Privacy Policy for SplitDay

Last Updated: April 4, 2026

---

1. INTRODUCTION

This Privacy Policy explains how **SplitDay** ("App," "we," "us," "our") collects, uses, stores, and shares your personal information. By using the App, you consent to the practices described in this Privacy Policy.

> **Note:** We take your privacy seriously, especially given the sensitive nature of custody and co-parenting data.

---

2. INFORMATION WE COLLECT

2.1 Information You Provide

- **Account Information:** Name, email address (when signing in via Google or Apple).
- **Custody Data:** Parent names, display names, custody patterns, exchange records, day overrides, shift hours.
- **Financial Data:** Expense amounts, descriptions, categories, vendor names, split ratios, payment status.
- **Receipt Images:** Photos of receipts you upload, which are compressed and may be stored in the cloud.
- **Messages:** In-app messages sent within Households, including sender name, message text, timestamps, and read status.
- **Helper/Contact Data:** Names, relationships, and notes for helpers (babysitters, grandparents, etc.).
- **Holiday Data:** Custom and imported holiday entries.
- **Child Information:** Child name (optional, in budget settings). Custody patterns implicitly relate to children's time with each parent.
- **Preferences:** Calendar view settings, notification preferences, language/locale.

2.2 Information Collected Automatically

- **Device Information:** Device type (iOS/Android), operating system version, app version.
- **Usage Analytics:** App opens, feature usage, screen views, errors (via Firebase Analytics).
- **Crash Reports:** Crash logs, stack traces, device state at time of crash (via Firebase Crashlytics).
- **Advertising Identifiers:** Device advertising ID (IDFA on iOS, GAID on

Android), subject to your consent.
- **Push Notification Tokens:** Firebase Cloud Messaging tokens for delivering notifications.
- **Subscription Status:** Purchase history and subscription state (via RevenueCat).

2.3 Information Processed by AI

When you use AI-powered features:

- **Receipt Scanning:** Receipt images are sent to **Google Gemini** for text extraction. Images are processed in real-time and are subject to Google's data handling policies.
- **Tone Analysis:** Message text drafts are sent to **Google Gemini** for tone assessment. Message content is processed in real-time.

---

3. HOW WE USE YOUR INFORMATION

Purpose	**Legal Basis (GDPR)**
Providing custody calendar and scheduling features	Performance of contract
Syncing data across devices (Pro users)	Performance of contract
Enabling Household sharing between co-parents	Performance of contract
Processing in-app messages	Performance of contract

Tracking expenses and budget	Performance of contract
Storing and retrieving receipt images	Performance of contract
AI receipt scanning and tone analysis	Consent / Performance of contract
Sending push notifications	Consent
Serving advertisements (free tier)	Legitimate interest
Analytics and app improvement	Legitimate interest
Crash reporting and bug fixing	Legitimate interest
Managing subscriptions and purchases	Performance of contract
Complying with legal obligations	Legal obligation

---

4. DATA STORAGE AND SECURITY

4.1 Local Storage

- All app data is stored locally on your device in an encrypted database (**Hive**).

- Local data persists until you reset the App or uninstall it.

4.2 Cloud Storage

- **Pro subscribers'** data is stored in **Google Firebase** (Firestore and Firebase Storage).
- Firebase uses encryption at rest and in transit (TLS/SSL).
- Receipt images are stored in Firebase Storage at: `receipts/{userId}/{expenseId}.jpg`.

4.3 Security Measures

- **Firebase App Check** prevents unauthorized API access.
- Authentication via **Google Sign-In** and **Apple Sign-In** (OAuth 2.0).
- **No security system is 100% secure.** We cannot guarantee absolute security of your data.

---

5. DATA SHARING AND THIRD-PARTY SERVICES

5.1 Third-Party Service Providers

Service	Provider	Data Shared	Purpose
Firebase Auth	Google	Email, name, auth tokens	User authentication
Cloud Firestore	Google	Custody data, expenses, messages	Cloud storage and sync
Firebase Storage	Google	Receipt images	Cloud receipt vault

Analytics	Google	Usage events, device info	App improvement
Crashlytics	Google	Crash logs, device info	Bug fixing
Cloud Messaging	Google	FCM tokens, device type	Push notifications
AI (Gemini)	Google	Receipt images, message drafts	AI scanning and tone analysis
RevenueCat	RevenueCat	User ID, purchase history	Subscription management
Google AdMob	Google	Device ID, IP address	Ads (free tier only)
Facebook Events	Meta	App events, purchase events	Analytics and attribution
Nager.Date	Public API	Country code	Holiday data retrieval

5.2 Household Data Sharing

When you join or create a Household, your custody data, expense data, and messages are shared with other Household members according to permission settings. **You control what data is shared by managing Household permissions.**

5.3 We Do NOT:

- **Sell** your personal information to third parties.
- **Share** your custody data, messages, or financial data with advertisers.
- **Provide** your data to data brokers.

---

6. ADVERTISING

- **Free-tier users** see advertisements served by Google AdMob.
- AdMob may collect device identifiers and IP addresses to serve personalized or contextual advertisements.
- On iOS 14.5+, we request **App Tracking Transparency (ATT)** permission. You may decline without losing access to the App.
- **Pro subscribers** do not see advertisements and their data is not shared with AdMob.

---

7. CHILDREN'S PRIVACY

- The App is intended for adults (parents/guardians) and is not directed at children under 13.
- We do not knowingly collect personal information from children under 13.
- The App processes children's information (names, schedules) **only** as entered by adult users.

---

8. DATA RETENTION

- **Local Data:** Retained until you reset the App, uninstall it, or clear app data.
- **Cloud Data:** Retained for as long as your account exists.
- **Analytics/Crash Reports:** Retained for up to 14 months (Analytics) or 90 days (Crashlytics).
- **Account Deletion:** Cloud data is deleted within **30 days** of a verified deletion request.

---

9. YOUR RIGHTS

9.1 All Users

- **Access:** Export your data in **CSV format** at any time.
- **Deletion:** Reset local data via the App or request cloud deletion via email.
- **Opt-Out:** Disable analytics or ads personalization through device settings.

9.2 EU/EEA Residents (GDPR)

Under the GDPR, you have the right to access, rectification, erasure ("right to be forgotten"), restriction of processing, data portability, and the right to object.

- **Data Controller:** SplitDay, techxplay@gmail.com

---

10. CONTACT US

For privacy questions, data requests, or concerns:

Email: techxplay@gmail.com

By using SplitDay, you acknowledge that you have read and understood this Privacy Policy.