Seleziona la tua lingua preferita

IT GB ES FR DE

Regolamento Generale sulla Protezione dei Dati di RescueCom

Informativa sul Regolamento (UE) 2016/679 (GDPR)

Ultimo aggiornamento: 28 Dicembre 2025

RescueCom è una piattaforma di comunicazione d'emergenza (Proof of Concept), sviluppata in ambito accademico per facilitare le operazioni di soccorso in scenari privi di connettività internet.

Questa informativa descrive in dettaglio le modalità di trattamento dei tuoi dati personali e particolari (sanitari), le misure di sicurezza crittografica adottate e i tuoi diritti. La nostra priorità è garantire la massima riservatezza: adottiamo un approccio **Privacy by Design** e **Privacy by Default**, minimizzando la raccolta dei dati al solo necessario per salvare vite umane.

Il sistema utilizza una rete decentralizzata (Mesh) in cui la sicurezza è garantita matematicamente tramite crittografia End-to-End. Nessun intermediario può accedere al contenuto delle tue comunicazioni.

Scarica l'informativa legale completa (PDF firmato digitalmente)

1. Categorie di Dati Trattati e Finalità

In conformità al principio di minimizzazione dei dati, raccogliamo esclusivamente le informazioni indispensabili per la gestione efficace delle emergenze:

- **Dati Identificativi Comuni:** Nome, cognome, data di nascita e un identificativo utente univoco . Questi dati servono per identificare in modo certo la persona che richiede soccorso.
- **Categorie Particolari di Dati (Dati Sanitari):** Il trattamento include dati sensibili critici per il triage medico, quali: gruppo sanguigno, allergie farmacologiche note, disabilità specifiche (motorie, sensoriali o cognitive) e patologie croniche rilevanti (es. diabete, cardiopatie).
- **Dati di Geolocalizzazione:** Coordinate GPS precise (latitudine/longitudine) acquisite in tempo reale o inserite manualmente, utilizzate esclusivamente per localizzare il dispositivo in scenario di crisi.
- **Dati di Telemetria Tecnica:** Metadati relativi allo stato della batteria e della connettività, necessari per valutare l'affidabilità del nodo nella rete mesh.

2. Base Giuridica del Trattamento

Il trattamento dei tuoi dati personali è legittimato dalle seguenti basi giuridiche:

- **Consenso Esplicito:** In ottemperanza allo pseudo-requisito tecnico di sistema PR_L.1, la memorizzazione dei dati sanitari avviene solo previo consenso libero, specifico ed informato, manifestato tramite un'azione positiva inequivocabile (opt-in) nell'app.
- **Salvaguardia degli Interessi Vitali:** Nelle situazioni di emergenza in cui l'interessato si trovi nell'incapacità fisica o giuridica di prestare il consenso, il trattamento è necessario per proteggere la vita dell'interessato o di terzi.

3. Architettura del Sistema e Modalità di Trattamento

Il trattamento avviene mediante un'infrastruttura ibrida resiliente, progettata per operare anche in scenari catastrofici:

- **Archiviazione Locale (Edge):** I dati risiedono primariamente sul dispositivo dell'utente in un database SQLite cifrato (SQLCipher). Questo garantisce che l'utente mantenga il possesso fisico dei propri dati.
- **Rete Mesh Peer-to-Peer (P2P):** In assenza di internet, i dati viaggiano attraverso una rete di dispositivi interconnessi via Bluetooth LE o Wi-Fi Direct. Ogni dispositivo funge da ripetitore, ma senza accesso ai dati (vedere punto 4).
- **Sincronizzazione Cloud Sicura:** Quando la connettività viene ripristinata, i dati critici vengono sincronizzati con il server centrale tramite API REST protette, garantendo la coerenza delle cartelle cliniche d'emergenza.

4. Misure di Sicurezza Tecniche

Per mitigare i rischi di accesso non autorizzato, perdita o alterazione, implementiamo misure di sicurezza allo stato dell'arte:

- **Crittografia AES-GCM-256:** Tutti i dati sensibili, sia a riposo che in transito nella rete mesh, sono cifrati con Advanced Encryption Standard (AES) in modalità Galois/Counter Mode (GCM) a 256 bit, garantizando confidenzialità e integrità autenticata.
- **Protocollo Blind Relay (RF_16):** I dispositivi che inoltrano i messaggi per conto di altri utenti agiscono come "blind relays" (nodi ciechi). Essi trasportano pacchetti cifrati senza possedere la chiave di decifrazione, rendendo tecnicamente impossibile l'accesso al contenuto dei messaggi di soccorso da parte di terzi intermediari.
- **Gestione delle Chiavi:** Utilizzo di curve ellittiche (ECDH e ECDSA) per la negoziazione sicura delle chiavi di sessione e per la firma digitale dei messaggi, prevenendo attacchi Man-in-the-Middle.

5. Segregazione dei Ruoli e Controllo Accessi

Il sistema impone una rigorosa separazione dei ruoli, definita a livello di codice e immutabile:

- **Utente "Rescuee" (Richiedente):** Può accedere, modificare e cancellare esclusivamente i propri dati. Non ha privilegi per consultare dati di altri utenti.
- **Utente "Rescuer" (Soccorritore Qualificato):** Ottiene l'accesso temporaneo ai dati sanitari e di posizione del Rescuee solo nel contesto attivo di una missione di soccorso. L'accesso è loggato e monitorato.
- **Amministratore di Sistema:** Gestisce l'infrastruttura tecnica ma non possiede le chiavi private per decifrare i dati sanitari degli utenti, garantendo la confidenzialità anche rispetto al gestore del servizio.

6. Retention Policy e Diritti dell'Interessato

Periodo di Conservazione: I dati operativi vengono conservati per la durata dell'emergenza. Al termine, vengono archiviati per finalità medico-legali per il periodo prescritto dalla legge (es. 10 anni per la responsabilità medica) o anonimizzati irreversibilmente per scopi statistici e di ricerca.

Esercizio dei Diritti: Puoi esercitare in ogni momento il diritto di accesso, rettifica, cancellazione ("diritto all'oblio"), limitazione, portabilità e opposizione. Puoi revocare il consenso tramite le impostazioni dell'app, comportando la cancellazione dei dati locali e remoti. Per reclami, puoi rivolgerti al Garante Privacy nazionale.