Privacy Policy - Mobile App

Definitions

For the purposes of this Privacy Policy:

- Application refers to the Cloud Softphone application for iOS, the Cloud Softphone application for Android; published by ring-u, LLC.
- Company (referred to as either "the Company", "Our", "Us" or "We" in this privacy policy) refers to ring-u, LLC, whose head office is at 2841 Dayton Blvd. Ste C Chattanooga, TN 37415 (USA).
- Service means - VoIP service for calls, instant messaging and collaboration provided via the Application.
- Personal Data is any information that specifically identifies an individual (such as your name, user name, address or e-mail address), processed by the Company for the purposes set forth in this privacy policy. Personal Data also includes any information about an individual that is directly linked to personally identifiable information and is processed by the Company for the purposes set forth in this privacy policy. Personal information does not include "aggregate" information, which is data the Company collects about the use of the Service (such as automated crash reports) or about a group or category of users, from which individual identities or other personal information has been removed. This privacy policy in no way restricts or limits our collection and use of aggregate information.
- Device means any device that can access the Service such as a cell phone, tablet or a computer, that allows the Application to be downloaded and the Service to be used.
- User means a natural person using the Application for personal or professional purposes.

Privacy information access preface

Company is very concerned for the privacy of the users of our products. To this extent, no user information is collected except when necessary for using a specific feature of our products (Apple Push Notification Service, Firebase Cloud Messaging) and is never shared with any third parties. The only time information is requested other than listed here is for use in troubleshooting technical issues and of course, the user has the option to refuse in that case (though that may negatively affect our ability to resolve any issues).

This privacy policy contains the full list of features built into the Application that in any way process users' private information. Whether a feature is enabled or not, and thus whether the private information required for the feature to work is accessed, depends solely on the SIP account configuration in the Application.

Push Notifications

In order for Push Notifications to work, we must register your account remotely when the Application is in the background or closed on your iOS or Android device. To accomplish this, we transmit your SIP account details to SIPIS (our server that handles push notifications) over a HTTPS secure connection. This information is shared with no one and is erased immediately when the push instance expires (usually within 3-6 days, depending on SIP account configuration) or the user disables Push Notifications in the Application. If the SIP account is configured to use one of our methods for multitasking instead of Push Notifications, this information is not sent to SIPIS.

Mobile App Contacts Usage

This part of the privacy statement describes how the Company collects and uses the contact information you provide by granting the contacts access permission in the Application. It also describes the choices available to you regarding our use of your information and how you can access and update this information.
We access the following personal information from your address book:

- Contacts' names
- Contacts' email
- Contacts' telephones
- Contacts' organization
- Contacts' postal address
- Contacts' birthday
- Contacts' gender

We use this information to:

- Populate your Contacts data in the app.
- To import your favorite contacts into the QuickDial list, if you also enable the "Busy Lamp Field" feature on a contact, the favorite contact's number (URI) will be included in your SIP traffic, but will not be stored anywhere.
- Enable the Smart Contacts feature, which helps you to make free calls and enjoy seamless communication with other users with SIP accounts on the same provider. If your SIP account is configured to use the Smart Contacts feature, we securely upload your contacts to the server in order to recognize Application users among your contacts.

We will only use your Contacts information for the specific reason for which it was provided to us.

Mobile App Location Information Usage

This part of the privacy statement describes how the Company uses the location information you provide by granting the Location access permission in the Application.

We ask the location access permission only if the SIP account is configured to do so, and only in the following use cases:

- When the SIP account is used in a country with Dispatchable Location for emergency calls - legal requirement. In this situation, the app attempts to acquire your location information in case a call to an emergency number is placed. Please note that emergency calls are usually routed to your phone's native dialer instead of requesting location access. Please consult with support to learn how emergency calls are handled for your account.
- When the SIP account is configured to send location data during SIP registration.

We will only use your Location information for the specific reason for which it was provided to us.

Mobile App Media Files and Documents Usage

This part of the privacy statement describes how the Company uses media files and documents shared with the Application. Depending on the operating system, you may need to grant additional file access-related permissions to the Application in order for the Application to access files.

We process your files such as photos, videos, and documents; only if the SIP account is configured to do

so, and only in the following use cases:

- When you select the option to share a media or file attachment via a multimedia message. We always access only the files that have been explicitly shared with the Application. The attached files are always encrypted and securely uploaded to a server in order for the message recipient to download them later.
- Other use cases in which the files never leave your device. An example of such a use case is adding a photo avatar to a favorite contact (also referred to as "QuickDial").

We will only use your files for the specific reason for which they were provided to us.

Google Calendar Usage
This privacy statement describes how the Company collects and uses the information you provide in your Google Calendar account via the Application for our UCaaS products. It also describes the choices available to you regarding our use of your information and how you can access and update this information.

We collect the following personal information from your Google Calendar and Google Contacts account:

- Event name
- Event date
- Event time
- Event description (will be inserted as a note)
- Event location (will be inserted as a note)
- Contacts' names
- Contacts' email
- Contacts' telephones
- Contacts' organization
- Contacts' postal address
- Contacts' birthday
- Contacts' gender

We add/import the following personal information from your "Cloud Softphone" account to your Google Calendar & Google Contacts account:

- Event name
- Event date
- Event time
- Event description
- Event resource name

We use this information to:

- Populate your Google Calendar & Google Contacts data in your installed Application.
- Populate your Application customer data in your Google Calendar & Google Contacts account.
- Create bookings from the Application's calendar for the imported/synchronized contacts.
- Keep your Google Calendar & Google Contacts in sync with your Application customers and vice versa.
- Send booking confirmation emails, booking cancellation emails, booking update emails or booking

reminder emails to the contacts imported from Google Calendar & Google Contacts – prior to sending out such emails your consent will be sought each time.

We will only use this information for the specific reason for which it was provided to us.

Mobile App Analytics Usage

The Company may collect aggregate data that no longer identifies individual users for purposes of usage and performance analysis. This may include diagnostic data such as login counts, screen view counts or crash information.

Troubleshooting Logs Usage

For the sole purpose of troubleshooting, the Company might ask users to provide debug logs from the Application. The debug logs contain full network traffic information for application provisioning, calls, messaging and other network in-app events generated by user activity.

Retention of Information

We maintain your personal information in our regular business records while you are a customer of your Service. We may also maintain this information for a period of time after you are no longer a customer if the information is necessary for the purposes for which it was collected or to satisfy our legal requirements and/or obligations. These purposes typically include business, legal, or tax purposes. If there are no pending requests, orders, or court orders for access to this personal information, we may destroy the information once it becomes unnecessary to those purposes for which it was collected.

Security

The security of personal information is important to us. We take commercially reasonable measures and follow generally accepted standards to protect the information you provide us, both during transmission and once we receive it. For example, the information you provide is transmitted via encryption using technologies such as secure socket layer technology (SSL).

Disclosure to Third Parties

We do not share or sell your personal information to third parties. We disclose information only in the following cases: as required by law, such as to comply with a subpoena or similar legal process when we believe in good faith that disclosure is necessary to protect our rights, protect your safety or the safety of others, to investigate fraud, or to respond to a government request. If we are involved in a merger, acquisition, or sale of all or a portion of its assets, you will be notified via email and/or a prominent notice through our app of any change in ownership or uses of your personal information, as well as any choices you may have regarding your personal information to any other third party with your prior consent to do so.

Privacy Statement Updates

We may update this privacy statement to reflect changes to our business or this app as it pertains to the information collected from you and our use of it. If the change impacts how we use or handle information collected from you, we will email you and/or your company's Google administrator, or post a notice where you first access this app prior to the change becoming effective. We encourage you to periodically review this page for the latest information on our privacy practices.

Support

As a user, you can request the following:

- Confirmation of access to personal data concerning you
- Access to the processed personal data concerning you.
  - Please note that pieces of personal data stored in encrypted format can only be provided in its encrypted form.
  - Please note that once data is removed it cannot be restored.
- Correct inaccurate or incomplete personal data concerning you
- Erase processed personal data concerning you
- Arrange how personal data concerning you should be processed in event of your death

To process a request, please send us an email to support@ring-u.com with the following:

- Subject of request, your name(s) and first name(s);
- Scan of both sides of your passport or identity card to enable us to verify your identity

Company support will respond to requests in a timely manner (within 30 days of request). Company support might ask you for further information, such as a username or a phone number, in order to determine what information has been collected about you.

If you have any questions or concerns about our privacy policy, please contact us at support@ring-u.com.

From:
https://wiki.ring-u.com/wiki/ - **support wiki**

Permanent link:
https://wiki.ring-u.com/wiki/doku.php?id=privacypolicy

Last update: **2025/11/02 18:49**