega in che misura tratterà dati personali nel quadro dell'utilizzo dell'applicazione «app SwissCovid» (di seguito app) in Svizzera. Non si tratta di una descrizione esaustiva; alcuni aspetti specifici possono essere regolamentati da altre informative sulla protezione dei dati, documenti analoghi, condizioni di utilizzo o programmi di applicazione.

Il trattamento dei dati personali è disciplinato dal diritto sulla protezione dei dati; al trattamento dei dati si applica la legislazione federale in materia. La presente informativa è inoltre conforme alla legge del 28 settembre 2012 sulle epidemie (LEp; RS 818.101) e all'ordinanza del 24 giugno 2020 sul sistema di tracciamento della prossimità per il coronavirus SARS-CoV-2 (OSTP; RS 818.101.25).

Per dati personali s'intendono tutte le informazioni relative a una persona identificata o identificabile. Il trattamento indica qualsiasi operazione relativa a dati personali, indipendentemente dai mezzi e dalle procedure impiegati, segnatamente la raccolta, la conservazione, l'utilizzazione, la modificazione, la comunicazione, l'archiviazione o la distruzione di dati.

1 Responsabile

Responsabile per il trattamento dei dati descritto nella presente informativa:

Ufficio federale della sanità pubblica UFSP
3003 Berna
Svizzera
Tel. +41 58 462 69 98
recht(at)bag.admin.ch

2 Raccolta e trattamento dei dati personali

L'intero sistema dell'app è concepito in modo tale che l'utente non sia identificabile. Il trattamento dei dati personali è ridotto al minimo, per cui non è in alcun modo tecnicamente possibile risalire a persone, luoghi o dispositivi. Non vengono rilevati dati sulla posizione, ma soltanto informazioni crittografate riguardanti i contatti avvenuti, protette tecnicamente da usi impropri. L'UFSP non può risalire agli utenti dell'app, che ne protegge i dati impedendo di stabilire un collegamento con una data persona sulle lunghe distanze. Un collegamento a una data persona non può tuttavia essere completamente escluso. Esiste infatti una certa probabilità che una persona informata di essere potenzialmente a rischio possa risalire all'identità della persona contagiata ricostruendo i contatti sociali avuti nei giorni precedenti. La notifica include l'informazione che l'utente è stato potenzialmente esposto al coronavirus, l'indicazione del giorno in cui lo è stato per l'ultima volta, l'informazione che

l'UFSP gestisce una linea di consulenza telefonica gratuita e le raccomandazioni di comportamento dell'UFSP. L'utilizzo dell'app potrebbe quindi permettere l'identificazione di persone.

Il sistema dell'app è costituito da due componenti:

- un sistema di gestione dei dati di prossimità, costituito da un software che viene installato dagli utenti sul proprio telefono cellulare e da un back end (back end GP);
- un sistema di gestione dei codici di attivazione delle informazioni (sistema di gestione dei codici), costituito da un front end e un back end basati sul web.

Entrambi i back end, che fungono da server centrali, sono sotto il controllo diretto dell'UFSP e sono tecnicamente gestiti dall'Ufficio federale dell'informatica e della telecomunicazione (UFIT). I front end per la gestione dei codici funzionano sui dispositivi degli specialisti autorizzati a generare il codice di attivazione (codice Covid).

Sul telefono cellulare sono memorizzati i seguenti dati:

- codici di identificazione (ID casuali) ricevuti da altri telefoni cellulari con l'app attivata;
- potenza del segnale;
- data e durata stimata della prossimità.

In caso di contagio confermato di un utente, nel sistema di gestione dei codici vengono registrati i seguenti dati:

- il codice di attivazione (codice Covid);
- la data in cui si sono manifestati i primi sintomi o, se l'utente contagiato non presenta sintomi, la data in cui è stato effettuato il test;
- il momento di distruzione di questi dati.

Il back end GP è costituito da un elenco con i seguenti dati:

- le chiavi private degli utenti contagiati che erano di attualità nel periodo in cui altri utenti erano potenzialmente esposti al coronavirus;
- la data di ogni chiave.

3 Scopi e basi giuridiche

Il sistema dell'app gestito dall'UFSP si fonda sulla LEp e sull'OSTP. L'app e i relativi dati trattati servono unicamente a informare, nel rispetto della protezione dei dati, gli utenti che sono stati potenzialmente esposti al coronavirus e a elaborare statistiche in relazione al coronavirus a partire dai dati dei due back end.

4 Trasmissione dei dati

L'elenco con i dati del back end GP viene messo a disposizione dell'app (o del front end) mediante procedura di richiamo. Laddove l'UFSP commissioni tali servizi a terzi situati in Svizzera o all'estero, questi ultimi s'impegnano contrattualmente a rispettare le prescrizioni dell'articolo 60*a* LEp e dell'OSTP; è fatta salva la disposizione sul codice sorgente di cui all'articolo 60*a* capoverso 5 lettera e LEp. L'UFSP controlla che questi terzi rispettino le prescrizioni e non utilizzino per scopi propri i metadati generati durante l'esecuzione del mandato. Questi dati sono analizzati soltanto dall'UFSP o dall'UFIT (cfr. pt. 8).

L'UFSP mette periodicamente a disposizione dell'Ufficio federale di statistica per valutazioni statistiche l'attuale raccolta di dati disponibili nei due back end in forma completamente anonimizzata. L'UFIT gestisce su incarico dell'UFSP tutti i software e fornisce il servizio di assistenza tecnica necessario. L'UFIT ha accesso solo ai dati necessari agli scopi descritti e all'attività dei collaboratori interessati, che sono tenuti a utilizzare i dati con riservatezza.

L'app utilizza un'interfaccia verso il sistema operativo del telefono cellulare dell'utente che elabora dati

attraverso Apple o Google. Le funzioni dei sistemi operativi utilizzate tramite l'interfaccia devono adempiere le prescrizioni di cui all'articolo 60*a* LEp e della presente ordinanza; è fatta salva la disposizione sul codice sorgente di cui all'articolo 60*a* capoverso 5 lettera e LEp. L'UFSP si assicura che queste prescrizioni siano rispettate, in particolare richiedendo le necessarie garanzie.

5 Periodo di conservazione

Quando non servono più a informare gli utenti, i dati sono distrutti come segue:

- dati del sistema di gestione dei dati di prossimità (sia nei telefoni cellulari sia nel back end GP): 14 giorni dopo la loro registrazione;
- dati del sistema di gestione dei codici: 24 ore dopo la loro registrazione.

6 Sicurezza dei dati

In stretta collaborazione con i suoi fornitori interni ed esterni di hosting e altri fornitori di servizi IT, l'UFSP adotta adeguati provvedimenti di sicurezza tecnici (p. es. crittografia, pseudo-anonimizzazione, registri, controlli e restrizioni degli accessi, sicurezza dei dati, soluzioni per la sicurezza IT e delle reti ecc.) e organizzativi (p. es. istruzioni ai collaboratori, accordi di riservatezza, controlli ecc.) per proteggere i dati da accessi non autorizzati, perdite e usi impropri, in conformità con le prescrizioni dell'Amministrazione federale e della legislazione svizzera in materia di protezione dei dati.

7 Diritti della persona interessata

La persona interessata ha diritto di accedere ai propri dati e di richiederne la rettifica, la cancellazione o la consegna. Ha inoltre il diritto di limitarne il trattamento o di opporvisi, nonché di revocare il proprio consenso senza che ciò pregiudichi la legalità del trattamento dei dati effettuato fino a quel momento. Questi diritti valgono laddove siano presenti dati personali. Il sistema dell'app si basa sul principio della «privacy by design», che mediante metodi crittografici innovativi e un trattamento dei dati decentralizzato permette di evitare il più possibile la presenza di dati su persone determinate o determinabili (dati personali). Per questo motivo l'UFSP non può, per esempio, fornire informazioni sui contatti ravvicinati registrati di una data persona né rettificare questi dati. L'UFSP non può consultare questi dati poiché sono memorizzati unicamente sui telefoni cellulari.

L'esercizio dei propri diritti presuppone che la persona interessata dimostri in modo univoco la propria identità (p. es. mediante copia di un documento). Per far valere i propri diritti si può contattare l'UFSP all'indirizzo indicato al punto 1.

In caso di violazione delle disposizioni legali sulla protezione dei dati ci si può rivolgere all'autorità di vigilanza competente oppure adire le vie legali previste dalla legislazione in materia.

8 Varie

Vengono memorizzati i registri degli accessi al back end GP e al sistema di gestione dei codici per gli scopi previsti agli articoli 57*l*–57*o* della legge del 21 marzo 1997 sull'organizzazione del Governo e dell'Amministrazione (LOGA; RS 172.010). Gli accessi possono essere analizzati statisticamente. Si applicano gli articoli 57*i*–57*q* LOGA e l'ordinanza del 22 febbraio 2012 sul trattamento di dati personali derivanti dall'utilizzazione dell'infrastruttura elettronica della Confederazione (RS 172.010.442).

I dati dei registri vengono distrutti come segue:

- dati dei registri di terzi incaricati dall'UFSP: 7 giorni dopo la loro registrazione;
- per il resto la distruzione dei dati dei registri è retta dall'articolo 4 capoverso 1 lettera b

dell’ordinanza del 22 febbraio 2012 sul trattamento di dati personali derivanti dall’utilizzazione dell’infrastruttura elettronica della Confederazione (RS 172.010.442).

9 Modifiche

L’UFSP può modificare in qualsiasi momento e senza preavviso la presente informativa. Fa fede la versione più recente pubblicata o la versione valida per il periodo interessato. La presente informativa è stata redatta in diverse lingue. In caso di divergenze fa fede la versione tedesca. In caso di aggiornamento l’utente dell’app viene informato sulla modifica in forma appropriata.

*****