Privacy Policy

Ring for a …

Last updated: 5 June 2026

1. Introduction

This Privacy Policy explains how Ring for a … (“the App”, “we”, “our”) collects, uses, and protects information when you use our mobile application available on Android and iOS. By using the App, you agree to the practices described in this policy.

We are committed to protecting your privacy. We collect only the minimum data necessary to provide the App’s core functionality and improve the user experience.

2. Information We Collect

2.1 Information You Provide

- Display name – an optional name you set so your partner can identify you when you ring them. This name is transmitted to our backend server solely for the purpose of delivering notifications.

2.2 Information Collected Automatically

- Device identifier – a randomly generated UUID created locally on your device and stored in local app storage. It is used to identify your device on our backend and is never linked to your real identity.
- Firebase Cloud Messaging (FCM) token – a push notification token issued by Google Firebase. It is sent to our backend to enable delivery of bell-ring notifications. The token may be refreshed periodically by the system.
- Ring history – a local log of ring events (type and timestamp) stored exclusively on your device. This data is never uploaded to any server.
- App settings and preferences – stored locally on your device (sound, haptics, dark mode, language, selected preset, etc.). Not transmitted to any server.
- Achievements and gamification data – stored locally on your device only.

2.3 Feedback and Optional Diagnostics

When you submit feedback through the App, we collect the feedback category and the message you choose to provide. This information is transmitted to our backend so we can review your request, investigate issues, and improve the App.

- Contact e-mail – optional. If you choose to provide your e-mail address, we use it only to respond to your feedback or support request. Providing an e-mail address is not required to send feedback.
- Basic feedback metadata – when feedback is sent, we may include basic technical information such as App version, build number, environment, platform (Android/iOS), operating system version, device model, manufacturer, whether the device is physical or an emulator/simulator, locale, and time zone. This helps us understand which App version and device environment the feedback relates to.

- Optional diagnostics – if you enable the “Attach diagnostic data” option, the App may also send additional technical diagnostic data, such as current App screen/route, selected theme, notification permission status, connectivity type, premium/subscription status, number of paired connections, selected bell type, recent sanitized API errors, recent Flutter exceptions and stack traces, push notification status, hashed FCM token, RevenueCat status/error information, short in-memory App logs, selected App settings, and basic performance metrics such as App uptime or recent API duration.
- Custom bell text – the full text of a custom bell is not automatically included in diagnostics. Diagnostics may only indicate that a custom bell text exists and its approximate length, unless you explicitly type that text into your feedback message.
- Screenshots – the App does not currently collect or upload screenshots as part of feedback.
- Data we do not include in feedback or diagnostics – we do not intentionally collect or send raw FCM/APNs tokens, authentication tokens, refresh/session tokens, Authorization headers, cookies, passwords, payment card details, purchase tokens, store receipts, advertising identifiers, IMEI, MAC address, device serial number, precise GPS location, contacts, clipboard content, installed app lists, private message content, notification content, names or identifiers of paired users, full API request/response bodies, full local storage, or raw RevenueCat customer information.

2.4 Data Collected by Third-Party Services

The App integrates the following third-party SDKs, each of which may collect data independently according to their own privacy policies:

- **Firebase –** Google Firebase (Firebase Cloud Messaging, Firebase Core) may collect device and diagnostics data. Privacy policy: https://firebase.google.com/support/privacy
- **RevenueCat –** RevenueCat processes in-app purchase and subscription data, including purchase receipts and subscription status. RevenueCat does not receive personally identifiable information from the App. Privacy policy: https://www.revenuecat.com/privacy
- **Google AdMob –** Google Mobile Ads (AdMob) may collect advertising identifiers and usage data to display personalised or contextual advertisements. Ads are shown only to users on the free plan. Privacy policy: https://policies.google.com/privacy

3. How We Use Your Information

We use the collected information for the following purposes:

- To deliver bell-ring notifications to your paired partner’s device.
- To identify your device on our backend and maintain the pairing connection.
- To display your chosen name in notifications received by your partner.
- To process and verify in-app subscription purchases through RevenueCat.
- To display advertisements to free-tier users via Google AdMob.
- To maintain and improve the App’s functionality and stability.
- To receive and process feedback, bug reports, and support requests submitted by users.
- To diagnose and reproduce technical issues when you choose to attach optional diagnostic data.

We do not sell, rent, or share your personal information with third parties for marketing purposes. Data is shared with third-party SDKs only to the extent required to provide the services described above.

4. Device Pairing and Backend Data

The App allows you to pair your device with a partner's device. To enable this feature, your device identifier, FCM token, display name, and pairing status are stored on our backend server. This data is used exclusively to route ring notifications between paired devices.

Pairing data is deleted from our servers when you disconnect the pairing within the App. Backend data is stored on servers operated by our hosting provider and is protected by industry-standard security measures.
Custom bell text or preset label – when you ring a paired device, the selected bell label may be transmitted through our backend and Firebase Cloud Messaging to deliver the notification. This data is used only to deliver the notification and is not used for advertising.

5. Data Retention

- Device identifier and FCM token are retained on our servers for as long as your device is actively paired or registered. They are removed when you delete the pairing or uninstall the App and your device is deregistered.
- Display name is retained on our servers alongside the device record and is deleted together with it.
- Local data (ring history, settings, achievements) is retained on your device until you uninstall the App or clear its data.
- Subscription and purchase data is retained by RevenueCat in accordance with their data retention policy.
- Feedback messages are retained for as long as reasonably necessary to review and resolve the request, improve the App, and maintain support records.
- Optional contact e-mail addresses provided with feedback are retained only for the purpose of responding to the feedback or support request and are not used for marketing.
- Optional diagnostic data attached to feedback is retained only as long as reasonably necessary for troubleshooting and App improvement. Diagnostic data is stored separately from advertising data and is not used for advertising or profiling.

6. Data Security

All communication between the App and our backend is transmitted over HTTPS/TLS. Each device is authenticated using a randomly generated secret key stored locally. We implement reasonable technical and organisational measures to protect the data we hold against unauthorised access, loss, or disclosure. However, no method of transmission over the internet or electronic storage is 100% secure.

Before diagnostic data is sent, the App is designed to sanitize the payload and remove or mask sensitive values such as tokens, authorization headers, cookies, e-mail addresses, phone numbers, pairing codes, and other accidental identifiers where technically feasible.

7. Your Rights

Depending on your location, you may have the following rights regarding your personal data:

- Right of access – you may request a copy of the personal data we hold about your device.

- Right to rectification – you may correct your display name at any time within the App settings.
- Right to erasure – you may request deletion of your device record and associated data by contacting us (see Section 10). Disconnecting all pairings within the App and uninstalling it will remove most data automatically.
- You may also request deletion of feedback records, optional contact e-mail addresses, and diagnostic data associated with your device or support request, where we can identify the relevant record.
- Right to restriction – you may request that we restrict processing of your data.
- Right to data portability – you may request your data in a machine-readable format.
- Right to object – you may object to data processing based on our legitimate interests.

To exercise any of these rights, please contact us using the details in Section 10. We will respond within 30 days.

8. Children's Privacy

The App is not directed to children under the age of 16. We do not knowingly collect personal information from children under 16. If you believe a child under 16 has provided us with personal information, please contact us and we will take steps to delete such data promptly.

9. Changes to This Privacy Policy

We may update this Privacy Policy from time to time. When we do, we will revise the "Last updated" date at the top of this page. If the changes are significant, we will provide a more prominent notice (for example, a notification within the App). We encourage you to review this policy periodically.

Your continued use of the App after changes are posted constitutes your acceptance of the updated Privacy Policy.

10. Contact Us

If you have any questions, requests, or concerns about this Privacy Policy or the handling of your data, please contact us at:

Email: info@progity.com

App: Ring for a … (Android / iOS)

We will do our best to address your concerns promptly and in accordance with applicable law.