Sélectionnez votre langue préférée

IT EN ES FR DE

Avis Étendu sur le Traitement des Données Personnelles

Avis conforme au Règlement (UE) 2016/679 (RGPD)

Dernière mise à jour : 28 décembre 2025

RescueCom est une plateforme de communication d'urgence (Preuve de Concept), développée dans un cadre académique pour faciliter les opérations de secours dans des scénarios dépourvus de connectivité internet.

Cet avis décrit en détail comment nous traitons vos données personnelles et particulières (santé), les mesures de sécurité cryptographiques adoptées et vos droits. Notre priorité est de garantir une confidentialité maximale : nous adoptons une approche de **Privacy by Design** et **Privacy by Default**, minimisant la collecte de données au strict nécessaire pour sauver des vies humaines.

Le système utilise un réseau décentralisé (Mesh) où la sécurité est mathématiquement garantie par un chiffrement de bout en bout. Aucun intermédiaire ne peut accéder au contenu de vos communications.

Télécharger l'avis juridique complet (PDF signé numériquement)

1. Catégories de Données Traitées et Finalités

Conformément au principe de minimisation des données, nous collectons exclusivement les informations indispensables à une gestion efficace des urgences :

- **Données d'Identification Communes :** Nom, prénom, date de naissance et un identifiant utilisateur unique (UUID). Ces données servent à identifier de manière certaine la personne demandant du secours.
- **Catégories Particulières de Données (Données de Santé) :** Le traitement inclut des données sensibles critiques pour le triage médical, telles que : groupe sanguin, allergies médicamenteuses connues, handicaps spécifiques (moteurs, sensoriels ou cognitifs) et pathologies chroniques pertinentes (ex. diabète, maladies cardiaques).
- **Données de Géolocalisation :** Coordonnées GPS précises (latitude/longitude) acquises en temps réel ou saisies manuellement, utilisées exclusivement pour localiser l'appareil en scénario de crise.
- **Données de Télémétrie Technique :** Métadonnées relatives à l'état de la batterie et à la connectivité, nécessaires pour évaluer la fiabilité du nœud dans le réseau maillé.

2. Base Juridique du Traitement

Le traitement de vos données personnelles est légitimé par les bases juridiques suivantes :

- **Consentement Explicite :** Conformément au pseudo-requis technique du système PR_L1, le stockage des données de santé n'a lieu qu'après un consentement libre, spécifique et éclairé, manifesté par une action positive sans équivoque (opt-in) dans l'application.
- **Sauvegarde des Intérêts Vitaux :** Dans les situations d'urgence où la personne concernée se trouve dans l'incapacité physique ou juridique de donner son consentement, le traitement est nécessaire pour protéger la vie de la personne concernée ou d'une autre personne physique.

3. Architecture du Système et Modalités de Traitement

Le traitement s'effectue via une infrastructure hybride résiliente, conçue pour fonctionner même dans des scénarios catastrophiques :

- **Stockage Local (Edge) :** Les données résident principalement sur l'appareil de l'utilisateur dans une base de données SQLite chiffrée (SQLCipher). Cela garantit que l'utilisateur conserve la possession physique de ses données.
- **Réseau Mesh Peer-to-Peer (P2P) :** En l'absence d'internet, les données voyagent à travers un réseau d'appareils interconnectés via Bluetooth LE ou Wi-Fi Direct. Chaque appareil agit comme un relais, mais sans accès aux données (voir point 4).
- **Synchronisation Cloud Sécurisée :** Lorsque la connectivité est rétablie, les données critiques sont synchronisées avec le serveur central via des API REST sécurisées, garantissant la cohérence des dossiers médicaux d'urgence.

4. Mesures de Sécurité Techniques

Pour atténuer les risques d'accès non autorisé, de perte ou d'altération, nous mettons en œuvre des mesures de sécurité de pointe :

- **Chiffrement AES-GCM-256 :** Toutes les données sensibles, au repos comme en transit dans le réseau maillé, sont chiffrées avec Advanced Encryption Standard (AES) en mode Galois/Counter Mode (GCM) à 256 bits, garantissant confidentialité et intégrité authentifiée.
- **Protocole Blind Relay (RF_16) :** Les appareils relayant des messages pour le compte d'autres utilisateurs agissent comme des "blind relays" (nœuds aveugles). Ils transportent des paquets chiffrés sans posséder la clé de déchiffrement, rendant techniquement impossible l'accès au contenu des messages de secours par des tiers intermédiaires.
- **Gestion des Clés :** Utilisation de courbes elliptiques (ECDH et ECDSA) pour la négociation sécurisée des clés de session et la signature numérique des messages, empêchant les attaques Man-in-the-Middle.

5. Ségrégation des Rôles et Contrôle d'Accès

Le système impose une séparation stricte des rôles, définie au niveau du code et immuable :

- **Utilisateur "Rescuee" (Demandeur) :** Peut accéder, modifier et supprimer exclusivement ses propres données. N'a pas les privilèges pour consulter les données d'autres utilisateurs.
- **Utilisateur "Rescuer" (Secouriste Qualifié) :** Obtient un accès temporaire aux données de santé et de position du Rescuee uniquement dans le contexte actif d'une mission de secours. L'accès est journalisé et surveillé.
- **Administrateur Système :** Gère l'infrastructure technique mais ne possède pas les clés privées pour déchiffrer les données de santé des utilisateurs, garantissant la confidentialité même vis-à-vis du fournisseur de service.

6. Politique de Conservation et Droits de la Personne Concernée

Période de Conservation : Les données opérationnelles sont conservées pendant la durée de l'urgence. Par la suite, elles sont archivées à des fins médico-légales pour la période prescrite par la loi (ex. 10 ans pour la responsabilité médicale) ou anonymisées de manière irréversible à des fins statistiques et de recherche.

Exercice des Droits : Vous pouvez exercer à tout moment le droit d'accès, de rectification, d'effacement ("droit à l'oubli"), de limitation, de portabilité et d'opposition. Vous pouvez retirer votre consentement via les paramètres de l'application, entraînant la suppression des données locales et distantes. Pour les réclamations, vous pouvez contacter l'Autorité Nationale de Protection des Données.