

Stanca Privacy Policy

Full technical version

Effective date: 5 August 2026

Last updated: 5 August 2026

Contact: hello@stanca.app

This document is the complete technical Privacy Policy for the Stanca mobile application (iOS and Android). A shorter, everyday-language summary is published on the Stanca website. By using Stanca, you agree to this Privacy Policy. If you do not agree, do not use the App.

1. Who we are

Stanca is a personal expense-tracking app. It helps you capture receipts, record spending, and optionally synchronise data with your own Google account (Google Drive and Google Sheets). For privacy questions or requests, email hello@stanca.app.

2. Overview

- Stanca is local-first: your expense data is stored primarily on your device.
- Optional Google features run in your Google account — we do not operate a separate cloud account for your expenses.
 - Receipt text is extracted on your device (on-device OCR).
 - We do not sell your personal data.
 - We do not show third-party advertising in the App.
 - You can use core features offline; sync and Google Sign-In need a network connection.

3. Information we collect

Depending on how you use Stanca, we may process the categories below.

3.1 Account and identity (Google Sign-In)

When you sign in with Google, we receive information your Google account shares with the App, typically:

- Name
- Email address
- Profile identifier / basic profile photo URL (if provided by Google)
- OAuth tokens needed to keep you signed in and to access features you authorise

We request only the Google permissions needed for the product (see Section 5).

3.2 Expense and budget data (you create)

You may enter or generate:

- Amounts, currencies, exchange rates used for conversion
- Merchants, categories, notes, dates, and statuses
- Budgets and related thresholds
- Sync status and related metadata

This data is stored on your device. If you enable Google sync, verified expense information may be written to a Google Spreadsheet you own, and receipt files may be uploaded to a Google Drive folder associated with the App in your account.

3.3 Receipts and images

With your permission, the App may access:

- Camera — to photograph receipts

- Photo library / media images — to select existing receipt or payment screenshots

Images may be stored locally until (or after) upload to your Google Drive when sync is enabled. Optical character recognition (OCR) runs on device to suggest amounts and related fields. You review and can edit results before saving.

3.4 Device and diagnostics

To keep the App reliable, we may collect:

- Crash reports and non-fatal error diagnostics (via Firebase Crashlytics), including device/OS information, app version, and redacted error messages
- Limited operational events for reliability (we do not use advertising analytics to profile you for ads)

We design logging so that OAuth tokens, full receipt OCR payloads, payment card numbers, and similar sensitive strings are not intentionally sent in diagnostics.

3.5 Notifications

With your permission, Stanca may send local notifications (for example budget-related reminders). Notification permission is optional and can be changed in system settings.

3.6 Information we do not collect

Stanca does not intentionally collect:

- Precise location / GPS tracking for advertising
- Contacts, call logs, or SMS
- Full access to your entire Google Drive or Gmail
- Payment card numbers as a payment processor (if a receipt image contains card digits, treat that as incidental content of an image you chose to capture; do not rely on the App as a PCI service)

4. How we use information

We use information to:

- Provide expense tracking, OCR suggestions, budgets, and multi-currency features
- Authenticate you and maintain your session
- Synchronise receipts and expenses with your Google Drive and Google Sheets when enabled
- Diagnose crashes and improve stability
- Respond to support and privacy requests
- Comply with law where required

We do not sell personal information. We do not use your expense or receipt content to train third-party advertising models.

5. Google permissions and third-party services

5.1 Google

With your consent, Stanca may use:

- Sign-In — OpenID, basic profile, email
- Receipts — Google Drive files created or opened by the App (drive.file-style access; not full Drive)
- Expenses — Google Sheets spreadsheet(s) created or used by the App for your workspace

Google's processing of data in your Google account is governed by Google's Privacy Policy (<https://policies.google.com/privacy>) and your Google account settings.

Important: When data is written to Drive or Sheets, it resides in your Google account. You control that account, including sharing, deletion, and Google retention rules.

5.2 Firebase (Google)

We use Firebase Crashlytics (and may use related Firebase/Google infrastructure) for crash and error reporting. See Google Firebase privacy disclosures: <https://firebase.google.com/support/privacy>

5.3 Other processors

Hosted infrastructure needed to operate Google Sign-In, Drive, Sheets, and Firebase may process technical data (IP address, device identifiers used by those services) under those providers' terms.

6. Where data is stored

- Expenses, budgets, local receipt copies, sync queue — on your device (local database / app storage)
- Sign-in tokens & workspace identifiers — secure storage on your device
- Synced receipts — your Google Drive
- Synced expense rows — your Google Sheets workbook
- Crash diagnostics — Firebase / Google systems

Android cloud backup of app data is disabled to reduce unintended copies of financial data onto device backups where configurable.

We do not operate a Stanca-branded server that stores your full expense history as the primary database of record.

7. Legal bases (EEA / UK / similar)

Where applicable, we process personal data under:

- Contract / service delivery — to provide the App features you request
- Consent — camera, photos, notifications, and Google OAuth scopes
- Legitimate interests — security, fraud prevention, crash diagnostics (balanced against your rights)
- Legal obligation — where we must respond to lawful requests

You may withdraw consent for device permissions in system settings and revoke Google access in your Google Account permissions.

8. Sharing of information

We share information only as needed to operate the App:

- With you / your Google account — Drive and Sheets sync
- With service providers — Google Sign-In, Drive, Sheets, Firebase Crashlytics
- With authorities — if required by law, court order, or to protect rights and safety
- Business transfer — if Stanca is involved in a merger, acquisition, or asset sale, information may transfer under continued confidentiality protections where feasible

We do not sell personal information and do not share expense content with data brokers for advertising.

9. Retention

- On device: Data remains until you delete it in the App, clear app storage, uninstall the App, or use in-app workspace/local wipe features where available.
- Google Drive / Sheets: Retained according to your Google account until you delete those files or the App's workspace reset/trash flows remove App-managed items (subject to Google Trash retention).
- Sign-out: Clears the local session and tokens on the device. Sign-out does not by itself delete files already in your Drive or spreadsheet.
- Crash diagnostics: Retained according to Firebase / Google product retention practices.

10. Your choices and rights

Depending on your location, you may have rights to access, correct, delete, restrict, or export personal data, and to object to certain processing.

You can typically:

- Edit or delete expenses and receipts in the App
- Revoke Google access at <https://myaccount.google.com/permissions>
- Delete Drive files / Sheets created by Stanca in your Google account
- Uninstall the App to remove local app storage (subject to OS behaviour)
- Contact hello@stanca.app for privacy requests

We will respond within a reasonable period and as required by applicable law. We may need to verify your request.

California / similar US state laws: We do not “sell” or “share” personal information for cross-context behavioural advertising as those terms are commonly defined. You may still contact us to exercise access/deletion rights where applicable.

11. Children’s privacy

Stanca is not directed at children under 13 (or the higher age required in your country, such as 16 in some regions). We do not knowingly collect personal information from children. If you believe a child has provided personal information, contact us and we will take appropriate steps to delete it.

12. Security

We use reasonable technical and organisational measures appropriate to an expense app, including:

- Encrypted transport (HTTPS / TLS) for network calls
- Secure storage for OAuth tokens on device
- Limited Google scopes (not full Drive or Gmail)
- Avoidance of logging sensitive payloads where feasible

No method of storage or transmission is 100% secure. You are responsible for securing your device and your Google account (strong password, 2-Step Verification recommended).

13. International transfers

Google and Firebase may process data in the United States and other countries. Where required, those providers use appropriate transfer mechanisms (for example Standard Contractual Clauses). By using Google-powered features, you acknowledge that your data may be processed outside your country of residence.

14. Permissions summary (stores)

- Internet — Sign-In, sync, exchange rates, crash reporting
- Camera — Capture receipts
- Photos / media images — Import receipts and payment screenshots
- Notifications (optional) — Budget and related reminders
- Google account — Identity + Drive/Sheets sync you enable

15. App Store and Play Store disclosures

This policy is intended to support:

- Apple App Privacy / nutrition labels
- Google Play Data safety form

Summary aligned with current product behaviour:

- Name, email — Yes (Google Sign-In) — Account
- User content (expenses, receipt images) — Yes — On device; optional sync to your Drive/Sheets
- Crash logs / diagnostics — Yes — Firebase Crashlytics

- Precise location — No
- Advertising ID for ads — No (no third-party ads)
- Data sold — No
- Data used for tracking across apps/websites for ads — No

Complete store forms to match this policy and your live build. Update both when features change.

16. Changes to this policy

We may update this Privacy Policy from time to time. The “Last updated” date will change when we do. Material changes will be communicated in a reasonable way (for example in-app notice or an updated hosted URL). Continued use after changes means you accept the updated policy, where permitted by law.

17. Contact

Privacy requests and questions:

Email: hello@stanca.app

If we appoint an EU / UK representative or change our legal entity name, this section will be updated.