

PhotoCall – Privacy Policy

Effective Date: 15 August 2026

PhotoCall is a simple photo-contact dialer that allows users to save names, phone numbers, and photos and quickly place calls. PhotoCall also provides optional Google Sign-In and Google Drive backup and restore features.

This Privacy Policy explains what information PhotoCall uses, where it is stored, and the choices available to users.

1. Information used by PhotoCall

PhotoCall may use the following information:

- **Contact information:** Names and phone numbers entered by the user or imported with the user's permission.
- **Contact photos:** Images selected using the system photo picker or captured using the device camera.
- **Google account information:** If the user chooses to sign in with Google, PhotoCall may access basic account information provided by Google, such as the user's name, email address, profile picture, and account identifier.
- **Backup information:** If the user chooses to create a Google Drive backup, the saved PhotoCall contacts and associated photos may be uploaded to the user's own Google Drive account.
- **Optional on-device usage information:** Call count or last-called time may be stored locally to improve the user experience. This information is not currently used to reorder the contact list.

Google Sign-In and Google Drive backup are optional. Users can continue using PhotoCall's main contact and calling features without creating a Google Drive backup.

PhotoCall does not contain advertising SDKs and does not use information for advertising or behavioural tracking.

2. How PhotoCall uses information

PhotoCall uses information only to provide its features, including:

- Displaying contacts created or imported by the user.
- Showing contact names, photos, and phone numbers.
- Placing a phone call when the user taps a contact.
- Allowing users to edit or delete contacts.
- Signing the user into their Google account when requested.
- Backing up PhotoCall data to the user's Google Drive when the user selects the backup option.
- Restoring PhotoCall data from the user's Google Drive when requested.
- Displaying basic Google account information within the app.
- Opening external links or supported applications when requested by the user.

PhotoCall does not sell users' personal information.

3. Google Sign-In and Google Drive

Google Sign-In is used to connect PhotoCall with the Google account selected by the user.

If the user chooses to make a backup, PhotoCall uploads the backup directly to the selected Google Drive account using Google's services. The backup may contain:

- Contact names.
- Phone numbers.
- Contact photos.
- Other app information required to restore the contacts.

The backup is stored in the user's Google Drive account and is governed by Google's privacy and security practices. The developer does not operate a separate server for storing PhotoCall backups.

PhotoCall requests only the Google permissions necessary to provide sign-in, backup, and restore functionality. Google account information and Drive access are not used for advertising.

PhotoCall's use and transfer of information received from Google APIs will comply with the **Google API Services User Data Policy**, including its Limited Use requirements.

4. Where information is stored

On the device

PhotoCall contact information and app settings are stored in the app's private storage on the user's device. Contact photos may also be stored in the app's private directory.

Under normal Android protections, other applications cannot access PhotoCall's private app data.

In Google Drive

If the user voluntarily creates a backup, a copy of the relevant PhotoCall data is stored in the user's Google Drive account.

Google Drive backups are associated with the Google account selected by the user. Google processes and protects this information according to the Google Privacy Policy and applicable Google Drive terms.

5. Data sharing

PhotoCall does not sell users' personal information or share it with advertisers.

Information may be processed by Google when the user uses Google Sign-In or Google Drive backup and restore. This processing is necessary to provide the feature requested by the user.

When users open an external service, such as an email application, social-media link, browser, or UPI application, that service may process information according to its own privacy policy.

6. Permissions and their purposes

Depending on the device, Android version, and features used, PhotoCall may request:

- **Phone/Call permission:** To place a phone call when the user taps a contact.
- **Contacts permission:** To import contacts from the device when requested by the user.
- **Camera permission:** To capture a photo for a contact.
- **Photos, Media, or Images permission:** To select a contact image, where required by the Android version. PhotoCall may use the Android system photo picker instead.
- **Internet permission:** To use Google Sign-In, communicate with Google Drive for backup and restore, and open online links.
- **Google account authorization:** To connect the selected Google account and access the Google Drive functionality required for backup and restore.

Permissions are used only to provide the related app features.

7. Data retention and deletion

Data stored on the device

Local information remains on the device until the user:

- Deletes an individual contact in PhotoCall.
- Clears PhotoCall's app data through Android Settings.
- Uninstalls PhotoCall.

When a user replaces or deletes a contact photo, PhotoCall may remove the associated local photo file when it is no longer needed.

Data stored in Google Drive

Google Drive backup data remains in the user's Google Drive until it is replaced or deleted by the user, or removed through an available PhotoCall backup-management feature.

Uninstalling PhotoCall or clearing its local app data may not automatically delete a backup already stored in Google Drive.

Users can manage their Google account's connected applications and revoke PhotoCall's access through their Google Account settings. Revoking access prevents future access but may not automatically delete an existing backup file.

Users may contact the developer at the email address below for assistance with privacy or deletion-related questions.

8. Security

PhotoCall relies on Android's app sandbox and Google's authentication and Drive services to help protect users' information.

PhotoCall does not send contact data or backup data to a server operated by the developer. However, no electronic storage or transmission method is completely secure. Users should protect their devices and Google accounts with suitable security measures.

9. Children's privacy

PhotoCall is not specifically directed to children under 13. The developer does not knowingly collect personal information from children.

If a parent or guardian believes that a child has provided personal information through PhotoCall, they may contact the developer for assistance.

10. External services

PhotoCall may interact with services or applications operated by third parties, including:

- Google Sign-In.
- Google Drive.
- Email applications.
- Web browsers.
- Social-media services.
- UPI applications, if a support or donation option is provided.

The privacy practices of these services are governed by their respective privacy policies.

Google Privacy Policy:

<https://policies.google.com/privacy>

11. Changes to this Privacy Policy

This Privacy Policy may be updated when PhotoCall's features or data practices change. The revised policy will be published with an updated effective date.

12. Contact

For questions, privacy requests, or assistance related to data deletion, contact:

Email: pushpendrahypernova@gmail.com

Short summary for Google Play Data Safety

- **Advertising ID:** Not used.
- **Advertising:** No advertising SDKs.
- **Local contact data:** Stored on the user's device.
- **Google account information:** Used for optional Google Sign-In and Google Drive connection.
- **Cloud backup:** Contact names, phone numbers, photos, and required app data may be transferred to the user's Google Drive only when the user requests backup.
- **Data selling:** No.
- **Developer-operated server storage:** No.
- **Deletion:** Users can delete local contacts, clear app data, uninstall the app, delete their Google Drive backup, or revoke Google account access.