


Wählen Sie Ihre bevorzugte Sprache

 IT EN ES FR DE

Erweiterte Datenschutzerklärung

Hinweis gemäß Verordnung (EU) 2016/679 (DSGVO)

Zuletzt aktualisiert: 28. Dezember 2025

RescueCom ist eine Notfallkommunikationsplattform (Proof of Concept), die im akademischen Bereich entwickelt wurde, um Rettungseinsätze in Szenarien ohne Internetverbindung zu erleichtern.

Diese Erklärung beschreibt im Detail, wie wir Ihre personenbezogenen und besonderen (Gesundheits-)Daten verarbeiten, die angewandten kryptografischen Sicherheitsmaßnahmen und Ihre Rechte. Unsere Priorität ist die Gewährleistung maximaler Vertraulichkeit: Wir verfolgen einen Ansatz von **Privacy by Design** und **Privacy by Default**, wobei die Datenerhebung auf das zur Lebensrettung Notwendige beschränkt wird.



Das System verwendet ein dezentrales Netzwerk (Mesh) in dem Sicherheit mathematisch durch End-to-End-Verschlüsselung garantiert wird. Kein Vermittler kann auf den Inhalt Ihrer Kommunikation zugreifen.

[Vollständigen rechtlichen Hinweis herunterladen \(Digital signiertes PDF\)](#)

1. Kategorien verarbeiteter Daten und Zwecke

Gemäß dem Grundsatz der Datenminimierung erheben wir ausschließlich Informationen, die für ein wirksames Notfallmanagement unerlässlich sind:

- **Allgemeine Identifikationsdaten:** Vorname, Nachname, Geburtsdatum und eine eindeutige Benutzerkennung (UUID). Diese Daten dienen der zweifelsfreien Identifizierung der Person, die Hilfe anfordert.
- **Besondere Datenkategorien (Gesundheitsdaten):** Die Verarbeitung umfasst sensible Daten, die für die medizinische Triage kritisch sind, wie: Blutgruppe, bekannte Medikamentenallergien, spezifische Behinderungen (motorisch, sensorisch oder kognitiv) und relevante chronische Erkrankungen (z.B. Diabetes, Herzkrankungen).
- **Geolokalisierungsdaten:** Präzise GPS-Koordinaten (Breitengrad/Längengrad), die in Echtzeit erfasst oder manuell eingegeben werden und ausschließlich zur Lokalisierung des Geräts in Krisenszenarien dienen.
- **Technische Telemetriedaten:** Metadaten zum Batteriestatus und zur Konnektivität, die zur Bewertung der Zuverlässigkeit des Knotens im Mesh-Netzwerk erforderlich sind.

2. Rechtsgrundlage der Verarbeitung

Die Verarbeitung Ihrer personenbezogenen Daten wird durch folgende Rechtsgrundlagen legitimiert:

- **Ausdrückliche Einwilligung:** In Übereinstimmung mit der technischen System-Pseudo-Anforderung PR_L1 erfolgt die Speicherung von Gesundheitsdaten nur nach freier, spezifischer und informierter Einwilligung, die durch eine eindeutige bestätigende Handlung (Opt-in) in der App erfolgt.
- **Schutz lebenswichtiger Interessen:** In Notfallsituationen, in denen die betroffene Person physisch oder rechtlich nicht in der Lage ist, ihre Einwilligung zu geben, ist die Verarbeitung zum Schutz des Lebens der betroffenen Person oder einer anderen natürlichen Person erforderlich.

3. Systemarchitektur und Verarbeitungsmethoden

Die Verarbeitung erfolgt über eine resiliente hybride Infrastruktur, die für den Betrieb auch in Katastrophenszenarien ausgelegt ist:

- **Lokale Speicherung (Edge):** Daten befinden sich primär auf dem Gerät des Benutzers in einer verschlüsselten SQLite-Datenbank (SQLCipher). Dies stellt sicher, dass der Benutzer den physischen Besitz seiner Daten behält.
- **Peer-to-Peer (P2P) Mesh-Netzwerk:** Ohne Internet reisen Daten durch ein Netzwerk von Geräten, die über Bluetooth LE oder Wi-Fi Direct verbunden sind. Jedes Gerät fungiert als Relay, jedoch ohne Zugriff auf die Daten (siehe Punkt 4).
- **Sichere Cloud-Synchronisation:** Wenn die Konnektivität wiederhergestellt ist, werden kritische Daten über sichere REST-APIs mit dem zentralen Server synchronisiert, um die Konsistenz der Notfall-Gesundheitsakten zu gewährleisten.

4. Technische Sicherheitsmaßnahmen

Um Risiken durch unbefugten Zugriff, Verlust oder Änderung zu mindern, implementieren wir Sicherheitsmaßnahmen auf dem neuesten Stand der Technik:

- **AES-GCM-256-Verschlüsselung:** Alle sensiblen Daten, sowohl im Ruhezustand als auch bei der Übertragung im Mesh-Netzwerk, werden mit dem Advanced Encryption Standard (AES) im Galois/Counter Mode (GCM) mit 256 Bit verschlüsselt, was Vertraulichkeit und authentifizierte Integrität garantiert.
- **Blind Relay Protokoll (RF_16):** Geräte, die Nachrichten im Auftrag anderer Benutzer weiterleiten, fungieren als "Blind Relays" (blinde Knoten). Sie transportieren verschlüsselte Pakete, ohne den Entschlüsselungsschlüssel zu besitzen, was den Zugriff auf den Inhalt von Rettungsnachrichten durch dritte Vermittler technisch unmöglich macht.
- **Schlüsselverwaltung:** Verwendung elliptischer Kurven (ECDH und ECDSA) für die sichere Aushandlung von Sitzungsschlüsseln und die digitale Signatur von Nachrichten, um Man-in-the-Middle-Angriffe zu verhindern.

5. Rollentrennung und Zugriffskontrolle

Das System erzwingt eine strikte Rollentrennung, die auf Code-Ebene definiert und unveränderlich ist:

- **Benutzer "Rescuee" (Antragsteller):** Kann ausschließlich auf seine eigenen Daten zugreifen, diese ändern und löschen. Hat keine Berechtigungen, Daten anderer Benutzer einzusehen.
- **Benutzer "Rescuer" (Qualifizierter Retter):** Erhält temporären Zugriff auf die Gesundheits- und Standortdaten des Rescuee nur im aktiven Kontext einer Rettungsmission. Der Zugriff wird protokolliert und überwacht.
- **Systemadministrator:** Verwaltet die technische Infrastruktur, besitzt jedoch keine privaten Schlüssel zur Entschlüsselung von Benutzergesundheitsdaten, wodurch die Vertraulichkeit auch gegenüber dem Dienstanbieter gewahrt bleibt.

6. Aufbewahrungsrichtlinie und Rechte der betroffenen Person

Aufbewahrungszeitraum: Betriebsdaten werden für die Dauer des Notfalls aufbewahrt. Danach werden sie zu medizinisch-rechtlichen Zwecken für den gesetzlich vorgeschriebenen Zeitraum archiviert (z.B. 10 Jahre für die ärztliche Haftung) oder für statistische und Forschungszwecke irreversibel anonymisiert.

Ausübung von Rechten: Sie können jederzeit das Recht auf Auskunft, Berichtigung, Löschung ("Recht auf Vergessenwerden"), Einschränkung, Übertragbarkeit und Widerspruch ausüben. Sie können Ihre Einwilligung über die App-Einstellungen widerrufen, was zur Löschung lokaler und entfernter Daten führt. Für Beschwerden können Sie sich an die nationale Datenschutzbehörde wenden.