

Privacy Policy

Document version: 1.0

Effective date: July 1, 2026

Last updated: July 1, 2026

1. Scope

This Privacy Policy explains how information is handled in the PaperToPhone Android application, on the PaperToPhone website and when you contact PaperToPhone support.

2. Privacy overview

PaperToPhone is designed with privacy in mind. The Android application does not require a user account and does not automatically transmit application data to the developer or to developer-operated servers.

3. Information processed in the application

Users may enter employee names, shift information, tasks, notes, reminders and optional sickness-related absence information. By default, this information is stored locally on the Android device.

Application data may leave the device only when:

- the user explicitly exports a backup;
- Android includes the data in a system backup; or
- the user voluntarily provides information when requesting support.

The developer cannot access locally stored application data unless the user voluntarily provides it.

4. Responsibility for employee information

The user or organization using PaperToPhone determines why employee information is entered and how it is used. That user or organization is responsible for complying with applicable data protection, employment and workplace rules.

The developer does not receive or control employee information that remains stored locally in the application. Users should enter only information that is necessary and that they are authorized to process.

5. Local storage

Application data is stored locally in an SQLite database and in local application settings. PaperToPhone does not provide developer-operated cloud storage or synchronization.

6. Backup and export

PaperToPhone creates a JSON backup only when the user explicitly requests one. The user chooses where the backup file is stored.

Exported JSON backup files are not encrypted. Users are responsible for storing and protecting exported backups securely and for deleting them when they are no longer needed. If the user selects a cloud storage provider or another application as the destination, that provider's privacy policy and security practices apply.

7. Android system backup

PaperToPhone does not initiate Android system backups. If device backup is enabled, Android may include the application's local database and settings in a system backup according to the device and Google Account settings.

Android system backups must be managed separately through the user's Android or Google Account settings. Clearing application data or uninstalling PaperToPhone may not immediately delete copies retained in an Android system backup.

8. Android permissions

PaperToPhone uses only the Android permissions required for reminder functionality:

- **POST_NOTIFICATIONS** – displays reminder notifications;
- **RECEIVE_BOOT_COMPLETED** – restores scheduled reminders after a device restart;
- **USE_EXACT_ALARM** – triggers reminders at the time selected by the user; and
- **VIBRATE** – provides vibration for reminder notifications.

The application does not request permissions for location, camera, microphone, contacts or SMS.

9. Analytics, advertising and tracking

The Android application does not include analytics, advertising, tracking or crash-reporting SDKs. PaperToPhone does not sell application data or use it for advertising or profiling.

10. Health-related information

If a user records sickness-related absence information, it remains on the device unless it is included in a user-initiated export, an Android system backup or information voluntarily provided to support.

The user or organization using PaperToPhone is responsible for ensuring that it has a lawful basis and appropriate authorization to record this information.

11. Data security

Local application data is protected by Android's application sandbox and the security measures enabled on the user's device. PaperToPhone does not automatically transmit application data to the developer or to developer-operated servers.

Users should protect their devices with an appropriate screen lock and keep exported backups in a secure location. No method of storage can guarantee absolute security.

12. Support correspondence

When you contact support@papertophone.com, we process your email address, message and any attachments solely to respond to your request and maintain reliable customer support.

Support correspondence is processed on the basis of our legitimate interest in answering support requests and operating the support service. Email hosting is provided by Nethely Kft. as a service provider.

Support communications are retained until the request has been resolved and thereafter only for as long as reasonably necessary for follow-up, security or legal obligations. You may request deletion of your support correspondence unless retention is required by law.

13. Website data

The PaperToPhone website is a static website and does not use analytics, advertising trackers or marketing cookies.

Like most websites, the hosting server processes limited technical information when a page is requested. This may include the IP address, date and time, requested page, response status, referring page and browser user-agent. These server logs are used only to maintain security, diagnose errors and operate the website reliably.

Server logs are processed on the basis of our legitimate interest in securing and operating the website and are normally deleted within 14 days. Website infrastructure providers may process this technical information only as necessary to provide hosting services.

14. Data retention and deletion

- **Local application data:** remains on the device until the user deletes records, clears the application data or uninstalls the application.
- **Exported backups:** remain under the user's control until deleted by the user.
- **Android system backups:** are controlled through the user's Android or Google Account settings.
- **Support correspondence:** is retained as described in Section 12.
- **Website server logs:** are normally retained for no longer than 14 days.

15. Your privacy rights

Depending on applicable law, you may have the right to request access to, correction of, deletion of or restriction of personal data processed by the developer. You may also have the right to object to processing based on legitimate interests.

These rights apply to information controlled by the developer, such as support correspondence and identifiable website logs. The developer cannot access or delete data stored only on your device, in your exported backups or in your Android system backup.

To exercise your rights, contact support@papertophone.com. You also have the right to lodge a complaint with the Hungarian National Authority for Data Protection and Freedom of Information (NAIH) at www.naih.hu.

16. Children's privacy

PaperToPhone is a professional workplace tool and is not designed or directed toward children.

17. Changes to this Privacy Policy

This Privacy Policy may be updated when the application, website or applicable requirements change. The latest version and its effective date will be published on this page.

18. Contact

Developer: Forgács László

Country: Hungary

Email: support@papertophone.com

Website: <https://papertophone.com>