

# Privacy Policy — FutureApp

---

**Last updated:** 22 February 2026 **App name:** FutureApp **Contact:** [gdpr@futuredomain.com](mailto:gdpr@futuredomain.com)

---

## 1. Data Controller

---

FutureApp ("we", "us", "our") is the data controller for your personal data processed through the FutureApp mobile and web application ("the App"). For any privacy-related inquiries, contact us at [gdpr@futuredomain.com](mailto:gdpr@futuredomain.com).

---

## 2. What Data We Collect

---

### 2.1 Account Data

- Email address (required for registration)
- Username and display name
- Avatar/profile photo (optional)
- Phone number (optional)
- Language preference

### 2.2 Authentication Data

- Password (hashed, never stored in plaintext)
- OAuth tokens when signing in via Google or Apple

### 2.3 Event Data

- Event titles, descriptions, dates, and locations (including coordinates)
- Event images
- Sub-event details

### 2.4 Financial Data

- Expense descriptions and amounts
- Receipt photos or PDFs
- Settlement records (who owes whom)
- Currency information

## 2.5 Transportation Data

- Departure locations and coordinates
- Available seats and costs for ride offers

## 2.6 Communication Data

- Invitation emails (invitee email addresses)
- Push notification tokens (device identifiers for notifications)
- In-app notification history

## 2.7 Feedback Data

- Event ratings (1–5 stars)
- Optional written feedback comments

## 2.8 Device & Technical Data

- Device type (iOS, Android, Web)
- Error logs and stack traces (only when Sentry error tracking is enabled; sensitive data such as passwords and tokens are automatically redacted)

---

# 3. How We Use Your Data

---

Purpose	Legal Basis (GDPR)
Account creation and authentication	Performance of contract (Art. 6(1)(b))
Event creation, management, and participation	Performance of contract (Art. 6(1)(b))
Expense tracking and debt settlement	Performance of contract (Art. 6(1)(b))
Sending event invitations by email	Legitimate interest (Art. 6(1)(f))
Push notifications (reminders, updates)	Consent (Art. 6(1)(a))

Purpose	Legal Basis (GDPR)
Geocoding addresses to coordinates	Legitimate interest (Art. 6(1)(f))
Error monitoring and debugging (Sentry)	Legitimate interest (Art. 6(1)(f))

## 4. Third-Party Processors

We share your data with the following service providers, each acting as a data processor on our behalf:

Processor	Data Shared	Purpose	Location
<b>Supabase Inc.</b>	All account, event, and financial data; stored images	Database, authentication, file storage, real-time updates, serverless functions	US (configurable region)
<b>Resend Inc.</b>	Invitee email addresses, event titles	Sending invitation emails	US
<b>Expo (820 Labs Inc.)</b>	Push notification tokens, notification content	Delivering push notifications	US
<b>Sentry (Functional Software Inc.)</b>	Error logs, stack traces (sensitive data redacted)	Error tracking and debugging (optional, disabled by default)	US
<b>OpenStreetMap / Nominatim</b>	Address queries, coordinates	Geocoding (converting addresses to map coordinates)	EU/Global
<b>Google (OAuth &amp; Maps)</b>	Email, profile data (OAuth); map tile requests (Maps, Android only)	Authentication; map rendering	US
<b>Apple Inc.</b>	Email, profile data (OAuth)	Authentication (Sign in with Apple)	US

Data Processing Agreements (DPAs) are in place or available upon request with each processor. For transfers outside the EU/EEA, Standard Contractual Clauses (SCCs) or equivalent safeguards apply.

## 5. Data Retention

---

Data Type	Retention Period
User profile	Retained until account deletion. Soft-deleted profiles are retained for expense calculation integrity.
Event and expense data	Retained for the lifetime of the event, or until the account is deleted.
In-app notifications	Automatically deleted after <b>30 days</b> .
Push notification tokens	Retained until the user logs out or uninstalls the app.
Error logs (Sentry)	Subject to Sentry's retention policy (default: 90 days).

---

## 6. Your Rights Under GDPR

---

As an EU/EEA resident, you have the following rights:

- **Right of Access (Art. 15)** — Request a copy of all personal data we hold about you.
- **Right to Rectification (Art. 16)** — Correct inaccurate data via your profile settings, or by contacting us.
- **Right to Erasure (Art. 17)** — Request deletion of your account and associated data. Note: certain financial records may be retained in anonymised form for expense integrity.
- **Right to Data Portability (Art. 20)** — Request your data in a machine-readable format. Contact us to initiate an export.
- **Right to Restrict Processing (Art. 18)** — Request that we limit how we use your data.
- **Right to Object (Art. 21)** — Object to processing based on legitimate interest.
- **Right to Withdraw Consent (Art. 7(3))** — Withdraw consent for push notifications at any time via your device settings.

To exercise any of these rights, contact us at [gdpr@futuredomain.com](mailto:gdpr@futuredomain.com). We will respond within **30 days**.

---

## 7. Device Permissions

---

Permission	Purpose	Required?
Camera	Taking photos for avatars, event images, and expense receipts	Optional
Photo Library	Selecting existing photos for upload	Optional
Location (foreground only)	Geocoding event addresses to map coordinates	Optional
Notifications	Receiving event reminders and updates	Optional

We do **not** access your contacts, microphone, calendar, SMS, or background location.

---

## 8. Data Security

---

- All data is transmitted over HTTPS/TLS encryption.
  - Passwords are hashed and never stored in plaintext.
  - Row-Level Security (RLS) policies enforce strict data isolation — users can only access events they participate in.
  - Expense receipts are stored in a private storage bucket accessible only to event participants.
  - Sensitive data (passwords, tokens, API keys) is automatically redacted from error logs.
- 

## 9. Cookies and Tracking

---

The App does **not** use cookies for advertising or analytics. We do **not** integrate any analytics services (no Google Analytics, Firebase Analytics, Mixpanel, or similar). The only optional tracking is Sentry error monitoring for debugging purposes, which is disabled by default.

---

## 10. Children's Privacy

---

The App is not intended for use by children under the age of 16. We do not knowingly collect personal data from children. If you believe a child has provided us with personal data, please contact us for immediate deletion.

---

## 11. Data Breach Notification

---

In the event of a personal data breach that poses a risk to your rights and freedoms, we will: - Notify the relevant supervisory authority within **72 hours** (Art. 33 GDPR). - Notify affected users without undue delay if the breach poses a high risk (Art. 34 GDPR).

---

## 12. Changes to This Policy

---

We may update this Privacy Policy from time to time. We will notify you of material changes via in-app notification or email. The "Last updated" date at the top reflects the most recent revision.

---

## 13. Contact & Complaints

---

For any questions or complaints regarding this Privacy Policy or your data:

- **Email:** [gdpr@futuredomain.com](mailto:gdpr@futuredomain.com)
- **Supervisory Authority:** You have the right to lodge a complaint with your local data protection authority or the relevant authority in your EU/EEA country of residence.