Select your preferred language

🌍 | IT EN ES FR DE

Extended Personal Data Processing Notice

Notice pursuant to Regulation (EU) 2016/679 (GDPR)

Last updated: December 28, 2025

RescueCom is an emergency communication platform (Proof of Concept), developed academically to facilitate rescue operations in scenarios lacking internet connectivity.

This notice describes in detail how we process your personal and special (health) data, the cryptographic security measures adopted, and your rights. Our priority is ensuring maximum confidentiality: we adopt a **Privacy by Design** and **Privacy by Default** approach, minimizing data collection to only what is necessary to save human lives.

The system uses a decentralized (Mesh) network where security is mathematically guaranteed via End-to-End encryption. No intermediary can access the content of your communications.

Download full legal notice (Digitally Signed PDF)

1. Categories of Processed Data and Purposes

In accordance with the data minimization principle, we collect exclusively the information indispensable for effective emergency management:

- **Common Identification Data:** First name, last name, date of birth, and a unique user identifier (UUID). These data are used to unmistakably identify the person requesting rescue.
- **Special Categories of Data (Health Data):** Processing includes sensitive data critical for medical triage, such as: blood type, known drug allergies, specific disabilities (motor, sensory, or cognitive), and relevant chronic conditions (e.g., diabetes, heart disease).
- **Geolocation Data:** Precise GPS coordinates (latitude/longitude) acquired in real-time or manually entered, used exclusively to locate the device in crisis scenarios.
- **Technical Telemetry Data:** Metadata regarding battery status and connectivity, necessary to assess node reliability in the mesh network.

2. Legal Basis for Processing

The processing of your personal data is legitimized by the following legal bases:

- **Explicit Consent:** In compliance with the technical system pseudo-requirement PR_L.1, the storage of health data occurs only following free, specific, and informed consent, manifested through an unambiguous positive action (opt-in) in the app.
- **Protection of Vital Interests:** In emergency situations where the data subject is physically or legally incapable of giving consent, processing is necessary to protect the life of the data subject or another natural person.

3. System Architecture and Processing Methods

Processing takes place via a resilient hybrid infrastructure, designed to operate even in catastrophic scenarios:

- **Local Storage (Edge):** Data resides primarily on the user's device in an encrypted SQLite database (SQLCipher). This ensures the user maintains physical possession of their data.
- **Peer-to-Peer (P2P) Mesh Network:** In the absence of internet, data travels through a network of devices interconnected via Bluetooth LE or Wi-Fi Direct. Each device acts as a relay, but without access to data (see point 4).
- **Secure Cloud Synchronization:** When connectivity is restored, critical data is synchronized with the central server via secure REST APIs, ensuring emergency health record consistency.

4. Technical Security Measures

To mitigate risks of unauthorized access, loss, or alteration, we implement state-of-the-art security measures:

- **AES-GCM-256 Encryption:** All sensitive data, both at rest and in transit within the mesh network, are encrypted with Advanced Encryption Standard (AES) in Galois/Counter Mode (GCM) at 256 bits, guaranteeing confidentiality and authenticated integrity.
- **Blind Relay Protocol (RF_16):** Devices forwarding messages on behalf of other users act as "blind relays." They transport encrypted packets without possessing the decryption key, making it technically impossible for third-party intermediaries to access the content of rescue messages.
- **Key Management:** Use of elliptic curves (ECDH and ECDSA) for secure session key negotiation and digital signature of messages, preventing Man-in-the-Middle attacks.

5. Role Segregation and Access Control

The system enforces strict role separation, defined at the code level and immutable:

- **"Rescuee" User (Requestor):** Can access, modify, and delete exclusively their own data. Does not have privileges to consult other users' data.
- **"Rescuer" User (Qualified Responder):** Obtains temporary access to the Rescuee's health and location data only within the active context of a rescue mission. Access is logged and monitored.
- **System Administrator:** Manages the technical infrastructure but does not possess private keys to decrypt user health data, ensuring confidentiality even from the service provider.

6. Retention Policy and Data Subject Rights

Retention Period: Operational data is retained for the duration of the emergency. Afterward, it is archived for medico-legal purposes for the period prescribed by law (e.g., 10 years for medical liability) or irreversibly anonymized for statistical and research purposes.

Exercise of Rights: You may exercise at any time the right of access, rectification, erasure ("right to be forgotten"), restriction, portability, and objection. You can withdraw consent via app settings, resulting in the deletion of local and remote data. For complaints, you may contact the national Privacy Authority.