Privacy Policy

ResQ Privacy Policy

1. Introduction

ResQ provides Rapid Location Emergency Response when the ResQ Bluetooth button is pressed, or via other activation methods such as shake, notification bar, or in app (availability depends on device). Where 'incident' is used in this document it refers to such an activation of the ResQ Emergency Response service.

ResQ needs to gather and use certain information about individual customers and users using the ResQ mobile application in order to protect you and them in case of an incident. This policy describes how the user's personal data is accessed, collected, handled, used, shared and stored by our ResQ team.

2. Data Accessed & Collected

We collect information from users' phones where the application is installed and depending on the permissions you/they have granted. Information the user enters into the app or website is also collected.

Here are some examples of the device and user information we collect:

- Attributes such as the device number, mobile number, battery level, the various connection statuses (cellular, GPS, Wi-Fi, Bluetooth etc). All this information is periodically collected.
- Device precise location history. Live precise location is only collected upon activation for the duration of the incident. Optionally, background precise location can be periodically collected for Geo-fencing and Crowd notification features.
- Video and audio from camera and microphone, but only during an incident when the user has activated the service.
- Any information the user provides in app or though the web portal such as name, picture, email, demographics, address, emergency contacts, medical information, etc.
- Payment information and purchase history where services or products are purchased.
- Diagnostic data such as crash data.

You may stop all collection of data easily by uninstalling the application.

3. Data Handling, Use and Sharing

Data is automatically sent to, and processed by our servers periodically. The data can be used by our ResQ Emergency Response operators to analyse and respond to the incident and send out broadcasts to warn other ResQ users through the application.

The data may be given to public and private firms to utilize the data to respond and help better protect the user during or after an incident. The data may also be used for customer support for that user when the user requests customer support.

Anonymised, aggregate data may also be used for statistical purposes.

The data will also be provided as required by law such as to comply with a subpoena or similar legal process.

We will not sell personal or sensitive user data.

4. Data Storage

Data is stored electronically in a database but can also be printed and stored in printed formats where these are useful to the company or a First Responder in order to investigate and respond to an incident.

The data is stored on Microsoft Azure cloud servers, an approved cloud servicing company.

We store data for as long as it is necessary to provide products and services to users and others. Information associated with your account/ their accounts will be kept until either any account is deleted or we decide that the data therein is no longer needed to provide products and services.

5. Security Policy

We encrypt all data (in-transit and at-rest) including sensitive information (such as credit card information) using Secure Sockets Layer (SSL) and other industry standard technologies to ensure that your Personally Identifiable Information is safe as it is transmitted and stored. For more information see https://docs.microsoft.com/en-us/azure/security/fundamentals/encryption-overview.

If you have any questions regarding this policy, our practises or otherwise, please contact us at support@resq.today.