# IMMUNI
# SISTEMA NAZIONALE DI CONTACT TRACING DIGITALE

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

Versione del 28 MAGGIO 2020
per la pubblicazione
emendata delle informazioni riservate relative
alla sicurezza del sistema

**IMMUNI**
**SISTEMA NAZIONALE DI CONTACT TRACING DIGITALE**

VALUTAZIONE DI IMPATTO SULLA PROTEZIONE DEI DATI PERSONALI

28 MAGGIO 2020

# INDICE

**EXECUTIVE SUMMARY**

Immuni è il sistema nazionale di contact tracing digitale finalizzato al contrasto della diffusione del virus Covid-19. Il sistema, formato dall'omologa applicazione mobile (app) e da tutte le componenti tecnologiche e organizzative che ne permettono il funzionamento, rileva sui dispositivi utente i contatti tra le persone in termini di distanza di prossimità e tempo attraverso tecnologia bluetooth, allo scopo di avvisare chi è entrato in contatto con un soggetto positivo al tampone Covid-19 ed elaborare statistiche ai fini di indagine epidemiologica su eventuali focolai territoriali.

Il progetto è stato studiato per minimizzare ogni impatto sulla protezione dei dati personali degli interessati, dei quali non tratta dati relativi all'identità o alla geolocalizzazione, in conformità al parere del Garante per la protezione dei dati personali [4] e alle previsioni del Dl 28 del 30 aprile 2020 [5]. In particolare:

- l'installazione dell'app è una libera scelta dell'interessato, senza alcuna forma di condizionamento e di disparità di trattamento;
- il trattamento è autorizzato dal Dl 28 del 30 aprile 2020 [5];
- agli interessati viene fornita adeguata informativa, anche in relazione alla pseudonimizzazione dei dati trattati e a quanto previsto dall'art. 6 del Dl 28 del 30 aprile 2020 [5];
- il codice sorgente dell'app è libero, aperto e rilasciato con licenza open source;
- il contact tracing è finalizzato esclusivamente al contenimento dei contagi e alla ricerca scientifica e statistica, nei termini previsti dal Regolamento e dal Dl 28 del 30 aprile 2020 [5];
- i dati raccolti sono strettamente necessari a fini di svolgere la funzione di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi e tutelarne la salute attraverso le previste misure di prevenzione nell'ambito delle misure di sanità pubblica legate all'emergenza COVID-19 prevista dall'art. 6 co. 1 e co. 2 lett. b) del DL 28 del 30 aprile 2020; salva la possibilità di utilizzo di dati in forma aggregata o comunque anonima, per soli fini di sanità pubblica, profilassi, statistici o di ricerca scientifica ai sensi dell'art.6 co. 3 del DL 28 del 30 aprile 2020;
- è stata effettuata la valutazione di conformità del sistema di allerta Covid-19 della app alle Linee guida dell'European Data Protection Board sulle app di contact tracing [15].

Per assicurare la riservatezza delle informazioni trattate e il pieno controllo dell'utente sui suoi dati, l'eventuale presenza di contatti con individui che hanno contratto il virus è verificato dall'app stessa sul singolo dispositivo. È cura dell'utente proteggere il dispositivo da accessi accidentali o illeciti da parte di terzi.

L'infrastruttura centrale registra gli invii dei dati pseudonimizzati generati randomicamente ogni 24 ore relativi a utenti positivi al tampone. L'infrastruttura centrale registra, altresì, al fine di consentire il miglioramento del modello di calcolo del rischio e quindi dell'efficacia del sistema nel notificare utenti a rischio, dati pseudonimizzati degli utenti che hanno avuto un contatto con un utente positivo.

L'invio di questi dati è su base volontaria, l'utente può decidere liberamente se inviare questi dati al fine di avvertire altri utenti a rischio di contagio. Inoltre, l'invio può avvenire solo se autorizzato da un operatore sanitario mediante la validazione di un codice OTP casuale visualizzato dal dispositivo.

Questi ultimi non contengono alcun legame con i dati dell'utente positivo, ma solamente la data dell'ultimo contatto e la provincia di domicilio.

Secondo il principio di privacy by default, Immuni tratta i dati minimi indispensabili per le sue finalità, pseudonimizzati. Tali dati sono conservati localmente e centralmente per 14 giorni, il periodo necessario ad assolvere le finalità del trattamento, e rimossi progressivamente. I dati sono conservati senza alcuna referenziazione. I dati ancora in vita alla fine dell'emergenza sanitaria o, al più tardi al 31 dicembre 2020, saranno cancellati.

In virtù delle tecniche di pseudonimizzazione e cifratura, dell'introduzione di rumore di fondo - invii di dati casuali per evitare l'identificabilità della persona tramite analisi del traffico dati dei dispositivi - e del breve ciclo di vita delle informazioni, la possibilità di risalire all'identità degli interessati comporterebbe l'utilizzo di sofisticate tecnologie oltre a un discreto dispendio di tempo. Tuttavia, per la delicatezza del progetto e l'appetibilità di azioni di disturbo finalizzate a inficiare l'iniziativa, non possono essere tralasciati tutti gli scenari di rischio per gli interessati che un trattamento su larga scala di dati sanitari, e quindi riferiti a soggetti particolarmente vulnerabili, porta in sé.

Come previsto dal parere del Garante per la protezione dei dati personali del 29 aprile [4] e dal successivo decreto legge del 30 aprile 2020 [5], il Ministero ha svolto una valutazione di impatto, riportata nel cap. 5 di questo documento. In conformità alla metodologia utilizzata per la protezione dei dati e la valutazione di impatto [8], i rischi stimati per i diritti e le libertà degli interessati sono stati ulteriormente arricchiti con le valutazioni inerenti alla perdita di riservatezza, integrità e disponibilità delle informazioni (cap. 6), portando quindi a prevedere un rischio intrinseco complessivo alto sulle minacce pertinenti (accesso, divulgazione, modifica, perdita e indisponibilità dei dati, illecite o accidentale) e la conseguente adozione di adeguate misure di sicurezza e la valutazione dei possibili rischi residui (cap. 7).

Le misure di protezione dell'infrastruttura tecnica di backend, ospitata presso il data center Sogei (cap. 8), completano le impostazioni di sicurezza sul trattamento nel suo complesso. L'allegato tecnico riporta i dettagli dell'app e dell'architettura del sistema.

**ACRONIMI E GLOSSARIO**

| | |
|---|---|
| API (Application Programming Interface) | Librerie di funzioni messe a disposizione dalle industrie informatiche che permettono ai programmatori di interagire con un programma o una piattaforma software. |
| App | L'applicazione mobile Immuni, comprensiva di codice sorgente, software, applicativi, tecnologie. |
| Autorità di controllo (o Autorità Garante) | L'autorità pubblica indipendente istituita da uno Stato membro ai sensi dell'art. 51 del GDPR. Per l'Italia è l'Autorità Garante per la protezione dei dati personali. |
| Backend | Il software, i sistemi e l'infrastruttura centrale necessari per il funzionamento dell'app |
| Comitato europeo per la protezione dei dati (*European Data Protection Board*) | Il gruppo di lavoro comune delle Autorità nazionali di vigilanza e protezione dei dati. Ha sostituito dal maggio 2018 il *Working Party article 29*. |
| GDPR o Regolamento | Regolamento europeo 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati. |
| Interessato | La persona fisica cui si riferiscono i dati personali. |
| Operatore Sanitario | Operatore Sanitario del Dipartimento della Prevenzione della ASL competente |
| OTP (One Time Password) | Password temporanea di 10 caratteri che può essere utilizzata una sola volta e scade dopo 2,5 minuti |

| | |
|---|---|
| Responsabile del trattamento | La persona fisica o giuridica, l'autorità pubblica o altro organismo che tratta dati personali per conto del Titolare del trattamento. |
| RPI (Rolling Proximity Identifier) | Identificativo di prossimità generato ogni 10 minuti da una chiave TEK |
| Servizio di autenticazione OTP | Il servizio reso disponibile dal sistema Tessera Sanitaria che consente all'operatore sanitario di validare l'invio al backend, attraverso l'app, dello stato di positività di un utente |
| TEK (Temporary Exposure Key) | Codice alfanumerico univoco generato randomicamente dall'app ogni 24 ore. |
| Valutazione di impatto o DPIA (*Data Protection* Impact *Assessment*) o | Le azioni che deve effettuare il Titolare quando «un tipo di trattamento […] può presentare un rischio elevato per i diritti e le libertà delle persone fisiche» (GDPR, art. 35). |
| *Working Party article 29* (o WP29), ora EDPB | Gruppo di lavoro comune delle Autorità nazionali di protezione dei dati istituito dalla direttiva europea 46/95. È stato sostituito nel 2018 dal Comitato europeo per la protezione dei dati (EDPB - *European Data Protection Board)*. |

# 1. DOCUMENTAZIONE CORRELATA

## 1.1 Riferimenti normativi

[1] Regolamento europeo 679/2016 relativo alla protezione delle persone fisiche con riguardo al trattamento dei dati personali nonché alla libera circolazione di tali dati.

[2] D.lgs. 30 giugno 2003, n. 196 e successive integrazioni e modificazioni

[3] WP 248 - Linee guida in materia di valutazione d'impatto sulla protezione dei dati e determinazione della possibilità che il trattamento possa presentare un rischio elevato ai fini del Regolamento Ue 2016/679

[4] Parere del Garante per la protezione dei dati personali sulla proposta normativa per la previsione di una applicazione volta al tracciamento dei contagi da Covid-19 – 29 aprile 2020

[5] Decreto legge 30 aprile 2020 n. 28 - Misure urgenti per la funzionalità dei sistemi di intercettazioni di conversazioni e comunicazioni, ulteriori misure urgenti in materia di ordinamento penitenziario, nonché disposizioni integrative e di coordinamento in materia di giustizia civile, amministrativa e contabile e misure urgenti per l'introduzione del sistema di allerta Covid-19

[6] Decreto del Presidente del Consiglio dei Ministri 26 marzo 2008 - Attuazione dell'articolo 1, comma 810, lettera c), della legge 27 dicembre 2006, n. 296, in materia di regole tecniche e trasmissione dati di natura sanitaria, nell'ambito del Sistema pubblico di connettività

[7] Decreto del Ministero dell'Economia e delle Finanze di concerto con il Ministero della Salute concernente la trasmissione dei dati dagli operatori sanitari per il tramite del sistema Tessera Sanitaria

### 1.2 Documentazione tecnica

[8] Metodologia per la protezione dei dati e per la valutazione di impatto, allegata all'atto di designazione di Sogei spa quale Responsabile del trattamento

[9] Immuni – Application Security Description, redatto dal gruppo di lavoro Immuni

[10] Immuni – High Level Description, redatto dal gruppo di lavoro Immuni

[11] Immuni – Privacy-Preserving Analytics, redatto dal gruppo di lavoro Immuni

[12] Immuni – Traffic Analysis Mitigation, redatto dal gruppo di lavoro Immuni

[13] Immuni – Technology Description, redatto dal gruppo di lavoro Immuni

[14] Immuni – Materiali DPIA, redatto dal gruppo di lavoro Immuni

[15] Immuni – Valutazione di conformità del sistema di allerta Covid-19 alle Linee guida dell'European Data protection Board sulle app di contact tracing (self-assessment)

[16] Immuni – MESSAGGIO App IMMUNI al Contatto Stretto

## 2. DESCRIZIONE GENERALE DEL SISTEMA DI CONTACT TRACING

Immuni è il sistema nazionale di contact tracing digitale formato dall'omologa app, dai relativi sistemi e componenti tecnologiche e organizzative che ne permettono il funzionamento (backend) e da un servizio di interazione con gli operatori sanitari veicolato dal sistema Tessera Sanitaria.

L'app Immuni si basa sulle API (*Application Programming Interface*) di contact tracing rese disponibili sui dispositivi con sistema iOS e Android dai fornitori Apple e Google per migliorare l'attuale tracciamento manuale dei contatti.

Dopo il download dell'app dagli store, vengono proposte all'utente una serie di schermate che illustrano il funzionamento e descrivono, come illustrato in Figura 1, quali dati non saranno trattati dall'app e quali invece saranno trattati e trasferiti all'infrastruttura centrale. Nella stessa schermata l'utente dichiara di avere almeno 14 anni e di aver letto l'informativa privacy. Durante questa procedura di *onboarding* l'app verifica la versione del sistema operativo installato ed eventualmente chiede di aggiornarlo, in base alle modalità di rilascio delle API di Apple e Google. Inoltre in questa fase l'app informa l'utente su quali siano i permessi necessari al suo funzionamento (Bluetooth, notifiche ed API di contact tracing) e ne richiede l'attivazione. Per completare il setup iniziale, l'app chiede di indicare la provincia in cui si trova l'utente, con la possibilità di cambiarla successivamente. Conoscere la provincia di domicilio dell'utente consente di rendere molto più utili i dati di analytics raccolti (in quanto analizzabili con una maggiore granularità geografica) e fornisce al Servizio Sanitario Nazionale informazioni essenziali per predisporre le risorse necessarie a prendere in carico gli utenti allertati.


**Figura 1.** Informativa privacy semplice visualizzata nella fase di onboarding.

Dopo la fase di *onboarding*, l'app inizia il suo lavoro in background generando ogni 24 ore in modo casuale una chiave temporanea (*Temporary Exposure Key* - TEK) diversa, dalla quale ogni 10 minuti vengono generati gli identificativi di prossimità (*Rolling Proximity Identifier* - RPI). Tali RPI vengono inviati in broadcast ai dispositivi raggiungibili via Bluetooth, producendo di fatto uno scambio di RPI tra i dispositivi.

In caso di esito positivo di un tampone, un operatore sanitario del Dipartimento di Prevenzione della ASL competente contatta il paziente per effettuare l'indagine epidemiologica, che prevede anche la verifica dell'installazione dell'app Immuni. Se il paziente ha installato l'app, l'operatore gli chiederà se voglia inviare le sue TEK al fine di allertare del rischio di contagio gli utenti con cui è entrato in contatto nei giorni

precedenti. Nel caso voglia procedere, l'operatore richiede all'utente di aprirla e di utilizzare la funzione di generazione del codice OTP (*One Time Password*). Il paziente comunica i 10 caratteri del codice OTP all'operatore e attende un'autorizzazione a procedere con l'upload delle proprie TEKs. L'operatore accede al sistema Tessera Sanitaria con le credenziali in suo possesso e, in virtù del particolare profilo attribuito, raggiunge la pagina web in cui inserisce il codice OTP, la data di inizio dei sintomi fornita dal paziente e risolve un captcha. Una volta cliccato il bottone, il sistema Tessera Sanitaria invia il codice al server di backend di Immuni, attivandolo per un tempo molto limitato (2,5 minuti), sufficiente al paziente per cliccare sul bottone di upload. A questo punto l'utente, tramite l'app, può inviare le TEKs che verranno memorizzate dopo aver verificato l'OTP all'*Exposure Ingestion Service*. La durata dell'intervallo di validità del codice OTP, così come la sua complessità, sono parametri calibrati per ridurre la finestra temporale di un eventuale attacco, mantenendo una sufficiente usabilità da parte degli utenti. Qualora l'intervallo temporale dovesse scadere, è possibile ripetere la medesima operazione con l'operatore. Errori di dettatura sono mitigati dalla presenza del check digit come ultimo carattere del codice OTP. Inoltre tale codice è generato su un alfabeto di 25 caratteri che esclude le principali ambiguità (il numero 0 e la lettera O ad esempio).

Una volta raccolte le TEKs di soggetti positivi, il server di Immuni impacchetta tali dati ogni 30 minuti (parametrizzabile) e li mette a disposizione di tutti i dispositivi degli utenti dell'app per il download.

Ogni istanza dell'app verifica l'esistenza di aggiornamenti all'incirca ogni 4 ore (la frequenza massima della verifica è parametrizzabile) ed effettua il download delle TEKs, avviando un confronto con gli RPI salvati localmente. Questo algoritmo che gira a livello locale può dar luogo a dei match che rappresentano un possibile contagio, in base a un grado di rischio calcolato sulla durata e sull'intensità del contatto. In caso di match, l'app invia una notifica locale al proprio possessore, avvertendolo che ha ricevuto un avviso in cui si comunica una possibile esposizione al contagio e invitandolo a contattare il proprio medico di medicina generale o il pediatra di libera scelta. Questo confronto e l'eventuale notifica che ne scaturisce costituiscono un processo locale al dispositivo e non coinvolgono il server di Immuni.

L'app invia periodicamente al server di Immuni (*Analytics Service*) alcune informazioni Questi dati includono alcuni indicatori tecnici di funzionamento dell'app, e precisamente lo stato di attivazione dei permessi necessari al corretto funzionamento, oltre alla provincia di domicilio, all'informazione se l'utente sia stato avvertito o meno di un contatto a rischio durante l'ultima procedura di scaricamento e controllo delle TEK e, in caso affermativo, il giorno (senza l'indicazione dell'orario) nel quale questo contatto è avvenuto. Questi dati sono inviati sia quando c'è stato un contatto a rischio che quando non c'è stato. Grazie a questi dati, il server di Immuni è in grado di capire statisticamente il livello di diffusione dell'app sul territorio e la correttezza del suo utilizzo. Inoltre, è possibile monitorare su base statistica l'epidemia, allocare in modo piu efficiente le risorse sanitarie e massimizzare quindi la prontezza e adeguatezza del supporto fornito agli utenti che risultano a rischio. Per far sì che i dati provengano da dispositivi validi e non compromessi, la soluzione in un primo momento sarà implementata solo sui dispositivi Apple, di cui si rileva l'integrità mediante Device Check technology (cfr. [11]). Gli utenti vengono informati dell'invio dei dati (Analytics Service) al server di Immuni sia nell'informativa sul trattamento dei dati personali ai sensi dell'art. 13 relativa alla app che, successivamente, nel caso in cui ci sia stato un contatto a rischio con una modalità chiara e trasparente.

Allo scopo di limitare la possibilità di inferire informazioni associabili ad una pseudo-identità dell'utente, e per limitare l'efficacia di tecniche di traffic analysis in generale (es. su larga scala, da parte di chi ha accesso al backbone Internet), è prevista l'introduzione di rumore di fondo basato sull'invio di dati casuali, in accordo a quanto indicato dalle principali proposte di sistemi di contact tracing decentralizzato. In particolare:

- l'app contatta il servizio *Exposure Ingestion Service* (cfr. Allegato tecnico), sia con dati validi (quando necessario) che con dati casuali, successivamente scartati dal backend. In questo modo, l'osservazione del traffico tra un client ed uno specifico indirizzo IP del backend non è sufficiente ad inferire informazioni relative all'utente;
- l'app invia una certa quantità di informazioni casuali al servizio *Analytics Service* (cfr. Allegato tecnico) per finalità analoghe a quelle riportate al punto precedente.

Per approfondimenti tecnici sull'app e sull'architettura del sistema si rimanda all'Allegato tecnico e ai documenti [9], [10], [11], [12], [13].

### 2.1 Verifica dell'integrità dei dati di analytics con tecnologia DeviceCheck

Ai fini di garantire che i dati inviati all'*Analytics Service* siano validi, senza tuttavia ricorrere all'autenticazione del client, si fa ricorso (limitatamente ai dispositivi iOS) a DeviceCheck, una tecnologia messa a disposizione da Apple. I dispositivi Android non inviano invece dati all'*Analytics Service*.

DeviceCheck permette di verificare che la comunicazione ricevuta dal server provenga da un dispositivo Apple autentico. Si compone di due parti: un'API client e un'API server. Un'app che intenda utilizzare DeviceCheck può richiedere all'API client un "device token", ovvero una stringa casuale che cambia ogniqualvolta l'API client viene contattata. Il server può usare il device token inviato dal client per effettuare tre operazioni:

1. Verificare che il device token sia stato generato da un dispositivo Apple autentico.
2. Leggere il valore di due bit che DeviceCheck associa al dispositivo e il mese e anno in cui i bit sono stati modificati per l'ultima volta.
3. Impostare il valore dei bit.

Il sistema è stato concepito per garantire la privacy degli utenti, infatti:

- Dal device token non si può estrarre alcuna informazione che possa identificare un dispositivo
- Il device token cambia ogni volta che viene richiesto all'API client e non può quindi essere usato per reidentificare lo stesso dispositivo.
- L'informazione che il server può decidere di associare ad un certo dispositivo è limitata a due bit, insufficienti quindi per salvare un identificativo univoco.

Forniamo di seguito una spiegazione semplificata, che però contempla tutte le componenti e i flussi dati, della strategia con cui il sistema garantisce che:

1. L'*Analytics Service* accetti solo dati provenienti da dispositivi autentici Apple.
2. Lo stesso dispositivo autentico non possa effettuare più di due invii al mese.

Il secondo punto impedisce che un attaccante possa inviare un quantitativo considerevole di informazione per inquinare i dati presenti sull'*Analytics Service*.

La strategia si compone di due parti, la generazione da parte dell'app di un *analytics token* effimero che varia una volta al mese e l'invio grazie ad esso dei dati.

All'installazione dell'app, e successivamente in corrispondenza della prima riattivazione dell'app nel mese, l'app genera un analytics token (una stringa randomica), la salva nel dispositivo, elimina un'eventuale

stringa precedentemente generata e invia all'*Analytics Service* il device token e l'analytics token. Alla ricezione dei dati, l'*Analytics Service* controlla la data in cui i bit sono stati modificati l'ultima volta. Se i bit non sono mai stati modificati o se la modifica è avvenuta in un mese precedente a quello attuale, il server imposta i due bit nella configurazione (0, 0) e salva l'analytics token nel database assieme al mese e anno correnti e a un contatore di invii inizialmente impostato a zero.

Quando il dispositivo sta per effettuare un invio all'*Analytics Service*, assieme ai dati invia l'analytics token generato in precedenza. Il server controlla se l'analytics token esiste, se è stato generato nel mese corrente e se non è già stato utilizzato per effettuare due invii. Se tutte queste condizioni sussistono, i dati di analytics vengono accettati e salvati nel database e il contatore viene incrementato di uno per registrare l'avvenuta ricezione. In caso contrario i dati vengono ignorati.

La privacy dell'utente è garantita come segue:

- L'analytics token cambia con cadenza mensile.
- Lo stesso analytics token viene inviato al server al massimo tre volte nel corso di un mese (la prima quando viene creato, le altre due per validare gli invii di dati), limitando quindi di molto la capacità del server di reidentificare lo stesso dispositivo a cavallo di più chiamate al server.
- L'analytics token viene cifrato prima di essere salvato nella memoria del dispositivo, impedendo che un attaccante che entri in possesso del dispositivo dell'utente possa accedervi.
- Nessun dato particolare viene inviato ad Apple, nemmeno in forma implicita. La comunicazione del device token di un dispositivo al sistema DeviceCheck avviene mensilmente per tutti i dispositivi su cui l'app è attiva indipendentemente dall'invio dati che verrà o meno effettuato nel corso del mese.

L'implementazione effettiva varia leggermente da quella semplificata spiegata sopra perché, per evitare uno picco di contatti al server all'inizio del mese, la generazione dell'analytics token avviene in un momento del mese scelto casualmente da ogni dispositivo. Per supportare questo accorgimento, l'analytics token può avere una validità massima di due mesi.

Il sistema prescelto non invia alcuna informazione sensibile al server Apple che gestisce il sistema DeviceCheck. DeviceCheck viene infatti usato soltanto per la validazione dell'analytics token, operazione che avviene per tutti i dispositivi indistintamente al massimo una volta al mese.

Per una trattazione più dettagliata dell'argomento si rimanda al documento [11].

### 2.2 Modello di rischio

Il sistema di Apple e Google mette a disposizione un algoritmo per il calcolo di un coefficiente di rischio. L'algoritmo è descritto nella documentazione ufficiale. Ne riportiamo una descrizione semplificata.

I due dati più importanti che l'algoritmo mette a disposizione sono la durata di un'esposizione e il valore medio dell'attenuazione del segnale durante l'esposizione stessa. Non potendo lo smartphone rilevare direttamente la distanza con un altro dispositivo, occorre usare l'attenuazione come surrogato della distanza.

Il fattore di rischio viene valutato sulla base dei dati di cui sopra nel modo seguente:

- per ogni dato, individua il parametro corrispondente al valore rilevato; e
- moltiplica i parametri individuati per ogni dato tra loro per ottenere il fattore di rischio.

***Durata***

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| D1 | D2 | D3 | D4 | D5 | D6 | D7 | D8 |
| 0 min | 0-5 min | 5-10 min | 10-15 min | 15-20 min | 20-25 min | 25-30 min | 30+ min |

***Attenuazione***

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| A1 | A2 | A3 | A4 | A5 | A6 | A7 | A8 |
| > 73 dBm | 73-63 dBm | 63-51 dBm | 51-33 dBm | 33-23 dBm | 23-15 dBm | 15-10 dBm | <= 10 dBm |

Nell'esempio rappresentato dalla tabella, l'esposizione è durata tra i 15 e i 20 minuti e l'attenuazione è stata compresa tra i 10 e i 15 dBm. In questo caso il fattore di rischio sarà:

Fattore di rischio = D5 x A7

Una volta determinato il fattore di rischio, l'app lo confronta con una soglia minima di rischio concordata con il Ministero della Salute. Se il fattore di rischio supera quella soglia, l'utente viene avvisato del potenziale rischio, altrimenti non accade nulla.

Fattore di rischio > Soglia di rischio

I parametri da definire sono quindi 17 (D1-D8, A1-A8 e soglia di rischio). D1-D8 e A1-A8 possono assumere solo valori interi da 0 a 8. È attualmente in corso una procedura di calibrazione con la finalità di trasformare le indicazioni del Ministero della Salute (avvisare persone che sono state in contatto a meno di 2 metri per 15 minuti o più con un COVID-19 positivo) nei suddetti parametri.

Se si vogliono ad esempio escludere completamente esposizioni durate meno di 15 minuti, come da indicazioni del Ministero della Salute, basterà associare a D1, D2, D3 e D4 il valore più basso possibile, ossia 0.

Per migliorare la calibrazione del modello di rischio in futuro ci si potrà avvalere delle seguenti strade:

- Effettuare ulteriori esperimenti di calibrazione, riproducendo situazioni reali e misurando i valori di durata e attenuazione rilevati dal sistema.
- Analizzare i dati epidemiologici, ovvero i dati di contatto con altri soggetti positivi (intensità, durata e data) raccolti contestualmente alle TEK.

### 2.3 Flussi dati

Per agevolare la comprensione del sistema e la lettura del documento indichiamo di seguito i flussi di dati, specificando quando avvengono e quali dati vengono scambiati . Si precisa che nel contesto delle comunicazioni client-server viene inviato l'indirizzo IP del dispositivo. L'indirizzo non viene memorizzato ed è usato ai soli fini di instaurare una connessione. Per una descrizione puntuale delle tipologie di dati si rimanda alla sezione 4.3.

**Download di Configuration Settings**

I Configuration Settings sono parametri che permettono di modificare il funzionamento dell'app senza dover rilasciare una nuova versione sugli store. A titolo esemplificativo, i parametri del modello di rischio possono essere modificati ricorrendo ai configuration settings. Questi dati vengono richiesti dal dispositivo al server (*App Configuration Service*) ogni volta che l'app inizia un processo di background.

**Download di TEKs**

Per consentire all'app di confrontare le TEKs caricate da utenti diagnosticati positivi con gli RPI salvati localmente, l'app scarica le TEKs dal server (*Exposure Reporting Service*) ogni volta che l'app inizia un processo di background.

**Download di FAQ**

L'app offre una sezione con risposte esaustive alle domande più frequenti per l'utilizzo dell'applicazione. Affinché domande e risposte siano sempre aggiornate, l'app richiede le FAQ ogni volta che inizia un processo di background.

**Accesso a informativa privacy e termini di utilizzo**

L'app permette di accedere a informativa privacy e termini di utilizzo sia durante il processo di onboarding, sia dal menù Impostazioni. Quando l'utente desidera visualizzare questi documenti, un file HTML unico e senza dipendenze esterne viene scaricato dal server.

**Dettatura OTP**

Quando un utente diagnosticato positivo esprime la volontà di caricare le sue TEKs, detta un codice alfanumerico di 10 cifre (OTP) all'operatore sanitario in connessione telefonica.

**Inserimento OTP**

L'operatore sanitario inserisce il codice OTP e la data di inizio sintomi nell'interfaccia web di Tessera Sanitaria, o in un sistema informativo regionale che si interfaccia con quello di Tessera Sanitaria. A sua volta, Tessera Sanitaria inoltra i dati al server (*OTP Service*). I dati inviati sono:

- Data di inizio dei sintomi
- Codice OTP

**Validazione OTP**

Dopo aver dettato l'OTP all'operatore sanitario e aver ricevuto da quest'ultimo la conferma che il codice è stato inserito nel sistema, l'utente preme un bottone che fa partire una richiesta di validazione dell'OTP dall'app nei confronti del server (*Exposure Ingestion Service*). Nel caso in cui l'OTP sia valido, il server risponde positivamente.

**Upload delle TEK**

Se l'OTP è stato validato, l'utente può procedere al caricamento volontario delle sue TEKs. Una volta che l'utente dà la conferma, i seguenti dati vengono trasmessi

- Codice OTP

- Chiavi temporanee (TEK)
- Clock del device
- Provincia di domicilio
- Dati epidemiologici (se presenti)

**Generazione dell'analytics token (lato client)**

Su base mensile tutti i dispositivi senza distinzione generano casualmente un analytics token necessario a verificare la validità dei dati di analytics inviati. Per l'autorizzazione di un nuovo token, il dispositivo invia automaticamente al server con frequenza non superiore a una volta al mese:

- Device check token
- Analytics token

**Validazione device check token (lato server)**

Per autorizzare il nuovo analytics token, il server (*Analytics Service*) invia all'API DeviceCheck di Apple il device check token ricevuto dall'app. L'unico dato inviato ad Apple, con frequenza non superiore a una volta al mese, è:

- Device check token

**Upload dei dati di analytics**

Successivamente allo scaricamento delle TEK e al confronto con le RPI salvate localmente, il dispositivo può (l'invio avviene su base probabilistica) inviare automaticamente al server le seguenti informazioni:

- Analytics token
- Provincia di domicilio
- Stato del Bluetooth
- Permesso per l'utilizzo del sistema Apple/Google
- Permesso per le notifiche
- Sistema operativo del dispositivo
- Ricezione o non di notifica di esposizione
- Data in cui è avvenuta l'ultima esposizione a rischio

**Upload di dummy analytics**

Per offuscare le informazioni a cui un attaccante potrebbe risalire a partire dall'analisi del traffico crittografato dal dispositivo al server (*Analytics Service*), il client invia, seguendo una programmazione probabilistica, rumore di fondo al server. Si tratta di rumore proprio perché l'informazione contenuta è nulla. Il rumore può essere inviato automaticamente da tutti i dispositivi, indifferentemente.

**Upload di dummy TEKs**

Per offuscare le informazioni a cui un attaccante potrebbe risalire a partire dall'analisi del traffico crittografato dal dispositivo al server (*Exposure Ingestion Service*), il client invia, seguendo una programmazione probabilistica, rumore di fondo al server. Si tratta di rumore proprio perché l'informazione contenuta è nulla. Il rumore può essere inviato automaticamente da tutti i dispositivi, indifferentemente.

## 3. FASE DI SPERIMENTAZIONE

Il Ministero della Salute ha convocato dapprima gli assessori regionali alla salute e i direttori generali degli Uffici regionali competenti in materia sanitaria e, successivamente, i referenti regionali per le attività di prevenzione e per i sistemi informativi sanitari, per un esame congiunto delle questioni attinenti all'inserimento del sistema di tracciamento digitale nelle attività di prevenzione e assistenza espletate dai servizi regionali.

In tali incontri, tutte le Regioni hanno accolto positivamente l'adozione di una app nazionale di contact tracing rappresentando l'esigenza condivisa di una preliminare fase di sperimentazione del processo di contact tracing digitale in un numero limitato di Regioni o Province autonome che rappresentino le diverse realtà territoriali del Paese, al fine di verificarne il buon funzionamento da un punto di vista tecnico (applicazione digitale delle euristiche epidemiologiche) e l'impatto sui servizi territoriali, in considerazione del possibile ulteriore carico di lavoro (contact tracing, individuazione, isolamento/quarantena, diagnostica, sorveglianza) derivante dalla diffusione del nuovo strumento digitale, il quale presumibilmente aumenterà la sensibilità del sistema rivelando anche contatti non rilevabili con le modalità tradizionali di contact tracing.

Al riguardo, è stata ritenuta congrua la durata di almeno una settimana della fase di sperimentazione, da svolgersi nelle Regioni o Province autonome che saranno individuate dai decisori politici nazionali e regionali.

Per realizzare la preventiva sperimentazione, l'app Immuni, non potendo essere rilasciata soltanto in zone limitate del Paese, sarebbe rilasciata a livello mondiale scaricabile da App Store, Google Play e, in prospettiva, anche dallo store di Huawei (l'app sarà pubblicata attraverso gli account del Ministero della Salute su questi store), ma inizialmente dovrebbe consentire l'utilizzo codice di sblocco OTP esclusivamente nelle Regioni o Province autonome incluse nella sperimentazione.

Pertanto, tutti i cittadini potrebbero, dal momento del rilascio, scaricare l'app dai suddetti store, ma dovrebbero essere preventivamente avvertiti che l'avviso di esposizione al rischio di contagio potrà pervenire soltanto se il contatto è avvenuto con soggetti risultati positivi al Covid-19 assistiti dalle Regioni o Province autonome deputate alla sperimentazione (ciò potrà essere indicato con apposito avviso nell'app store).

## 4. SPECIFICHE DEL TRATTAMENTO

### 4.1 Caratteristiche del trattamento

La tabella seguente riassume le caratteristiche principali del trattamento Immuni.

| Caratteristica | Descrizione |
|---|---|

| | |
|---|---|
| **Descrizione del trattamento** | Sistema nazionale di contact tracing digitale |
| **Titolare del trattamento** | Ministero della Salute |
| **Responsabili del trattamento** | Sogei spa, Via Mario Carucci 99, 00143 Roma |
| **Tipo di trattamento** | Informatizzato |
| **Base giuridica** | Esecuzione di un compito di interesse pubblico per esigenze di sanità pubblica in base al DI 28 del 29 aprile 2020 |
| **Finalità** | ● Allerta delle persone che sono entrate in contatto con soggetti risultati positivi al tampone Covid-19 e tutela della salute.<br>● Sanità pubblica, profilassi, statistica o ricerca scientifica |
| **Categorie di interessati** | Soggetti che hanno installato su base volontaria l'applicazione mobile Immuni e che abbiano dichiarato di aver compiuto il quattordicesimo anno di età |
| **Categorie di destinatari** | I dati non vengono comunicati a soggetti terzi. |
| **Trasferimenti dati extra Ue** | I dati non sono trasferiti in Paesi extra Ue |

### 4.2 Componenti del trattamento

Il trattamento si articola in tre componenti informatizzate, con caratteristiche diverse, che interagiscono tra loro:

- **app**, l'applicazione mobile comprensiva di codice sorgente, software, applicativi e tecnologie
- **backend**, il software, i sistemi e l'infrastruttura centrale necessari per il funzionamento del'app

- **servizio di autenticazione OTP**, il servizio reso disponibile dal sistema Tessera Sanitaria le cui modalità operative sono descritte nel Decreto del Ministero dell'Economia e delle Finanze adottato di concerto con il Ministero della Salute ([7], che consente all'operatore sanitario di validare l'invio al backend, attraverso l'app, dello stato di positività di un utente

Tutte le componenti sono gestite interamente da Sogei spa, in qualità di Responsabile del trattamento per l'erogazione delle attività previste dall'art. 6 comma 5 del Dl 28 del 29 aprile 2020 [5].

Per garantire disponibilità e resilienza del sistema, l'esposizione delle chiavi temporanee relative agli utenti risultati positivi al tampone Covid-19 viene effettuata attraverso fornitori di servizi di Content Delivery Network (CDN) che saranno designati sub-Responsabili del trattamento da Sogei. Sogei, infatti, è autorizzata dal Ministero della Salute a designare ai sensi dell'art. 28 del Regolamento i fornitori quali sub-Responsabili del trattamento.

Le TEK vengono scaricate dalle app installate sui dispositivi più volte al giorno allo scopo di verificare un eventuale match tra le chiavi registrate dal dispositivo e quelle pubblicate dalla piattaforma attraverso la CDN (cfr. [14] e cap. 2). L'esposizione dei dati è coerente con quanto prescritto dal Dl [5] (art. 6, comma 2, lett. c).

### 4.3 Dati trattati e loro conservazione

Immuni è stato progettato per trattare i dati minimi indispensabili relativamente alla finalità di allertare le persone che siano entrate in contatto stretto con soggetti risultati positivi al tampone Covid-19, tutelare la salute ed elaborare statistiche ai fini di sanità pubblica per rilevare eventuali focolai territoriali.

In particolare, i dati trattati sono:

***Dati comuni***

**Indirizzo IP del dispositivo** sul quale è installata l'app

- Categorie di interessati: tutti gli utenti dell'applicazione
- Modalità e momento della raccolta: ad ogni connessione del dispositivo verso il backend
- Eventuale trasferimento al back-end: non è applicabile perché non è trasferito al server di backend
- Modalità (trigger) di trasferimento: il dato viene acquisito solamente dagli apparati di sicurezza perimetrale
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1).
- Successivi trattamenti: nessuno
- Modalità di conservazione: il dato non perviene allo strato applicativo
- Modalità di aggregazione: il dato non perviene allo strato applicativo
- Modalità di anonimizzazione/pseudonimizzazione: il dato non perviene allo strato applicativo
- Tempo di cancellazione locale: nessuna retention (non viene memorizzato)
- Tempo di cancellazione remota: nessuna retention
- Finalità: l'unica finalità è di rendere la comunicazione tra client e server possibile. L'indirizzo IP non viene salvato sui sistemi di backend ma solo tracciato dagli apparati di sicurezza perimetrale. Il trattamento del dato risponde quindi a una finalità meramente tecnica.

**Chiavi temporanee (TEK) degli utenti**, ossia chiavi crittografiche univoche e completamente casuali generate dall'app ogni 24 ore per creare gli identificativi di prossimità

- Categorie di interessati: utenti diagnosticati positivi
- Modalità e momento della raccolta: la generazione locale avviene quotidianamente tramite il Framework Apple/Google, vengono inviate al server al momento in cui un utente diagnosticato positivo procede all'upload sul server di backend
- Eventuale trasferimento al back-end: si
- Modalità (trigger) di trasferimento: invio volontario al server da parte di un utente diagnosticato positivo, previa validazione dell'operatore sanitario
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1)
- Successivi trattamenti: pubblicazione tramite CDN al fine di alerting ai soggetti a rischio
- Modalità di conservazione: memorizzazione in DataBase
- Modalità di aggregazione: i dati non saranno oggetto di aggregazione
- Modalità di anonimizzazione/pseudonimizzazione: i dati vengono dissociati dall'indirizzo IP e quindi non sono referenziati/referenziabili a un utente
- Tempo di cancellazione locale: dopo 14 giorni
- Tempo di cancellazione remota: dopo 14 giorni
- Finalità: sul dispositivo dell'utente le TEK permettono di ottenere, mediante procedura crittografica, gli RPI, ovvero gli identificativi di prossimità scambiati dai device. Quando vengono caricate da un utente diagnosticato positivo, le TEK permettono a ogni dispositivo nel sistema di rilevare un'esposizione a rischio. Il trattamento del dato risponde quindi alla finalità di rendere possibile la verifica della condizione di "avvenuto contatto" e di consentire il funzionamento del sistema di alert.

**Identificativi di prossimità (RPI)**: identificatori di prossimità di altri dispositivi che si sono trovati nelle vicinanze usati per la trasmissione/ricezione tra dispositivi degli utenti mediante tecnologia Bluetooth Low Energy

- Categorie di interessati: tutti gli utenti dell'applicazione
- Modalità e momento della raccolta: generate giornalmente sul dispositivo dell'utente, con validità di 10 minuti
- Eventuale trasferimento al back-end: no
- Modalità (trigger) di trasferimento: dato non trasferito
- Soggetti autorizzati: Non applicabile (NA) in quanto il dato rimane esclusivamente sui dispositivi degli utenti
- Successivi trattamenti: NA in quanto il dato rimane esclusivamente sul dispositivo dell'utente
- Modalità di conservazione: il dato è conservato esclusivamente in locale sul dispositivo dell'utente
- Modalità di aggregazione: NA in quanto il dato rimane esclusivamente sul dispositivo dell'utente
- Modalità di anonimizzazione/pseudonimizzazione: NA in quanto il dato rimane esclusivamente sul dispositivo dell'utente
- Tempo di cancellazione locale: dopo 14 giorni
- Tempo di cancellazione remota: NA
- Finalità: sul dispositivo dell'utente gli RPI vengono confrontati con le TEK caricate da utenti diagnosticati positivi per identificare eventuali match e allertare gli utenti a rischio. Il trattamento del dato risponde quindi alla finalità di rendere possibile la verifica della condizione di "avvenuto contatto" e di consentire il funzionamento del sistema di alert.

**Codice OTP** generato dall'app per permettere all'operatore sanitario di convalidare la segnalazione di positività di un utente

- Categorie di interessati: utenti diagnosticati positivi
- Modalità e momento della raccolta: generato dall'applicazione su richiesta dell'utente diagnosticato positivo che vuole caricare le proprie TEK sul server
- Eventuale trasferimento al back-end: sì
- Modalità (trigger) di trasferimento: comunicato all'operatore sanitario da un utente diagnosticato positivo; l'operatore sanitario poi lo invia al server
- Soggetti autorizzati: operatori sanitari e personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1).
- Successivi trattamenti: nei 2.5 minuti successivi all'invio dell'OTP al backend da parte dell'operatore sanitario
- Modalità di conservazione: in forma cifrata
- Modalità di aggregazione: NA
- Modalità di anonimizzazione/pseudonimizzazione: NA
- Tempo di cancellazione locale: NA
- Tempo di cancellazione remota: dopo 2.5 minuti dall'invio al server
- Finalità: validare che le TEK provengano dal dispositivo di un utente diagnosticato positivo, evitando quindi che chiunque possa caricare le proprie TEK, creando falsi allarmi. Il trattamento del dato risponde quindi alla finalità di rendere possibile la verifica della condizione di "avvenuto contatto" e di consentire il funzionamento del sistema di alert in condizioni di sicurezza.

**Provincia di domicilio**

- Categorie di interessati: tutti gli utenti dell'applicazione
- Modalità e momento della raccolta: dato immesso dall'utente al momento del primo avvio dell'applicazione
- Eventuale trasferimento al back-end: sì
- Modalità (trigger) di trasferimento: invio al server durante il processo di invio dati dell'utente diagnosticato positivo e/o di invio dati di analytics da parte di utenti entrati in contatto stretto con un utente positivo e/o di invio mensile di dati di analytics da parte degli utenti
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1).
- Successivi trattamenti: conservazione e utilizzo come criterio di aggregazione
- Modalità di conservazione: memorizzazione in DataBase
- Modalità di aggregazione: esso stesso è criterio di aggregazione
- Modalità di anonimizzazione/pseudonimizzazione: il dato viene dissociato dall'indirizzo IP e quindi non è referenziato/referenziabile ad un utente
- Tempo di cancellazione locale: contestualmente alla disinstallazione dell'applicazione
- Tempo di cancellazione remota: cessazione dello stato di emergenza e comunque non oltre il 31/12/2020
- Finalità: scomporre i dati di analytics su base geografica per consentire al Servizio Sanitario Nazionale di allocare le risorse necessarie. Il trattamento del dato risponde quindi anche a finalità di tutela della salute pubblica e, in particolare, a finalità di carattere epidemiologico.

**Analytics token (solo iOS)**

- Categorie di interessati: tutti gli utenti dell'applicazione con dispositivi iOS
- Modalità e momento della raccolta: generato sul dispositivo mediamente ogni 30 giorni
- Eventuale trasferimento al back-end: sì

- Modalità (trigger) di trasferimento: invio al server durante ogni caricamento di dati di analytics per validare l'invio e prevenire il rischio di inquinamento dei dati
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1).
- Successivi trattamenti: il dato è usato esclusivamente per validare l'invio di dati di analytics
- Modalità di conservazione: in forma criptata
- Modalità di aggregazione: NA
- Modalità di anonimizzazione/pseudonimizzazione: il dato viene dissociato dall'indirizzo IP e quindi non è referenziato/referenziabile ad un utente
- Tempo di cancellazione locale: dopo 2 mesi
- Tempo di cancellazione remota: dopo 2 mesi
- Finalità: per validare l'invio al server di dati di analytics e per imporre un limite mensile di invio volto a evitare l'inquinamento dei dati. Il trattamento del dato risponde quindi a una finalità meramente tecnica strumentale a garantire sicurezza e maggior affidabilità dei dati trattati.

**Device check token (solo iOS)**

- Categorie di interessati: tutti gli utenti dell'applicazione con dispositivi iOS
- Modalità e momento della raccolta: codice randomico generato ex novo ad ogni cambio di analytics token (in media una volta al mese)
- Eventuale trasferimento al back-end: sì (inviato per verifica anche al server Device Check di Apple)
- Modalità (trigger) di trasferimento: invio al momento dell'autorizzazione del nuovo analytics token (in media una volta al mese)
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1).
- Successivi trattamenti: il dato è usato esclusivamente per validare l'autorizzazione di un nuovo analytics token
- Modalità di conservazione: il dato non viene conservato
- Modalità di aggregazione: NA
- Modalità di anonimizzazione/pseudonimizzazione: il dato viene dissociato dall'indirizzo IP e quindi non è referenziato/referenziabile ad un utente
- Tempo di cancellazione locale: dato non memorizzato
- Tempo di cancellazione remota: dato non memorizzato
- Finalità: per validare l'invio al server di dati di analytics e per imporre un limite mensile di invio volto a evitare l'inquinamento dei dati. Il trattamento del dato risponde quindi a una finalità meramente tecnica strumentale a garantire sicurezza e maggior affidabilità dei dati trattati.

***Dati particolari***

**Data di inizio dei sintomi** (per persone positive al tampone)

- Collocazione del dato: sul server di backend
- Categorie di interessati: utenti diagnosticati positivi a COVID-19
- Modalità e momento della raccolta: dato fornito al momento in cui l'utente diagnosticato positivo carica le proprie TEK sul server
- Eventuale trasferimento al back-end: NA
- Modalità (trigger) di trasferimento: NA

- Soggetti autorizzati: operatori sanitari e personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1)
- Successivi trattamenti: conservazione e utilizzo come criterio di aggregazione
- Modalità di conservazione: memorizzato nel database
- Modalità di aggregazione: esso stesso è criterio di aggregazione
- Modalità di anonimizzazione/pseudonimizzazione: il dato viene dissociato dall'indirizzo IP e quindi non e' referenziato/referenziabile ad un utente
- Tempo di cancellazione locale: cessazione dello stato di emergenza e comunque non oltre il 31/12/2020
- Tempo di cancellazione remota: cessazione dello stato di emergenza e comunque non oltre il 31/12/2020
- Finalità: per rendere disponibili agli altri dispositivi solo ed esclusivamente le TEK relative ai giorni in cui l'utente diagnosticato positivo era contagioso, evitando di allertare utenti in modo immotivato. Il trattamento del dato risponde quindi anche a finalità di tutela della salute pubblica e, in particolare, a finalità di carattere epidemiologico.

**Data in cui è avvenuta l'ultima esposizione a rischio**:

- Collocazione originaria del dato: sul dispositivo dell'utente
- Categorie di interessati: utenti entrati in contatto stretto con un positivo
- Modalità e momento della raccolta: valore memorizzato nel caso venga riscontrato un contatto con un utente positivo
- Eventuale trasferimento al back-end: sì
- Modalità (trigger) di trasferimento: invio al server durante il processo di invio dati di analytics da parte di utenti entrati in contatto stretto con un utente positivo
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1).
- Successivi trattamenti: conservazione e utilizzo come criterio di aggregazione
- Modalità di conservazione: memorizzazione nel database
- Modalità di aggregazione: esso stesso è criterio di aggregazione
- Modalità di anonimizzazione/pseudonimizzazione: il dato viene dissociato dall'indirizzo IP e quindi non è referenziato/referenziabile ad un utente
- Tempo di cancellazione locale: dato dinamico, il valore non può avere una vita superiore ai 14 giorni
- Tempo di cancellazione remota: cancellazione al momento della dismissione del progetto (31/12/2020 al più tardi)
- Finalità: fornire all'utente informazioni utili per la tutela della salute sua e altrui nonché all'adozione di adeguate misure di prevenzione da parte del Servizio Sanitario regionale competente. Il trattamento del dato risponde quindi anche a finalità di tutela della salute pubblica e, in particolare, a finalità di carattere epidemiologico.

**Ricezione notifica di esposizione**

- Collocazione originaria del dato: sul dispositivo dell'utente
- Categorie di interessati: utenti dell'app

- Modalità e momento della raccolta: impostato a "vero" nel momento in cui l'utente riceve la notifica di essere stato a contatto stretto con un contagiato
- Eventuale trasferimento al back-end: sì
- Modalità (trigger) di trasferimento: invio al server al momento in cui il dispositivo di un utente scarica le nuove TEK e le confronta con gli RPI memorizzati sul dispositivo
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1)
- Successivi trattamenti: conservazione e aggregazione
- Modalità di conservazione: memorizzazione su DataBase
- Modalità di aggregazione: aggregazione del dato su base geografica (provincia di domicilio) e su base temporale
- Modalità di anonimizzazione/pseudonimizzazione: il dato viene dissociato dall'indirizzo IP e quindi non è referenziato/referenziabile ad un utente
- Tempo di cancellazione locale: trascorsi 14 giorni dall'avvenuta ricezione della notifica
- Tempo di cancellazione remota: cessazione dello stato di emergenza e comunque non oltre il 31/12/2020
- Finalità: per fornire al Ministero della Salute il numero di utenti allertati dall'app (eventualmente anche su base provinciale, incrociando il dato geografico) consentendo l'allocazione di risorse in modo da tutelare la salute degli utenti allertati. Il trattamento del dato risponde quindi a finalità di tutela della salute pubblica e, in particolare, a finalità di carattere epidemiologico.

**Exposure Summary[1] ed Exposure Info[2]** (Dati epidemiologici) - cap. 2 del documento [14] e documento [11]:

- Collocazione originaria del dato: sul dispositivo dell'utente
- Categorie di interessati: utenti diagnosticati positivi a COVID-19
- Modalità e momento della raccolta: valore memorizzato nel caso venga riscontrato un contatto con un utente positivo
- Eventuale trasferimento al back-end: sì
- Modalità (trigger) di trasferimento: invio al server durante il processo di invio dati dell'utente diagnosticato positivo
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1).
- Successivi trattamenti: conservazione ed elaborazione
- Modalità di conservazione: memorizzazione in DataBase
- Modalità di aggregazione: aggregazione sulla base di criteri temporali e di prossimità

[1] Per *Exposure Summary* si intende il compendio sintetico del numero di contatti a rischio verificati, i giorni trascorsi dall'ultimo contatto a rischio, la durata aggregata degli episodi di contatto a rischio e l'indice di rischio più elevato tra quelli relativi ai contatti a rischio.
(https://developer.apple.com/documentation/exposurenotification/enexposuredetectionsummary).

[2] Per *Exposure Info* si intende, per ogni singolo utente contagiato con cui si è venuti in contatto: data dell'evento di contatto, durata del contatto - in multipli di 5 minuti fino ad un massimo di 30 - stima della distanza tra i dispositivi durante il contatto, distribuzione statistica della durata dei contatti aggregata per tre livelli di distanza, rischio di contagiosità, indice di rischio totale per i contatti avvenuti col singolo utente.
(https://developer.apple.com/documentation/exposurenotification/enexposureinfo).

- Modalità di anonimizzazione/pseudonimizzazione: i dati vengono disassociati dall'indirizzo IP e quindi non sono referenziati/referenziabili ad un utente
- Tempo di cancellazione locale: trascorsi 14 giorni
- Tempo di cancellazione remota: cessazione dello stato di emergenza e comunque non oltre il 31/12/2020
- Finalità: per consentire l'affinamento dell'algoritmo di calcolo del rischio derivante da un contatto e allertare solo le persone che sono effettivamente a rischio. Il trattamento del dato risponde anche a finalità di tutela della salute pubblica e, in particolare, a finalità di carattere epidemiologico e serve, in particolare, a procedere a un progressivo affinamento dei parametri di rischio contagio.

***Dati tecnici***

**Stato del bluetooth**

- Collocazione originaria del dato: sul dispositivo dell'utente
- Categorie di interessati: tutti gli utenti dell'app
- Quando viene generato quel dato: al momento dell'invio di dati di analytics al server
- Eventuale trasferimento al back-end: sì
- Modalità (trigger) di trasferimento: invio al server durante il processo di invio dati di analytics da parte di utenti entrati in contatto stretto con un utente positivo e/o di invio mensile di dati di analytics da parte degli utenti
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1)
- Successivi trattamenti: conservazione, elaborazione e aggregazione di dati statistici sull'uso dell'applicazione
- Modalità di conservazione: memorizzazione su DataBase
- Modalità di aggregazione: esso stesso è criterio di aggregazione
- Modalità di anonimizzazione/pseudonimizzazione: il dato viene disassociato dall'indirizzo IP e quindi non è referenziato/referenziabile ad un utente
- Tempo di cancellazione locale: dato non memorizzato
- Tempo di cancellazione remota: cessazione dello stato di emergenza e comunque non oltre il 31/12/2020
- Finalità: per fornire al Ministero della Salute visibilità sul corretto funzionamento dell'app e intervenire se necessario (ad esempio migliorando il software o adottando specifiche iniziative di comunicazione) per assicurarsi che l'app possa effettivamente allertare utenti a rischio.

**Permesso per l'utilizzo del sistema Apple/Google che rende possibile il tracciamento dei contatti**

- Collocazione originaria del dato: sul dispositivo dell'utente
- Categorie di interessati: tutti gli utenti dell'app
- Modalità e momento della raccolta: al momento dell'invio di dati di analytics al server
- Eventuale trasferimento al back-end: sì
- Modalità (trigger) di trasferimento: invio al server durante il processo di invio dati di analytics da parte di utenti entrati in contatto stretto con un utente positivo e/o di invio mensile di dati di analytics da parte degli utenti
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture

organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1)
- Successivi trattamenti: conservazione, elaborazione e aggregazione di dati statistici sull'uso dell'applicazione
- Modalità di conservazione: memorizzazione su DataBase
- Modalità di aggregazione: esso stesso è criterio di aggregazione
- Modalità di anonimizzazione/pseudonimizzazione: il dato viene disassociato dall'indirizzo IP e quindi non è referenziato/referenziabile ad un utente
- Tempo di cancellazione locale: dato non memorizzato
- Tempo di cancellazione remota: cessazione dello stato di emergenza e comunque non oltre il 31/12/2020
- Finalità: per fornire al Ministero della Salute visibilità sul corretto funzionamento dell'app e intervenire se necessario (ad esempio migliorando il software o adottando specifiche iniziative di comunicazione) per assicurarsi che l'app possa effettivamente allertare utenti a rischio.

**Permesso per le notifiche**

- Collocazione originaria del dato: sul dispositivo dell'utente
- Categorie di interessati: tutti gli utenti dell'app
- Modalità e momento della raccolta: al momento dell'invio di dati di analytics al server
- Eventuale trasferimento al back-end: sì
- Modalità (trigger) di trasferimento: invio al server durante il processo di invio dati di analytics da parte di utenti entrati in contatto stretto con un utente positivo e/o di invio mensile di dati di analytics da parte degli utenti
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1).
- Successivi trattamenti: conservazione, elaborazione e aggregazione di dati statistici sull'uso dell'applicazione
- Modalità di conservazione: memorizzazione su DataBase
- Modalità di aggregazione: esso stesso è criterio di aggregazione
- Modalità di anonimizzazione/pseudonimizzazione: il dato viene disassociato dall'indirizzo IP e quindi non è referenziato/referenziabile ad un utente
- Tempo di cancellazione locale: dato non memorizzato
- Tempo di cancellazione remota: cessazione dello stato di emergenza e comunque non oltre il 31/12/2020
- Finalità: per fornire al Ministero della Salute visibilità sul corretto funzionamento dell'app e intervenire se necessario (ad esempio migliorando il software o adottando specifiche iniziative di comunicazione) per assicurarsi che l'app possa effettivamente allertare utenti a rischio.

**Sistema operativo del dispositivo**

- Collocazione originaria del dato: sul dispositivo dell'utente
- Categorie di interessati: tutti gli utenti dell'app
- Modalità e momento della raccolta: al momento dell'invio di dati di analytics al server
- Eventuale trasferimento al back-end: sì

- Modalità (trigger) di trasferimento: invio al server durante il processo di invio dati di analytics da parte di utenti entrati in contatto stretto con un utente positivo e/o di invio mensile di dati di analytics da parte degli utenti
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1).
- Successivi trattamenti: conservazione, elaborazione e aggregazione di dati statistici sull'uso dell'applicazione
- Modalità di conservazione: memorizzazione su DataBase
- Modalità di aggregazione: esso stesso è criterio di aggregazione
- Modalità di anonimizzazione/pseudonimizzazione: il dato viene disassociato dall'indirizzo IP e quindi non è referenziato/referenziabile ad un utente
- Tempo di cancellazione locale: dato non memorizzato
- Tempo di cancellazione remota: cessazione dello stato di emergenza e comunque non oltre il 31/12/2020
- Finalità: per fornire al Ministero della Salute visibilità sul corretto funzionamento dell'app e intervenire se necessario (ad esempio migliorando il software o adottando specifiche iniziative di comunicazione) per assicurarsi che l'app possa effettivamente allertare utenti a rischio.

**Clock del device**

- Collocazione originaria del dato: sul dispositivo dell'utente
- Categorie di interessati: utenti diagnosticati positivi a COVID-19
- Modalità e momento della raccolta: contestualmente all'invio delle TEK Eventuale trasferimento al back-end: sì
- Modalità (trigger) di trasferimento: invio al server durante il processo di invio dati dell'utente diagnosticato positivo
- Soggetti autorizzati: personale Sogei delle strutture organizzative applicative che seguono il progetto, espressamente designato "autorizzato al trattamento"; personale Sogei delle strutture organizzative sistemistiche, espressamente designato amministratore di sistema. Le designazioni avvengono secondo un processo strutturato e automatizzato che individua l'ambito di applicazione e i relativi permessi (par. 7.2.1 e 7.3.1).
- Successivi trattamenti: confronto con il Clock di sistema
- Modalità di conservazione: dato non memorizzato
- Modalità aggregazione: NA
- Modalità di anonimizzazione/pseudonimizzazione: il dato viene dissociato dall'indirizzo IP e quindi non è referenziato/referenziabile ad un utente
- Tempo di cancellazione locale: NA in quanto non memorizzato
- Tempo di cancellazione remota: NA in quanto non memorizzato
- Finalità: Per verificare un eventuale sfasamento dell'orario del device rispetto all'orario reale al fine di correggere l'orario errato delle TEK acquisite. I dati vengono trasferiti ai sistemi di backend nei casi descritti. Ogni trasferimento include necessariamente l'indirizzo IP del dispositivo, che non viene memorizzato nei sistemi di backend (cfr. 4.4).

Riportiamo di seguito una diversa tassonomia dei dati sopra elencati, raggruppati per comodità di lettura in base allo "stato" (positivo al virus, a rischio, nessuna delle due ipotesi) dell'utente.

***Utenti positivi al tampone Covid-19***
Nel caso di tampone positivo, l'utente sceglie volontariamente di inviare i dati al sistema di backend affinché siano allertati gli utenti con cui è entrato in contatto stretto. I dati inviati sono:

- Exposure Summary ed Exposure Info
- TEK
- provincia di domicilio
- codice OTP
- clock del device

***Utenti entrati in contatto stretto con un utente positivo***
Se l'algoritmo (cfr. [14], cap. 2) rileva un'esposizione che supera la soglia di rischio, l'utente visualizza una notifica generata dall'app stessa all'interno del dispositivo. Contestualmente, vengono inviati al sistema di backend i seguenti dati:

- ricezione notifica di esposizione
- data in cui è avvenuta l'ultima esposizione a rischio
- provincia di domicilio
- stato del bluetooth
- permesso per l'utilizzo del sistema Apple/Google che rende possibile il tracciamento dei contatti
- permesso per le notifiche di esposizione
- sistema operativo del dispositivo
- analytics token

L'invio è possibile al massimo una volta nell'arco di un mese. Allo stato attuale è possibile solo per dispositivi Apple, di cui si rileva l'integrità mediante Device Check technology (cfr. [11]).

***Utenti dell'app***
Allo scopo di monitorare la diffusione e la pervasività del sistema di contact tracing, ogni dispositivo trasmette, al massimo ogni 30 giorni, ai sistemi di backend le seguenti informazioni tecniche:

- stato del bluetooth
- permesso per l'utilizzo del sistema Apple/Google che rende possibile il tracciamento dei contatti
- permesso per le notifiche di esposizione
- provincia di domicilio
- sistema operativo del dispositivo
- analytics token

Ogni dispositivo invia inoltre rumore di fondo, ossia traffico casuale verso il backend allo scopo di mascherare gli invii di dati da utenti positivi o a rischio di contagio.

Ai fini di sanità pubblica, profilassi, statistici o di ricerca scientifica ([5], art. 6, comma 3) sono conservati sui sistemi di backend in database dedicati i seguenti dati:

- Provincia di domicilio
- Data di inizio sintomi dei soggetti risultati positivi
- Data in cui è avvenuta l'ultima esposizione a rischio
- Ricezione notifica di esposizione
- Exposure Summary
- Exposure Info
- Stato del Bluetooth

- Permesso per l'utilizzo del sistema Apple/Google che rende possibile il tracciamento dei contatti
- Permesso per le notifiche
- Sistema Operativo del dispositivo

La fornitura dei dati da parte di Sogei sarà effettuata giornalmente, in forma anonima e aggregata via PEC, agli uffici competenti del Ministero della Salute.

### 4.4 Adeguatezza, necessità e proporzionalità del trattamento

Il principio di privacy by default ha guidato tutte le scelte organizzative e tecnologiche per la realizzazione del sistema di contact tracing digitale. I dati di prossimità trattati da Immuni sono i minimi indispensabili relativamente alle finalità del trattamento, escludendo ogni forma di tracciamento degli spostamenti (geolocalizzazione) degli interessati e, in quanto pseudonimizzati come descritto nel cap. 2, riducono al minimo la possibilità di identificazione diretta della persona.

I dati risiedono sul dispositivo utente e sono inviati dall'app all'infrastruttura di backend solo nei casi descritti nel par. 4.3, necessari per perseguire le finalità del trattamento.

L'indirizzo IP del dispositivo che invia i dati viene trasformato in un indirizzo fittizio attraverso tecniche di *Network Address Translation* (NAT) dall'infrastruttura di backend all'atto dell'upload dei dati e non viene memorizzato né nel database né nei file di log.

Per quanto riguarda i dati registrati localmente nel dispositivo dell'utente, il Ministero della Salute non è Titolare del loro trattamento. La responsabilità di tali dati è in carico all'interessato, al quale viene raccomandata la corretta gestione del dispositivo e in particolare la sua protezione in modo da non permettere a terzi di accedere, anche involontariamente, ad informazioni inerenti al loro stato di salute.

Le azioni rimesse all'interessato (scarico e installazione dell'app, configurazione, corretta gestione del dispositivo) costituiscono una fase tecnica propedeutica al funzionamento del sistema preordinato al perseguimento della finalità di interesse pubblico.

L'interessato riceve, all'atto di installazione e configurazione della app:

- adeguata informativa, in linguaggio semplice e chiaro, riguardo alle finalità del trattamento, ai dati trattati, alla loro conservazione e cancellazione sul dispositivo e sull'infrastruttura centrale; l'informativa specifica inoltre che tali dati non vengono comunicati a terzi e che il Ministero della Salute non è in grado di risalire alla identità degli utenti dell'app
- istruzioni, anche in forma di infografica, sulle funzionalità dell'app
- raccomandazioni sulla corretta gestione del dispositivo (uso personale, modalità di custodia sicura, impostazione di password o PIN di sicurezza), a salvaguardia della riservatezza delle informazioni memorizzate dall'app

### 4.5 Diritti degli interessati

In virtù delle robuste tecniche di pseudonimizzazione utilizzate per la protezione dei dati personali (cfr. cap. 2), che rendono l'interessato non identificabile dal Titolare del trattamento, gli articoli dal 15 al 20 del

Regolamento inerenti ai diritti degli interessati non sono applicabili in conformità a quanto previsto dall'art. 11 comma 2 dello stesso Regolamento.

Il diritto di opposizione al trattamento ([1], art. 21) si concretizza nella disinstallazione dell'app; le chiavi saranno via via cancellate, al termine del quattordicesimo giorno di vita, anche sull'infrastruttura centrale. E' possibile per l'utente provvedere in ogni momento alla cancellazione dal dispositivo di tutte le chiavi temporanee (TEK) e gli identificativi di prossimità (RPI) mediante la funzione appositamente messa a disposizione dal framework Apple/Google.

Le chiavi temporanee (TEK) raccolte dal server non possono dar luogo a meccanismi automatici di profilazione ([1], art. 22) sia perché non associate nè associabili all'identità dell'interessato, sia perché sono cancellate progressivamente ogni 14 giorni. I dati raccolti per fini di sanità pubblica, profilassi, statistici o di ricerca scientifica sono conservati separatamente dalle chiavi temporanee e non a esse riconducibili.

## 5. VALUTAZIONE DI IMPATTO

La progettazione di Immuni ha tenuto conto sin dall'inizio della necessità di applicare misure tecniche e organizzative idonee a limitare il più possibile l'eventualità di identificare gli utenti che utilizzano la app.

Tuttavia appare chiaro che stante la riservatezza dei dati trattati, l'utilizzo di soluzioni tecnologiche che prevedono l'impiego di dati acquisiti direttamente dall'applicazione e l'uso di protocolli di comunicazione, non è possibile escludere a priori che vengano acquisite informazioni che per loro stessa natura potrebbero, attraverso elaborazioni e associazioni con dati detenuti da terzi (ad esempio operatori di telecomunicazioni) permettere, in via ipotetica, di riuscire ad identificare gli utenti.

### 5.1 Categorie di trattamento ad elevato rischio

La valutazione di impatto su Immuni si rende necessaria anche in relazione a quanto riportato dalle linee guida WP 248 del Comitato europeo per la protezione dei dati [1] e recepito dalla metodologia [8] adottata dal Ministero della Salute, secondo la quale un trattamento che rientri in almeno due tra le nove categorie di trattamento ad elevato rischio delineate dalle linee guida è soggetto alla valutazione di impatto.

Per quanto riguarda Immuni, si riscontra la sussistenza delle seguenti cinque tipologie di trattamento ad elevato rischio:

| Trattamento a rischio elevato | Esempi |
|---|---|

| | |
|---|---|
| Elaborazione di dati sensibili o aventi carattere altamente personale | Il trattamento prevede l'uso di categorie di dati particolari (stato di salute, opinioni politiche, credo religioso, etc.) o che possano accrescere i rischi per i diritti e le libertà degli interessati (dati di localizzazione, finanziari, dati strettamente personali e confidenziali, etc.) di cui agli artt. 9 e 10 del GDPR. |
| Elaborazione di dati su larga scala | Il trattamento prevede che siano elaborati dati su larga scala in termini di:<br>- numero di soggetti interessati dal trattamento, in termini numerici o di percentuale rispetto alla popolazione di riferimento<br>- volume dei dati e/o ambito delle diverse tipologie di dati oggetto di trattamento<br>- durata, o persistenza, dell'attività di trattamento<br>- ambito geografico dell'attività di trattamento |
| Elaborazione di dati relativi a soggetti vulnerabili per cui è più accentuato lo squilibrio di poteri fra interessato e titolare del trattamento | Il trattamento prevede l'elaborazione di dati e di informazioni riferite a minori o a persone che non siano in grado di opporsi o acconsentire, in modo consapevole e ragionato, al trattamento dei propri dati personali (i soggetti con patologie psichiatriche, i richiedenti asilo, gli anziani, i pazienti) e ogni interessato per il quale si possa identificare una situazione di disequilibrio nel rapporto con il rispettivo titolare del trattamento. |
| Utilizzi innovativi o applicazione di nuove soluzioni tecnologiche o organizzative | Il trattamento prevede l'associazione di tecniche dattiloscopiche (digitazione del PIN) con il riconoscimento del volto per migliorare il controllo degli accessi fisici oppure il trattamento prevede l'utilizzo di applicazioni legate al c.d. "Internet delle cose" (biomedicale, monitoraggio, servizi ai cittadini riferibili alle smart city). |
| Decisioni automatizzate con significativi effetti giuridici o di analoga natura | Il trattamento può comportare l'esclusione di una persona fisica da determinati benefici ovvero la sua discriminazione. Il trattamento che produce effetti minimi o nulli su un interessato non soddisfa questo specifico criterio. |

A prescindere dalla valutazione dei rischi per i diritti e le libertà degli interessati, illustrata nel paragrafo seguente, il trattamento di dati personali svolto da Immuni è soggetto a valutazione di impatto. Le misure di sicurezza tecniche e organizzative adeguate sono riportate nel cap. 7.

### 5.2 Rischi per i diritti e le libertà degli interessati

I rischi per i diritti e le libertà degli interessati sono calcolati come combinazione tra probabilità di accadimento e gravità del danno fisico-biologico, finanziario, reputazionale e di identità (trascurabile, basso, medio, alto) stimati sulle seguenti minacce relative ai dati:

- accesso non autorizzato e/o trattamento illecito
- divulgazione non autorizzata o accidentale
- modifica non autorizzata o accidentale
- perdita, distruzione accidentale o illegale
- indisponibilità temporanea o prolungata

I dati trattati non fanno esplicito riferimento all'interessato, pertanto il verificarsi delle minacce su citate non può generare danni rilevanti. Tuttavia, proprio per la sensibilità del tema, le valutazioni sono state svolte supponendo che i dati di salute trattati siano riconducibili a una persona specifica. Sono perciò valutazioni sovrastimate allo scopo di implementare misure di protezione che, seppur per ipotesi marginali, non possono essere escluse. L'identificazione degli utenti, infatti, richiederebbe l'adozione di tecnologie molto sofisticate e un dispendio di tempo e costi non proporzionati all'appetibilità delle informazioni. Piuttosto, potrebbero avere maggiore appetibilità le azioni di disturbo, finalizzate per loro stessa natura più a ostacolare l'iniziativa che a identificare gli interessati e diffonderne le generalità.

La progettazione del sistema decentralizzato per il contact tracing digitale e l'adozione delle tecniche di pseudonimizzazione non consentono al Ministero della Salute di conoscere le identità degli utenti, per cui il rischio di discriminazione degli interessati per il mancato utilizzo dell'app ([5], art. 6, comma 4) non è stato incluso nelle valutazioni.

Il rischio di discriminazione di categorie particolari di interessati potrebbe riguardare gli stranieri presenti alla data sul territorio italiano, linguisticamente svantaggiati. Al lancio l'app sarà disponibile in quattro lingue, anche per tener conto degli obblighi di bilinguismo previsti nel nostro ordinamento: italiano, tedesco, francese e inglese. L'app si adatterà alla lingua di sistema; nel caso non rientri tra queste, l'app verrà visualizzata in inglese.

Il sistema di contact tracing non comporta decisioni automatizzate che abbiano effetto sugli interessati. La notifica di positività viene inviata volontariamente all'infrastruttura di backend dai soggetti positivi al tampone Covid-19 e trattata al solo scopo di allertare le persone con cui sono stati in contatto; i dati relativi al rischio di esposizione per gli utenti che sono entrati in contatto stretto con un positivo vengono raccolti ai soli fini di sanità pubblica, profilassi, statistici o di ricerca scientifica, non comportando alcun effetto sull'interessato, che viene invitato a contattare il proprio medico di medicina generale o il pediatra di libera scelta e a seguire alcuni indicazioni di comportamento. Il Ministero della Salute non ha alcun modo di verificare se l'utente segue le indicazioni che gli sono fornite, non potendo risalire alla sua identità.

I prossimi paragrafi riportano l'esito del calcolo dei rischi diversificato per i dati trattati, comuni e particolari (sanitari).

### *5.2.1 Accesso non autorizzato e/o trattamento illecito*

I dati comuni non sono particolarmente appetibili e inoltre non forniscono alcuna informazione diretta sull'identità dell'interessato. Diverso il discorso per l'accesso ai dati sanitari che può generare, per le persone positive al tampone e per quelle che sono state in contatto con positivo, un danno reputazionale

medio legato alla perdita di riservatezza di informazioni strettamente legate al loro stato di salute e un danno fisico-biologico medio conseguente a una possibile stigmatizzazione.

Lo scenario di rischio è legato a un eventuale controllo illecito del traffico generato dall'app mediante:

- furto del dispositivo
- intercettazione dei dati trasmessi
- reidentificazione dell'interessato dopo un contagio accertato
- deduzione di informazioni dal comportamento del traffico di rete
- exploit dei servizi mediante invio di richieste malformate

La tabella seguente sintetizza le valutazioni svolte e la sintesi dei rischi.

| Dati | Probabilità di accadimento | Danno fisico-biologico | Danno finanziario | Danno reputazionale | Danno di identità | Rischio intrinseco | Rischio intrinseco per minaccia |
|---|---|---|---|---|---|---|---|
| comuni | B | T | T | T | T | T | M |
| particolari (sanitari) | M | M | T | M | M | M | |

### *5.2.2 Divulgazione non autorizzata o accidentale*

I dati comuni non sono particolarmente appetibili e inoltre non forniscono alcuna informazione sull'interessato. Nel caso di divulgazione dei dati sanitari, è stato valutato medio il danno fisico-biologico (possibile discriminazione/stigmatizzazione, stato di ansia), finanziario (impossibilità di svolgere l'attività lavorativa) e di identità (possibile controllo indiretto della popolazione, limitazione della libertà personale); alto invece il danno reputazionale, come conseguenza della violazione della riservatezza di informazioni strettamente personali e della possibilità, seppur remota, di arricchimento di tali dati con altre fonti.

La divulgazione in ogni caso presuppone un accesso, accidentale o illecito, pertanto valgono considerazioni analoghe a quelle riportate nel par. 5.2.1. a cui si aggiungono i seguenti scenari di rischio:

- accesso da parte di terzi a dati locali dell'app
- presenza di vulnerabilità, malware o backdoor nel codice e in librerie di terze parti

La tabella seguente sintetizza le valutazioni svolte e la sintesi dei rischi.

| Dati | Probabilità di accadimento | Danno fisico-biologico | Danno finanziario | Danno reputazionale | Danno di identità | Rischio intrinseco | Rischio intrinseco per minaccia |
|---|---|---|---|---|---|---|---|
| comuni | B | T | T | T | T | T | A |
| particolari (sanitari) | M | M | M | A | M | A | |

### *5.2.3 Modifica non autorizzata o accidentale*

La modifica dei dati comuni non comporterebbe in sé alcuna conseguenza se non legata all'associazione tra questi e i dati sanitari, per cui la stima dei rischi si è concentrata su questi ultimi e sui danni che un inquinamento dei dati (per azioni malevole mirate, per errato funzionamento dell'app o per errore umano) può portare all'interessato. Il danno fisico-biologico è valutato alto (errata consapevolezza dell'interessato che ha un forte impatto sull'accesso alle cure, stato d'ansia generato da una errata comunicazione, possibile discriminazione/stigmatizzazione), mentre si rileva medio il danno reputazionale (per variazione dello stato di salute) e di identità (possibile limitazione della libertà personale).

Si profilano quindi i seguenti scenari di rischio legati alla compromissione delle informazioni gestite dal servizio:

- falsi positivi generati dall'algoritmo di calcolo del rischio di esposizione
- errore nel codice o nelle librerie utilizzate
- caricamento di chiavi altrui
- errore da parte dell'interessato nell'uso dell'app o nella comunicazione dell'OTP
- accesso illecito al sistema Tessera Sanitaria
- inquinamento dei dati di contagio (Exposure)
- inquinamento dei dati epidemiologici (Analytics)

La tabella seguente sintetizza le valutazioni svolte e la sintesi dei rischi.

| Dati | Probabilità di accadimento | Danno fisico-biologico | Danno finanziario | Danno reputazionale | Danno di identità | Rischio intrinseco | Rischio intrinseco per minaccia |
|---|---|---|---|---|---|---|---|
| comuni | B | T | T | T | T | T | A |
| particolari (sanitari) | M | A | T | M | M | A | |

### *5.2.4 Perdita, distruzione accidentale o illegale*

La perdita o distruzione dei dati, dovuta ad esempio ad attacco informatico, può comportare un danno fisico-biologico stimabile in medio per i dati comuni (l'interessato potrebbe non essere allertato di un eventuale contatto con un positivo) e alto per i dati sanitari (compromissione del sistema di prevenzione). Le altre tipologie di danni sono valutate trascurabili.

Lo scenario di rischio è pertanto legato alla compromissione dal servizio a causa di:

- guasto, malfunzionamento, errore umano
- intrusione nei sistemi informatici

La tabella seguente sintetizza le valutazioni svolte e la sintesi dei rischi.

| Dati | Probabilità di accadimento | Danno fisico-biologico | Danno finanziario | Danno reputazionale | Danno di identità | Rischio intrinseco | Rischio intrinseco per minaccia |
|---|---|---|---|---|---|---|---|
| comuni | B | M | T | T | T | B | M |
| particolari (sanitari) | M | A | T | T | T | M | |

### *5.2.5 Indisponibilità temporanea o prolungata*

Le stime dei danni per gli interessati sono equiparabili alle valutazioni svolte nel caso di perdita o distruzione dei dati, salvo per il danno fisico-biologico. Trattandosi di indisponibilità temporanea o prolungata e non di perdita, si può ipotizzare che le persone che sono state in contatto con individui contagiati siano avvertite, seppur con ritardo.

Lo scenario di rischio è pertanto legato alla compromissione dal servizio a causa di:

- guasto, malfunzionamento, errore umano
- intrusione nei sistemi informatici

La tabella seguente sintetizza le valutazioni svolte e la sintesi dei rischi.

| Dati | Probabilità di accadimento | Danno fisico-biologico | Danno finanziario | Danno reputazionale | Danno di identità | Rischio intrinseco | Rischio intrinseco per minaccia |
|---|---|---|---|---|---|---|---|
| comuni | B | B | T | T | T | B | M |
| particolari (sanitari) | B | A | T | T | T | M | |

## 6. RISCHI PER PERDITA DI RISERVATEZZA, INTEGRITÀ, DISPONIBILITÀ DELLE INFORMAZIONI

Oltre ai rischi per i diritti e le libertà dell'interessato, valutati nel capitolo precedente, è stato considerato l'impatto della perdita di riservatezza, integrità e disponibilità delle informazioni sul servizio pubblico di prevenzione dei contagi rappresentato da Immuni. A fronte di una perdita finanziaria non pertinente, si stimano danni medi sull'operatività, e quindi efficienza, del servizio relativi alla perdita di disponibilità dei dati (alti per indisponibilità prolungata), una perdita di immagine alta per il Sistema Sanitario in caso di compromissione degli attributi (media solo per indisponibilità a breve termine) legata alla stigmatizzazione mediatica dell'iniziativa e alla perdita di fiducia dei cittadini nel sistema di prevenzione, e una apprezzabile possibilità di sanzioni normative in caso di perdita di riservatezza e integrità dei dati.

Le stime tengono in considerazione anche l'alta appetibilità di attacchi di interruzione del servizio di tipo Distributed Denial of Service (DDoS) allo scopo di sabotaggio dell'iniziativa.

La tabella seguente riporta le valutazioni svolte e i valori di sintesi degli attributi.

| Attributo | Perdita Finanziaria | Perdita Operativa | Perdita d'immagine | Sanzioni normative | Valore attributo |
|---|---|---|---|---|---|
| Riservatezza | Nullo | Nullo | Alto | Medio | Alto |
| Integrità | Nullo | Nullo | Alto | Basso | Alto |
| Disponibilità breve termine | Nullo | Medio | Medio | Nullo | Medio |
| Disponibilità medio termine | Nullo | Medio | Alto | Nullo | Alto |
| Disponibilità prolungata | Nullo | Alto | Alto | Nullo | Alto |

## 7. RISCHI COMPLESSIVI E MISURE DI SICUREZZA ADEGUATE

La tabella di seguito mostra il riepilogo dei rischi per i diritti e libertà dell'interessato (cfr. par. 5.2), per la perdita di riservatezza, integrità e disponibilità dei dati (cfr. cap. 6) e il calcolo complessivo dei rischi ai fini di individuare misure tecniche e organizzative adeguate a contrastarli in relazione alle singole minacce.

| Minaccia sui dati | Rischio intrinseco per l'interessato | Rischio per perdita di riservatezza, integrità, disponibilità | Rischio intrinseco complessivo |
|---|---|---|---|
| Accesso non autorizzato e/o trattamento illecito | M | A | A |
| Divulgazione non autorizzata o accidentale | A | A | A |
| Modifica non autorizzata o accidentale | A | A | A |
| Perdita, distruzione accidentale o illegale | M | A | A |
| Indisponibilità temporanea o prolungata | M | A | A |

Come riportato nel cap. 4.2, Immuni si articola in tre componenti informatizzate, l'app e il servizio di interazione con Tessera Sanitaria e il backend, che differiscono tra loro per funzionalità e tecnologie. La selezione delle misure da applicare al trattamento, riportata nei prossimi paragrafi, è stata perciò svolta separatamente sulle tre componenti, considerando un rischio intrinseco complessivo alto su tutte le

minacce, derivante dalla valutazione di impatto (cfr. par 5.1) e confermato dai dati di sintesi riportati in tabella.

## 7.1 Misure di protezione per l'app

### *7.1.1 Protezione per accesso, divulgazione, modifica non autorizzata o accidentale dei dati e trattamento illecito*

| MISURA | DESCRIZIONE E IMPLEMENTAZIONE (omessa nella pubblicazione per motivi di sicurezza) |
|---|---|
| Pseudonimizzazione | |
| Gestione informative | |
| Cifratura del canale | |
| Mascheramento del traffico generato | |
| Protezione dell'identità della persona per furto del dispositivo | |
| Controllo di qualità e sicurezza del software | |
| Controllo di autenticità dei dati di contagio inviati | |
| Controllo di autenticità dei dati epidemiologici inviati | |

### *7.1.2 Protezione per perdita, distruzione accidentale o illegale e indisponibilità temporanea o prolungata dei dati*

| MISURA | DESCRIZIONE E IMPLEMENTAZIONE<br>(omessa nella pubblicazione per motivi di sicurezza) |
|---|---|
| Conservazione dei dati e backup | |
| Istruzioni all'utente | |

## 7.2 Misure di protezione per il backend

### *7.2.1 Protezione per accesso, divulgazione, modifica non autorizzata o accidentale dei dati e trattamento illecito*

| MISURA | DESCRIZIONE E IMPLEMENTAZIONE<br>(omessa nella pubblicazione per motivi di sicurezza) |
|---|---|
| Protezione da exploit | |
| Pseudonimizzazione | |
| Autorizzazione al trattamento per amministratori di sistema | |
| Autorizzazione per l'accesso ai dati | |
| Firma digitale delle chiavi temporanee | |
| Log degli amministratori di sistema | |
| Log degli autorizzati all'accesso alle basi dati | |
| Log di sistema | |
| Conservazione dei log | |

### *7.2.2 Protezione per perdita, distruzione accidentale o illegale e indisponibilità temporanea o prolungata dei dati*

| MISURA | DESCRIZIONE E IMPLEMENTAZIONE (omessa nella pubblicazione per motivi di sicurezza) |
|---|---|
| Backup del servizio | |
| Backup del database | |
| Backup delle componenti del servizio | |
| Ripristino dei dati | |
| Disaster Recovery Base | |
| Conservazione dei dati e cessazione del trattamento | |

## 7.3 Misure di protezione per il servizio di autenticazione OTP

### *7.3.1 Protezione per accesso, divulgazione, modifica non autorizzata o accidentale dei dati e trattamento illecito*

| MISURA | DESCRIZIONE E IMPLEMENTAZIONE (omessa nella pubblicazione per motivi di sicurezza) |
|---|---|
| Registrazione utenti de visu | |
| Autenticazione a due fattori | |
| Autenticazione per accesso tramite applicativi | |
| Autenticazione, password policy | |
| Autorizzazione, privilegio minimo | |

| | |
|---|---|
| Autenticazione, form di accesso | |
| Disattivazione delle credenziali | |
| Distribuzione credenziali | |
| Limitazione riutilizzo password | |
| Verifica identità dell'utente | |
| Inibizione accessi non autorizzati | |
| Informazioni su ultimo accesso | |
| Disconnessione della sessione | |
| Controllo status utenti | |
| Elenco banche accessibili | |
| Cifratura del canale | |
| Comunicazione tra applicazioni autorizzate | |
| Tracciamento accessi e operazioni | |
| Autorizzazione al trattamento per amministratori di sistema | |
| Autorizzazione per l'accesso ai dati | |
| Log degli amministratori di sistema | |
| Log degli autorizzati all'accesso alle basi dati | |

| | |
|---|---|
| Log di sistema | |
| Conservazione dei log | |

### *7.3.2 Protezione per perdita, distruzione accidentale o illegale e indisponibilità temporanea o prolungata dei dati*

| MISURA | DESCRIZIONE E IMPLEMENTAZIONE (omessa nella pubblicazione per motivi di sicurezza) |
|---|---|
| Backup del servizio | |
| Backup delle componenti | |
| Ripristino dei dati | |

## 7.4 Valutazioni finali

La valutazione dei rischi svolta nei cap. 5 e 6 ha portato alla applicazione delle misure previste dalla metodologia [8] per la loro mitigazione, relativamente al contesto tecnologico delle tre componenti del trattamento.

Si riporta nella tabella di seguito una descrizione dei rischi residui, valutati al momento di bassi impatto o probabilità.

*(Paragrafo omesso nella pubblicazione per motivi di sicurezza)*

# 8. PROTEZIONE DELL'INFRASTRUTTURA

*(Paragrafo omesso nella pubblicazione per motivi di sicurezza)*

# 9. ELEMENTI DI VALUTAZIONE EVENTUALMENTE ACQUISTI AI SENSI DELL'ART. 35 (9) DEL GDPR

Ai sensi dell'Articolo 35 (9) GDPR, il titolare del trattamento raccoglie, se del caso, le opinioni sul trattamento previsto da parte degli interessati che saranno coinvolti nel trattamento stesso, o dei loro rappresentanti, fatta salva la tutela degli interessi commerciali o pubblici o la sicurezza dei trattamenti.

L'EDPB (European Data Protection Board) ritiene che tali opinioni possano essere raccolte attraverso una varietà di mezzi a seconda del contesto. L'EDPB ha peraltro chiarito che il titolare potrebbe legittimamente

decidere di non procedere alla raccolta delle opinioni degli interessati qualora lo ritenga non appropriato, purché tale decisione sia giustificata e documentata.

Ciò detto, la doverosa premessa è che il trattamento in esame si svolge in un contesto sociale caratterizzato da un elevatissimo numero di potenziali interessati, dato che l'epidemia ha coinvolto l'intera popolazione italiana e ha richiesto misure eccezionali per fare fronte alla situazione di emergenza che si è venuta a creare con penetranti limitazioni delle libertà individuali garantite dalla Costituzione. Pertanto gli interessati hanno ampia conoscenza del dibattito sulla migliore strategia di contrasto dell'epidemia che si basa sul testare, tracciare e trattare il maggior numero possibile di individui per impedire – o comunque prontamente individuare - nuovi focolai di infezione.

Alla luce di queste considerazioni, si è ritenuto anzitutto di privilegiare il pieno rispetto degli obblighi di trasparenza attraverso, tra le altre cose, il carattere libero e aperto del software utilizzando lo strumento della piattaforma GitHub per la condivisione e la cooperazione sulle questioni tecniche legate all'applicazione, lasciando ad un momento successivo, e segnatamente al termine della fase di sperimentazione, la raccolta di opinioni sull'uso vero e proprio dell'applicazione da parte dei diretti interessati. E' dunque in corso un primo momento di confronto con le opinioni esperte sulla parte più strettamente tecnica dell'applicazione e sulle misure di sicurezza volta a rafforzare quel vincolo di fiducia che è un elemento fondamentale per il buon esito del progetto. Quanto alla raccolta delle opinioni dei cittadini che saranno chiamati, in modo del tutto libero e volontario, a scaricare l'applicazione, la scelta più ragionevole è rimandare alla fase di sperimentazione la raccolta di dette opinioni.

Tale scelta si giustifica con due ordini di ragioni.

Anzitutto, il dibattito sull'opportunità di dotarsi, nell'ambito di una più ampia strategia di contrasto della pandemia, di una applicazione di contact tracing a supporto dell'attività ordinaria di identificazione dei potenziali contagi è il tema più dibattuto negli organi di informazione da quando il Governo, attraverso il Commissario straordinario per l'attuazione e il coordinamento delle misure di contenimento e contrasto dell'emergenza epidemiologica COVID-19, ha individuato la soluzione tecnologica in esame. Non vi è stato giorno senza un ampio ed articolato dibattito su tutti gli organi di stampa che ha evidenziato sia posizioni a favore sia posizioni contrarie all'utilizzo di questa applicazione. Tali posizioni, sia favorevoli sia contrarie, sono ben note e sono state tenute in debita considerazione nello sviluppo dell'applicazione e nell'individuazione delle specifiche misure di mitigazione del rischio già illustrate nella presente valutazione di impatto.

In secondo luogo, alla luce di quanto sopra, si ritiene che procedere oggi alla raccolta delle opinioni degli interessati in relazione al trattamento in oggetto risulterebbe di scarsa utilità sia per quanto detto sopra, sia perché in contrasto con il contesto emergenziale in cui il trattamento si inserisce e quindi con la necessità di adottare misure di contenimento del Covid-19 nel più breve tempo possibile.