Privacy & Data Policy

MINIZORA / iOS & Android
Effective date: October 26, 2026

MiniZora compresses and converts images, videos, audio, and documents. This policy explains how the app handles the files you select, local settings, and technical diagnostics in its current implementation.

1. Files and on-device processing

MiniZora reads the files you choose through the system file or media picker. It uses file contents, names, file types, sizes, and local file references to import, preview, process, and save your results. Compression and conversion run on your device. The app does not upload your selected files to a MiniZora server for processing.

If you choose a file from a cloud storage provider, or save a result to one, that provider may transfer the file under its own privacy practices. This is separate from MiniZora's local compression pipeline.

2. Local storage and retention

Imported working copies and generated results are stored in temporary app folders. MiniZora attempts to remove these folders when a processing session is reset or its resources are disposed of. An interruption or crash may leave temporary files until a later cleanup or operating system cache removal. Immediate or secure erasure is not guaranteed.

Files you explicitly export remain in the destination you choose until you delete them there. Device backups, cloud synchronization, and external storage providers may retain additional copies. MiniZora also stores your selected language locally so it can restore that preference.

3. Crash reports and technical data

MiniZora integrates Google Firebase Crashlytics to diagnose crashes and processing failures and improve reliability. Crash reporting is enabled by default in non-debug builds when initialization succeeds; debug builds disable collection by default. The current app does not provide an in-app crash reporting switch.

Reports may include crash traces, error descriptions, app and operating system information, device details, and installation identifiers collected by the SDK. Developer-defined diagnostic text is filtered to redact common file paths, filenames, email addresses, URLs, and secrets before submission. Filtering reduces exposure but cannot guarantee removal of all personal information, and does not control all automatically collected SDK data.

Your data, choices & controls

4. Service providers and data sharing

Crash diagnostics are sent to Google Firebase Crashlytics for reliability monitoring. MiniZora's current implementation does not include user accounts, advertising SDKs, or Google Analytics event tracking, and does not implement the sale of personal data. Operating system services and any storage provider you select handle data under their own policies.

Google states that Crashlytics retains crash traces and associated identifiers for 90 days before beginning removal from live and backup systems. Google may process diagnostic data outside your country. See Firebase Privacy and Security (firebase.google.com/support/privacy) for provider processing, retention, and international transfer information.

5. Access, permissions, and security

You control which files you select and where results are saved. System permissions, when required, are used to support the requested file operation and can be managed in device settings. Restricting access may prevent some app functions from working.

MiniZora uses app storage and platform access controls for working files. Do not assume that compression removes embedded metadata, location information, document properties, or other sensitive content. Review files before sharing them. No storage or transmission method can guarantee absolute security.

6. Managing and deleting your data

You can delete exported files using the destination app or device file manager. Clearing app data, where supported, or uninstalling MiniZora removes app-local data according to your operating system's behavior. These actions do not delete exported files, backups, cloud copies, or diagnostic reports already received by Firebase.

For privacy questions or requests concerning diagnostic data, use the developer contact or support channel shown on MiniZora's official app store listing. Avoid sending private files or sensitive information unless needed to resolve your request. The ability to locate a diagnostic report may be limited because MiniZora does not require an account.

7. Children and policy updates

MiniZora does not require age information or create user profiles. File contents may contain information about other people, including children; select and share only files you are authorized to use. A parent or guardian with privacy concerns can contact the developer through the official store listing.

This policy may be updated when app behavior or service providers change. The effective date identifies the version of this document. Review the current policy supplied with the app for changes.