clogra Privacy Policy (English)

This document describes how the locally operated daily report app clogra handles personal data.

clogra Privacy Policy

Last updated: 17 November 2026

This Privacy Policy ("Policy") explains how clogra (the daily report application, "App") handles personal data and related information. Work data such as daily reports is stored on the device. Section 3 explains communication by Google Play Billing on Android.

1. Information collected

The App stores information on the device only when the user enters it, including:

- Daily report data (work description, worker names, hours, man-days, etc.)
- Site and project configuration data
- Employee information (names, roles, etc.)
- Signature data (prime contractor signatures)
- App settings (language preferences, device-specific settings)

2. Purpose of use

Collected information is used only for the following purposes:

- Creating, editing, and storing daily reports and work logs
- Generating PDF outputs
- Maintaining app settings required for proper operation
- Improving usability for the user

3. Data sharing and third parties

Work data is not sent automatically. If you share a file such as a PDF, it is passed to your selected destination. The App does not collect advertising IDs.

The Android app uses Google Play Billing for purchases and restoration. The library may send Google encrypted billing diagnostics, such as response and error codes, device model, OS version and network type, to monitor billing operation and analyze faults. These diagnostics do not contain daily reports, photos, signatures or PDF contents. Google Play processes payment information. clogra does not receive payment method details such as card numbers. https://policies.google.com/privacy?hl=en

4. Data retention

Data is stored on the device until the user deletes it. Because data may be lost if the App is uninstalled or the device is damaged, we recommend that important information be backed up as PDFs or other formats when necessary.

5. Security

Because data is stored locally, users are responsible for securing their devices. Recommended security measures include:

- Using OS-level screen lock
- Using passcodes or biometric authentication
- Managing PDFs appropriately when sending them outside the organization

6. User rights
Users can:
- View the data they have entered
- Edit or update data
- Delete data
- Change app settings
Because we do not store any user data on our own servers, we cannot respond to requests for data disclosure from our side.

7. Compliance with laws
The App is designed to comply with the Act on the Protection of Personal Information in Japan and other applicable privacy laws and regulations as far as reasonably possible.

8. Contact
For questions about this Policy, please contact:
clogra support: clogra2025@gmail.com

9. Changes to this Policy
We may update this Policy as necessary. The latest version will always be published on the official clogra website.

10. Operator information
The App is operated by the clogra development team.
Contact: clogra2025@gmail.com