Dinary Privacy Policy

Effective July 15, 2026 | Version 1.0

Operator	First Taste Ventures Ltd.
Applies to	the Dinary mobile application, website, waitlist, beta programs, and related services (collectively, the "Service")

This Privacy Policy explains how First Taste Ventures Ltd. collects, uses, discloses, retains, and safeguards personal information through the Service. It is intended to provide meaningful, understandable notice. It does not replace any just-in-time notice or consent request shown when a feature is used.

1. Scope and accountability

First Taste Ventures Ltd. is accountable for personal information under its control, including information processed by service providers on its behalf. This Policy applies to visitors, waitlist members, beta testers, registered users, and people who communicate with us.

A designated privacy lead oversees this Policy, privacy requests, vendor reviews, and incident response. Questions or complaints may be sent to founder@dinary.net. We will investigate and respond within a reasonable period and as required by applicable law.

This Policy does not govern third-party services reached through external links or independent restaurants, merchants, advertisers, reservation services, or payment providers. Their own notices apply to information they collect independently.

2. Information we collect

2.1 Information you provide

- Account and profile information, such as name or display name, username, email address, password credential or authentication token, profile image, biography, preferences, and account settings.
- User content, such as food and venue photographs, captions, reviews, flame ratings, tags, comments, saved items, reports, and metadata you add to a post.
- Location information you choose to provide, such as a city, restaurant, tagged place, or precise or approximate device location when you grant permission.
- Communications, survey answers, waitlist details, support requests, beta feedback, contest entries, and correspondence with us.
- Transaction and entitlement information if paid features, subscriptions, marketplace transactions, or rewards are offered. Payment card details may be collected directly by an app store or payment processor rather than by Dinary.

2.2 Information collected automatically

- Usage information, including screens viewed, searches, taps, posts viewed, interactions, session timing, referral information, feature use, and inferred content preferences.
- Device and technical information, including IP address, device and app identifiers, device model, operating system, language, time zone, app version, network information, and push-notification token.
- Diagnostics and security information, including crash reports, performance data, error logs, authentication events, suspected abuse signals, and records needed to secure the Service.
- Cookie, SDK, pixel, local-storage, and similar technology data on the website and, where applicable, in the app.

2.3 Information from other sources

We may receive information from authentication providers, app stores, analytics or infrastructure providers, restaurant and mapping-data providers, rewards partners, users who interact with you, public sources, and business partners. If a social or third-party login is offered, the provider will describe what it shares before you connect it.

2.4 Information we do not request at launch

At launch, Dinary does not intend to request access to contacts, microphone, Bluetooth, calendar, health data, motion and fitness data, or local network devices. We will update disclosures and request permission before using a new protected device capability. Dinary does not use Apple or Android system permission data to create a database for sale.

3. Device permissions and choices

- Camera: used only when you choose to capture a photo or other supported media for a post or profile. Dinary does not continuously access the camera.
- Photo library: used when you choose media to upload or save. Where supported, Dinary may use a limited photo picker rather than full-library access.
- Location (optional): used for nearby discovery, tagging a restaurant or place, local feeds, regional recommendations, events, offers, fraud prevention, and other location-enabled features described at the point of use. Precise location is not required when approximate location or a manually selected city is sufficient.
- Notifications (optional): used for account and security notices, social activity, product messages, beta invitations, rewards, promotions, and local updates according to your settings. Push tokens are used to route notifications.
- Tracking permission: Dinary will request App Tracking Transparency permission before engaging in tracking as Apple defines that term. Denial will not block core app access. If no tracking occurs, no tracking request is required.

You can change system permissions in device settings. Withdrawing a permission stops future access through that permission but does not automatically erase information already lawfully collected. You may use available deletion controls or contact us.

4. Why we use information

- Provide accounts, profiles, diaries, feeds, search, posting, ratings, comments, saves, moderation, support, and other requested features.

- Personalize and rank content, recommend dishes or places, infer taste preferences, match similar tastes, and create local or contextual discovery experiences.
- Operate beta tests; diagnose errors; measure performance; conduct product analytics, research, forecasting, and service improvement.
- Detect spam, fraud, security incidents, policy violations, and manipulation of ratings or rewards; enforce agreements and protect users.
- Send transactional messages and, with any consent required by law, marketing, promotions, coupons, partner offers, and product news.
- Administer subscriptions, rewards, badges, promotions, contests, marketplace features, restaurant tools, creator programs, and partnerships.
- Comply with law, respond to lawful requests, establish or defend legal claims, complete corporate transactions, and maintain business records.
- Create statistics and insights that have been aggregated or de-identified so they are not reasonably capable of identifying an individual.

Artificial intelligence and automated features

Dinary may use machine learning or artificial intelligence to classify images, suggest tags or dishes, detect unsafe content, identify trends, rank recommendations, and develop taste or restaurant insights. We may use content and interaction data to evaluate and improve Dinary-controlled models or features where permitted by law and disclosed at the relevant time. We will not disclose personal information to an unaffiliated third-party AI provider for that provider's independent model training without additional notice and any consent required by law or platform rules. Automated outputs may be inaccurate and should not be treated as dietary, allergy, medical, or safety advice.

5. Consent and legal grounds

We obtain consent appropriate to the sensitivity of the information and the context. Consent may be express, such as enabling precise location, opting into marketing, or authorizing tracking, or implied where a use is obvious and reasonably expected, such as uploading a selected photo. We may also process information without consent where permitted or required by applicable law.

You may withdraw consent, subject to legal or contractual restrictions and reasonable notice. Withdrawal may prevent a feature from working. We will not make core access conditional on unnecessary location, notification, or tracking permission.

6. When we disclose information

- Public and social features: profile and post information you choose to publish may be visible to other users and may be reshared or captured by them.
- Processors and service providers: hosting, storage, content delivery, authentication, mapping and places data, analytics, crash reporting, communications, moderation, security, customer support, payment, and AI-processing providers acting for Dinary under contractual restrictions.
- Partners you choose to engage: restaurants, merchants, rewards providers, event organizers, creators, reservation or delivery providers, and marketplace participants when needed to complete a request or with notice and consent where required.
- Legal, safety, and integrity: authorities, advisers, insurers, counterparties, and affected parties where reasonably necessary to comply with law, protect rights or safety, investigate misconduct, or establish and defend claims.

- Business transactions: prospective or actual purchasers, investors, lenders, and advisers in a financing, reorganization, merger, sale, or transfer, subject to confidentiality and applicable notice requirements.
- Aggregated or de-identified information: statistics and insights that are not reasonably capable of identifying you may be used and disclosed for research, analytics, restaurant dashboards, trend reports, advertising measurement, APIs, and commercial licensing.

Dinary does not sell personal and sensitive user data as prohibited by Google Play policy. If Dinary introduces a practice considered a sale or sharing under an applicable privacy law, we will provide required notice and opt-out rights before that practice begins. We do not permit service providers to use personal information for unrelated purposes.

7. Advertising, analytics, cookies, and communications

We may use first-party analytics and service providers to measure use and reliability. Website cookies are described in the Cookie & Analytics Policy. Non-essential cookies will be subject to consent where required.

If interest-based advertising or cross-company tracking is introduced, Dinary will update this Policy and app-store disclosures, provide any legally required controls, and use Apple's App Tracking Transparency framework where applicable. Location, notifications, or tracking will not be required to obtain compensation or core functionality.

You may unsubscribe from commercial email using the message link. Service, safety, legal, and account communications may still be sent.

8. Retention, deletion, and account closure

We retain personal information only as long as reasonably necessary for the disclosed purposes, legal obligations, dispute resolution, safety, and enforcement. Retention varies by category, sensitivity, account status, contractual need, and backup cycle.

- Active account information and public content are generally retained while the account is active or until deleted.
- After a verified deletion request, Dinary will delete or de-identify the account and associated personal information within a reasonable period, subject to permitted exceptions. User-identifiable posts will be removed from public display.
- Dinary may retain minimal records needed for fraud prevention, security, legal compliance, tax/accounting, dispute resolution, and enforcement for the applicable limitation or statutory period.
- Residual copies may remain in encrypted backups until overwritten through the ordinary backup cycle and will not be restored to active use except for disaster recovery, security, or legal necessity.
- Aggregated ratings, statistics, and genuinely de-identified insights that cannot reasonably be linked back to the user may be retained indefinitely. A venue's aggregate rating may therefore change less than the removal of an individual post would suggest.
- Information independently provided by another user or third party is not part of the deleted account, although Dinary will assess valid privacy or rights requests relating to it.

Instructions and further detail appear in the Account Deletion & Data Retention Policy. Deactivation is not account deletion.

9. Your rights and choices

Subject to law and identity verification, you may request access to or correction of personal information, withdraw consent, ask questions about disclosures, request deletion, and challenge our compliance. We may refuse or limit a request only where permitted by law and will explain the reason where required.

Requests may be sent to founder@dinary.net. We may ask for information sufficient to verify the request and protect the account. Authorized agents must provide evidence of authority. We do not discriminate for exercising privacy rights.

10. Security and privacy incidents

We use safeguards appropriate to the sensitivity of information, which may include access controls, encryption in transit, credential hashing, logging, backups, vendor controls, staff confidentiality, and incident-response procedures. No system is completely secure.

Where required under PIPEDA or other applicable law, Dinary will assess breaches, keep required records, notify affected individuals, and report to regulators when a breach creates a real risk of significant harm or another reporting threshold is met.

11. Cross-border processing

Dinary and its service providers may process information in Canada, the United States, and other jurisdictions. Information may therefore be accessible to courts, law enforcement, or national-security authorities under local law. Dinary remains accountable for information transferred to processors and uses contractual or other safeguards appropriate to the circumstances.

12. Children and youth

The Service is not directed to children under 13, and Dinary does not knowingly collect their personal information. A person under the age of majority should use the Service only with permission of a parent or legal guardian where required. If we learn that information was collected from a child who could not provide meaningful consent, we will take appropriate steps to delete it. Parents or guardians may contact founder@dinary.net.

13. Changes and contact

We may update this Policy to reflect product, legal, or operational changes. The updated version will show a revised date. We will provide prominent notice and seek additional consent where required for material new uses. Continuing to use the Service after an effective update signifies acknowledgment, but does not replace consent where law requires express consent.

Contact: First Taste Ventures Ltd., Privacy Lead, founder@dinary.net. You may also raise an unresolved concern with the Office of the Privacy Commissioner of Canada or another competent regulator.