RELAZIONE PROPOSTA n. 100

Nome soluzione

Immuni

Soggetto proponente

Bending Spoons S.p.A..
L'iniziativa è presentata unitamente a Arago, GeoUniq, Centro Medico Santagostino e Jakala.

Tipologia di dati trattati dall'app

Alla luce dei chiarimenti forniti dalla proponente in data 02/04/2020, pare che l'app non tratti dati personali fino al momento in cui, a seguito di diagnosi da parte di un operatore sanitario, non venga contattato l'utente.
All'utente all'atto del login viene assegnato un codice generato pseudo-randomicamente, dal sistema Bluetooth LE, circostanza che non permette di identificare l'utente dello specifico dispositivo. Non viene richiesto alcun numero di telefono in fase di login.
L'App consente pertanto una minimizzazione di tutti i dati personali e particolari fino all'eventuale e futuro contatto con l'operatore.
Non sono previsti dati di geolocalizzazione essendo sufficiente allo scopo il contatto di prossimità con i terzi soggetti attraverso la memorizzazione dei Bt_ID (bluetooth Identification), ma è possibile aggiungere anche il georeferenziamento (che potrebbe rimanere su base volontaria).
L'applicazione consente altresì la memorizzazione sul device personale dei dati di familiari/conviventi in relazione ai quali - fino all'implementazione di dispositivi wearable - può essere attivata solo la funzione di "diario clinico" con le stesse garanzie di minimizzazione dei dati implementate per l'utente principale dell'App.

Modalità del trattamento

I dati inerenti lo stato di salute che vengono memorizzati ed elaborati esclusivamente in locale sul device dell'utente non vengono associati ad un'identità o a dati anagrafici. Neanche in fase di Login. L'applicazione, basata esclusivamente su tecnologia Bluetooth LE, consente di gestire una funzione di *contact tracing* basata su una serie di ID (temporanei) non associati ad una identità dell'utente sia sul device sia in modalità tracing di prossimità. Al momento l'app non usa tecnologie di geolocalizzazione, nonostante il proponente dichiari che è possibile implementarla successivamente.
L'app fornisce una funzione di alerting nel caso ad un utente venga richiesto, a seguito di diagnosi da parte di un operatore sanitario, o per volontà dell'utente stesso di provvedere

ad inviare al server centrale una copia del database locale al server remoto contenente i Bt_ID crittografati dei dispositivi degli altri utenti con cui il paziente è stato in prossimità (max 50 mt) nel lasso di tempo di riferimento. Ove poi risulti necessario, dal server - su input dell'operatore sanitario - attraverso l'app, è possibile inviare (con modalità notifiche push) opportuni messaggi ai dispositivi che si sono trovati in prossimità di quello dell'utente positivo; tutto ciò senza che all'operatore sia noto alcun dato personale dei destinatari della notifica push. Tutto ciò avviene sfruttando un'applicazione mobile specifica per gli operatori sanitari che permette a questi ultimi di fornire all'utente un codice da inserire nell'applicazione installata sul proprio device e che consente di effettuare il dump remoto dei dati del diario clinico dell'utente e dei dati di prossimità rilevati.
Non sono previste né l'acquisizione di dati di geolocalizzazione né di metadati associati alle informazioni salvo la condizione di salute dell'utente diagnosticata dall'operatore sanitario in virtù delle misurazioni di temperatura inserite dallo stesso utente.

Dalla documentazione trasmessa è possibile ricavare che il rilevamento dei contatti di prossimità avviene con una precisione nell'ordine di 1 metro senza l'acquisizione di altri dati che non sia il codice bt_ID, la durata dell'interazione e la potenza di segnale (da cui è possibile inferire la distanza tra i dispositivi).

Per quanto riguarda il trattamento dei dati degli operatori sanitari viene effettuata la memorizzazione dei dati personali di quegli operatori sanitari che accedono al sistema, solo ai fini di autorizzazione/autenticazione sul sistema stesso.

Uso di soluzioni di terze parti

L'app utilizza la tecnologia di tracciamento contatti basate sul Bluetooth Low Energy (LE) di Arago.
Per la parte server del progetto, invece, viene utilizzata la piattaforma Google Cloud Platform.

Privacy by design – Privacy by default

Dall'esame della documentazione esaminata, emerge che nella progettazione di quest'applicazione si sono tenuti presenti i principi di privacy by design e by default in quanto è stato tenuto conto dello stato dell'arte, della natura, dell'ambito di applicazione, del contesto e delle finalità del trattamento, come anche dei rischi per i diritti e le libertà delle persone fisiche.
Dalla documentazione prodotta e dalla descrizione delle misure di protezione implementate si evince come siano state messe in atto misure tecniche e organizzative adeguate, quali la pressoché totale minimizzazione dei dati e la pseudonimizzazione degli stessi lasciando

soltanto nella fase finale e all'operatore sanitario l'attività di identificazione dell'utente successivamente all'accertamento della positività.
Inoltre le tecnologie utilizzate consentono di acquisire soltanto gli ID degli altri dispositivi presenti ad una distanza inferiore ai 50 metri.

Misure di sicurezza

Sotto il profilo della sicurezza informatica la società proponente non ha fornito report in merito a test di sicurezza sulle applicazioni o sui server in uso. Anche per quest' App, come per le altre esaminate, non si possono pertanto valutare in modo adeguato gli aspetti relativi alla cybersecurity e alla resistenza o meno ad attività di *reverse engineering* o ad altre tipologie di attacco informatico sia sull'app sia anche sui flussi di dati intercorrenti tra gli smartphone e il server.
Dalla documentazione fornita è stato dichiarato ed è stato possibile accertare la presenza di cifratura dei dati solo sui server del cloud provider (Google Cloud Platform) con algoritmi AES256 o AES128. Inoltre è stato dichiarato che il Cloud pro Google Cloud Platform è certificato ISO/IEC 27001, ISO/IEC 27017 e ISO/IEC 27018.
È stato dichiarato inoltre che i dati utilizzati nell'ambito del progetto verranno memorizzati esclusivamente in datacenter collocati all'interno dell'Unione Europea.
Si suggerisce di richiedere ulteriori informazioni in merito alle misure di sicurezza effettivamente implementate.

Analisi dei rischi per le libertà e i diritti degli interessati

Sulla base della documentazione prodotta dalla proponente e della descrizione del funzionamento dell'app ivi contenuta, non si ravvisano particolari rischi per la libertà e i diritti degli interessati.
Non vi è la possibilità di ricostruire i movimenti degli utenti, la lista dei loro contatti/incontri e nemmeno di acquisire in un unico punto le informazioni memorizzate nei diari clinici (destinate a rimanere sui dispositivi).
Queste caratteristiche rappresentano un punto di forza della soluzione proposta. Conseguentemente, se non indispensabile, si raccomanda di non implementare la funzione di geolocalizzazione che - al contrario - consentirebbe la raccolta dei dati sulla posizione degli interessati e, quindi, la ricostruzione dei loro movimenti con evidenti rischi per i diritti e libertà dei cittadini. Si precisa che anche ove la geocalizzazione rimanesse una opzione volontaria ed eventuale anche un'adesione minima espone a rischi di reidentificazione che andrebbero comunque apprezzati sia ai fini della tutela dei diritti e libertà fondamentali sia quale serio disincentivo all'adozione.
In ogni caso, vista la rilevanza e il numero di utenti che utilizzerebbero l'applicazione, si raccomanda di:

- effettuare robusti test di sicurezza informatica sull'applicazione prima del rilascio definitivo all'autorità pubblica;

- condurre una valutazione d'impatto ai sensi dell'art. 35 Reg. UE 2016/679.