

Foresee App Privacy Policy (Beta)

Last modified: October 17, 2025

Introduction

Capacity Creator Corp. (the “Company”, “we”, “us”) operates the Foresee mobile application (the “App”). This policy explains how we collect, use, disclose, and protect personal information when you download, install, register with, access, or use the App and related services.

By downloading, registering with, or using the App during the beta, you acknowledge that features are pre-release and may change, and you consent to our collection and use of additional diagnostics and feedback to improve stability, performance, and user experience.

This policy applies only to information we collect in the App (and in email, text, and other electronic communications sent through or in connection with the App). It does not apply to information collected offline, on our websites, or by third parties that may link to or be accessible from the App.

If you do not agree with our policies and practices, do not download, register with, or use the App.

Information We Collect About You and How We Collect It

We collect information:

- Directly from you when you provide it (for example, by filling in forms or corresponding with us).
- Automatically when you use the App (for example, usage details, device data, crash logs, and diagnostic telemetry).
- From integrations you choose to connect (for example, calendar, task, fitness/wellness platforms, or single sign-on).

Information You Provide to Us

Depending on the features you use, we may ask you for: name, email address, password or login credential, profile photo/alias; preferences (e.g., notification settings,

time zone); feedback/support messages, survey responses, bug reports, feature requests; and content you choose to submit (e.g., notes or journal entries). If you engage in purchases in future phases, we may request payment information at that time (not applicable during this beta).

You may sign up with name, email, and password (with email verification) or by using Google or Apple single sign-on (SSO).

Health and Wellness Data (Integrations)

If you choose to connect Apple HealthKit (iOS) or Google Fit/Health Connect (Android), the App may request read access to categories you select (e.g., steps, exercise minutes, heart rate, heart rate variability (HRV), sleep, mindfulness). These platforms can also make sensitive categories available (e.g., reproductive health, pregnancy, nutrition logs). We request only the categories you choose, and you can grant, withhold, or revoke each category in your device settings. Data obtained through these integrations is used only for wellness features and not for advertising.

On-device processing: Your burnout score remains on your device by default; we do not access it. If multi-device sync is later introduced, we will provide advance notice, additional consent, and safeguards (e.g., encryption).

Spotify (optional): If you connect your Spotify account, we may receive listening activity to personalize audio experiences. You can disconnect Spotify at any time in the App or in Spotify settings.

Automatic Information Collection and Tracking Technologies

When you access or use the App, we automatically collect certain details of your use (e.g., screens viewed, session duration), device and network information (e.g., device type, OS, language, IP address, device identifiers), performance metrics, diagnostic logs, and crash data.

- **Location:** We do not collect precise GPS; we may derive coarse location from IP.
- **Cookies/SDKs:** Our web properties use cookies; the mobile App may use SDKs that perform similar functions (e.g., analytics/telemetry). Where available, you can adjust analytics/telemetry settings in the App.
- **No Online Behavioural Advertising in beta:** We do not conduct cross-app tracking for targeted advertising during beta.

Third-Party Information Collection

When you use the App or its content, certain third parties may collect information about you or your device, including: analytics/telemetry providers, cloud hosting/support vendors, and single sign-on providers. These parties may collect information using SDKs or similar tools to provide their services to us (e.g., crash diagnostics). We do not use third-party advertising networks in the beta.

Third-party services may include: Firebase Analytics, Firebase Crashlytics, Firebase Cloud Messaging, Apple StoreKit, Google Play Billing, Google and Apple SSO, Spotify, cloud database hosting (Postgres), and Replit Mail. We do not use third-party advertising networks during the beta.

How We Use Your Information

We use information to:

- Provide and operate the App (including account creation, authentication, personalization, and core features).
- Run the beta program (diagnose issues, perform A/B testing, measure performance, enhance stability and usability).
- Communicate with you (service notices, updates, onboarding, security alerts, and, where permitted, product tips or surveys).
- Maintain the security and integrity of the App (fraud, abuse, and threat detection and prevention).
- Comply with legal obligations and enforce terms.
- Personalize audio if you connect Spotify.
- Measure engagement with tools and tasks (frequency, duration, completion) to improve features.

Burnout score privacy: Burnout calculations remain on your device by default; we do not access them.

We may create de-identified or aggregated information for analytics and reporting, and we will not attempt to re-identify such data.

No advertising during beta: We do not sell personal information or show third-party targeted ads in the beta.

In-App Purchases and Subscriptions (Planned)

There are no purchases during this beta. After soft launch, we plan to introduce subscriptions through Apple StoreKit and Google Play Billing. Pricing will be announced before purchases are enabled. Before enabling purchases, we will update this policy.

Disclosure of Your Information

We may disclose personal information:

- To service providers that support the App (e.g., hosting, storage, diagnostics/telemetry, email delivery, support tooling, security monitoring). They are restricted to using information only to provide services to us and must protect it.
- For business transactions, such as a merger, acquisition, financing, or sale of assets, subject to applicable law and existing commitments.
- For legal/safety reasons, to comply with law, legal process, or governmental requests; to enforce our terms; and to protect users, the public, or Capacity Creator.
- At your direction, for example when you connect an integration or share a report.

Transferring Your Personal Information

Availability: The App is intended for users in Canada, excluding Québec.

Platforms during beta: Mobile (iOS and Android) only

If accessed from outside Canada, this policy still applies as a Canadian privacy notice.

We and our service providers may process and store information in Canada and the United States for hosting, diagnostics, email delivery, and support. When information is processed outside your province or outside Canada, it may be subject to foreign laws and lawful access by courts, law enforcement, and national security authorities. We implement contractual and organisational safeguards. Where required by provincial law (e.g., Alberta PIPA), we disclose the countries involved and the purposes of foreign service providers and provide contact information for questions. By submitting personal information or using the App, you consent to such transfers, storage, and processing.

For more information about our service providers and the safeguards used for cross-border processing, contact our Privacy Officer at privacy@capacitycreator.com.

Choices About How We Use and Disclose Your Information

We strive to provide choices, including:

- Telemetry/analytics: In App settings (where available), you can disable non-essential analytics/telemetry.
 - Telemetry controls during beta: No in-App toggle at launch, Email opt-out only
 - During beta, if in-App controls are not available, you may email privacy@capacitycreator.com to request disabling non-essential analytics.
- Location: You can control device-level location permissions. Disabling precise location will limit location-based features.
- Promotional emails: Where required, we obtain express consent (consistent with CASL) before sending marketing communications. You can unsubscribe using in-message links or by contacting us; unsubscribing does not affect service or security messages.
- Account deletion (beta): Request deletion by contacting privacy@capacitycreator.com
- Data export (beta): Request a copy of your information by contacting privacy@capacitycreator.com

Data Security

We use administrative, technical, and physical safeguards appropriate to the sensitivity of the information (including encryption in transit, role-based access controls, and audit logging). No system is perfectly secure; we continuously assess and enhance our protections. Report security issues to security@capacitycreator.com.

Data Retention

We retain personal information only as long as necessary to fulfill the purposes described in this policy (or as required/permitted by law). Current beta defaults (subject to refinement for production):

- Account data: retained while your account is active and for up to 24 months after last activity.
- Crash logs: retained up to 18 months when Crashlytics is enabled.
- In-app feedback and surveys: retained up to 24 months.
- De-identified/aggregated analytics: retained without a defined expiry because they no longer reasonably identify you.
- Burnout scores: stored on-device only; not retained by us. If sync is added, retention rules will be updated.

When retention periods expire, we delete or de-identify information, subject to legal holds. A detailed retention schedule is available on request.

Use of the App by Minors

The App is not intended for individuals under 18 years of age. We do not knowingly collect personal information from anyone under 18. If we learn that we have collected personal information from a person under 18 without proper consent, we will delete that information promptly.

Accessing and Correcting Your Personal Information

You may request access to or correction of your personal information, or ask questions about our policies and practices (including cross-border processing and retention), by contacting us at privacy@capacitycreator.com. We may need to verify your identity. Where permitted by law, we may refuse requests that are unreasonable or would infringe others' privacy, and we will explain why (subject to legal restrictions).

Your rights under Canadian law: As an organization subject to PIPEDA, you have rights to access and request correction of your information, subject to limited exceptions. If you are not satisfied with our response, you may file a complaint with the Office of the Privacy Commissioner of Canada.

Withdrawing Your Consent

Where we rely on consent, you may withdraw it at any time (subject to legal/contractual restrictions and reasonable notice) by contacting privacy@capacitycreator.com or using available in-App controls. We will explain any service impact so you can make an informed decision.

Changes to Our Privacy Policy

We may update this policy from time to time. If we make material changes, we will notify you (e.g. email, in-App notice) and, where required, obtain consent before the changes apply. The "Last modified" date shows the latest revision.

Contact Information and Challenging Compliance

Privacy Officer at Capacity Creator Corp.

Email: melanie@capacitycreator.com

Mailing address: [Insert mailing address]

We have procedures to receive and respond to questions, complaints, and requests about our handling of personal information and our compliance with this policy and applicable privacy laws.

Beta-Specific Notices

- Pre-release: Features and data flows may change quickly during beta; we will update this policy for material changes and, where required, seek renewed consent.
- Diagnostics during beta: We may enable Firebase analytics and crash reporting to improve stability.
- Feedback: Suggestions and feedback you provide may be used to develop and improve the App without obligation to you.
- Privacy by default: Where feasible, settings are initially configured to the most protective levels; you can adjust them in Settings.
- Payments: No purchases during beta; subscriptions may be added later with notice.