

PRIKME, INC.

PRIVACY POLICY

Effective Date: May 4, 2026

This Privacy Policy describes how Prikme, Inc., a Delaware corporation qualified to do business in California (“Prikme,” “we,” “us,” or “our”), collects, uses, discloses, and protects information in connection with the Prikme mobile applications, related websites, and online services (collectively, the “Platform”). Prikme operates the Platform as an internet-based technology marketplace that provides advertising, appointment booking, and patient information services connecting prospective patients (“Patients”) with independent licensed healthcare professionals (“Providers”) offering aesthetic and wellness services. Prikme is not a healthcare provider and does not deliver medical, nursing, aesthetic, or wellness services.

This Privacy Policy applies to all users of the Platform, including Patients, Providers, and individuals administering business accounts on behalf of Provider organizations. By accessing or using the Platform, you acknowledge that you have read and understood this Privacy Policy.

1. Scope and Relationship to Other Policies

This Privacy Policy applies solely to information collected by Prikme through the Platform. It does not apply to information collected, used, or disclosed by Providers in their capacity as healthcare providers; the privacy and security of Provider-collected health information are governed by each Provider’s own privacy practices and notices and by applicable law. To the extent Prikme transmits or stores protected health information on a Provider’s behalf, Prikme acts as a “business associate” of that Provider under the Health Insurance Portability and Accountability Act of 1996 (“HIPAA”), and the relevant Business Associate Agreement between Prikme and the Provider governs the handling of such information. The California Confidentiality of Medical Information Act (Civil Code section 56 et seq.) (“CMIA”) applies independently of HIPAA and is also addressed in this Policy.

2. Information We Collect

2.1 Information You Provide Directly.

When you register for or use the Platform, we collect the information you provide, including:

Account information: first name, last name, email address, mobile telephone number, password (which is stored only in salted, hashed form by our authentication infrastructure), and your role on the Platform (Patient, Provider, or business account administrator).

Patient profile information: name, contact details, and (if you elect) saved payment method tokens stored by our payment processor.

Provider profile information: professional biography, profile and gallery photographs, business address, services offered and pricing, license type, license number, license state, National Provider Identifier (NPI), supervising or delegating physician information where applicable, and professional liability insurance details (carrier and expiration).

Identity verification information (Providers only): government-issued photo identification (such as a driver's license or passport) and license documentation, used solely to verify professional licensure during onboarding.

Booking information: appointment date and time, services selected, group size, service address, deposit amount, and any optional notes you provide.

Patient health information: information you submit through intake forms, consent forms, treatment notes, before-and-after photographs, and similar materials in connection with a Provider appointment.

Communications: in-app messages between Patients and Providers, content of support requests, and any other communications you direct to Prikme.

Reviews and ratings: written reviews, star ratings, and any related information you submit about a Provider following a completed booking.

Legal acceptances: records of your acceptance of the Patient Platform Waiver, Terms of Service, End User License Agreement, this Privacy Policy, and any other legal acceptances, including the version of the document you accepted, the date and time of acceptance, your IP address, and the platform and version of the device used.

2.2 Information Collected Automatically.

When you use the Platform, we and our service providers collect certain information automatically, including device identifiers, IP address, mobile operating system and version, application version, browser user-agent, crash and error data, log data, and approximate or precise geolocation as described in Section 2.3.

2.3 Location Information.

The Platform uses your device's built-in location services to compute the distance between Patient addresses and Provider service areas. Location data is collected only while the Platform is being used in the foreground; the Platform does not collect location data in the background. The Platform uses the operating system's native location and geocoding services (Apple location

and geocoding services on iOS; Android Location Services and Geocoder on Android) and does not transmit your location to third-party advertising networks.

2.4 Payment Information.

Payments are processed by Stripe, Inc. and Stripe Connect Express on behalf of Providers. Prikme does not collect, store, or have access to full payment card numbers, card verification values, or other PCI-scope data. Prikme stores only payment metadata, including Stripe customer identifiers, payment intent identifiers, the last four digits of the card used, and amounts charged.

2.5 Information from Third Parties.

In the course of verifying Provider licensure, Prikme may obtain information from publicly available licensure databases, the National Provider Identifier registry, and state medical or professional licensing boards. Prikme does not purchase personal information about Patients or Providers from data brokers.

2.6 Sensitive Personal Information.

Some of the information described above is “sensitive personal information” under the California Privacy Rights Act, including precise geolocation, account login credentials, government-issued identifiers (Provider only), and information concerning health. Prikme uses sensitive personal information only for the purposes for which it was provided and other purposes permitted under California Civil Code section 1798.121, and does not use or disclose sensitive personal information for the purpose of inferring characteristics about you.

3. How We Use Information

Prikme uses the information described above to: operate, maintain, and improve the Platform; create and manage user accounts; verify Provider licensure and credentials; facilitate bookings and process payments; transmit intake forms, consents, and waivers between Patients and Providers; deliver transactional communications such as booking confirmations, appointment reminders, password resets, and support replies; protect the security and integrity of the Platform; detect, investigate, and prevent fraud and other unlawful activity; comply with applicable law; and enforce our Terms of Service, End User License Agreement, and other contractual rights.

Prikme does not use personal information for cross-context behavioral advertising and does not sell or share personal information for advertising or third-party marketing purposes. Prikme does not engage in profiling of users for advertising purposes, and the Platform does not currently use artificial intelligence or automated decision-making to rank, match, or recommend Providers. Search results are presented in randomized order. If Prikme later introduces ranking, automated matching, or similar features, this Privacy Policy will be updated and, where required, additional notice or consent will be obtained.

4. How We Share Information

Prikme shares information only as described in this Section.

4.1 With Providers.

When you book an appointment, Prikme shares relevant Patient information with the Provider you select, including your name, contact details, appointment details, service location, completed intake forms, completed consent forms, signed waivers, and any photographs or other information you submit through the Platform in connection with the appointment. The Provider's use and disclosure of that information is governed by the Provider's own privacy practices and applicable law.

4.2 With Service Providers.

Prikme shares information with vendors that provide services on Prikme's behalf and that are contractually limited to using personal information only as needed to perform their services. These vendors include:

Supabase, Inc. — cloud database, authentication, file storage, and real-time infrastructure. Supabase stores all user account data, profile data, booking and payment metadata, intake and consent forms, treatment notes, before-and-after photographs, and in-app messages. Photographs and form documents are stored in private storage buckets with row-level security so that access is limited to the assigned Provider and the Patient.

Stripe, Inc. (including Stripe Connect Express) — payment processing, including authorization, capture, refunds, and Provider payouts.

Twilio Inc. — transactional SMS messaging (booking confirmations, appointment reminders, intake-form links, support replies). Marketing SMS is not used.

Resend (Resend Inc.) — transactional email (booking confirmations, password resets, administrative invitations, support replies). Marketing email is not used.

Google LLC — to the extent Firebase Cloud Messaging is enabled in the future, transactional push notifications.

Apple Inc. and Google LLC — distribution of the Platform through the Apple App Store and Google Play, and operating-system services such as native location and geocoding.

Codemagic Ltd. — build and continuous-integration services. No end-user personal information is processed by Codemagic.

To the extent any service provider receives, maintains, or transmits protected health information on Prikme's behalf, Prikme has entered into or will enter into a Business Associate Agreement with that service provider as required by HIPAA.

4.3 For Legal and Safety Reasons.

Prikme may disclose information when required to comply with applicable law, valid legal process, or governmental request; to enforce our agreements; to protect the rights, property, or safety of Prikme, our users, or others; and to investigate or prevent suspected fraud, abuse, or violations of our policies.

4.4 Business Transfers.

If Prikme is involved in a merger, acquisition, financing, reorganization, bankruptcy, or sale of all or part of its assets, information may be transferred as part of that transaction, subject to standard confidentiality protections.

4.5 Aggregate or De-Identified Information.

Prikme may use and share aggregate or de-identified information that cannot reasonably be used to identify any individual.

4.6 No Sale or Sharing for Advertising.

Prikme does not "sell" or "share" personal information as those terms are defined under the California Consumer Privacy Act, as amended by the California Privacy Rights Act, and does not integrate Meta/Facebook Pixel, Google Ads SDK, TikTok Pixel, or any other third-party advertising or cross-context behavioral tracking technology in the Platform.

5. Data Retention

Prikme retains personal information only as long as reasonably necessary to fulfill the purposes for which it was collected, to comply with legal, tax, accounting, and regulatory obligations, and to resolve disputes and enforce our agreements. Our standard retention periods are as follows:

User account and profile data: retained for the lifetime of the account and deleted upon account deletion, subject to the legal-evidence and audit-record exceptions below.

Booking and payment records: retained for seven (7) years for tax and audit purposes.

Patient health information (intake forms, consent forms, treatment notes, before-and-after photographs): retained for seven (7) years from the date of the last related Patient interaction, consistent with applicable medical-records retention requirements.

Reviews and ratings: retained for the lifetime of the Provider account.

In-app messages: retained for the lifetime of the conversation and deleted with the account.

Legal acceptances (Patient Platform Waiver, Terms of Service, End User License Agreement, intake-form adoptions, and similar): retained as immutable legal evidence and not deleted upon account deletion.

Where information must be retained for one of these reasons after account deletion, Prikme will minimize the data retained and apply appropriate access restrictions.

6. Security

Prikme implements administrative, technical, and physical safeguards designed to protect personal information against unauthorized access, alteration, disclosure, or destruction. These include encryption of data in transit and at rest, role-based access controls, row-level security on all storage buckets containing Patient health information, audit logging, and least-privilege access policies. No method of electronic transmission or storage is one hundred percent secure, and Prikme cannot guarantee absolute security.

7. Your Privacy Rights

7.1 California Residents.

If you are a California resident, you have the following rights under the California Consumer Privacy Act, as amended by the California Privacy Rights Act:

Right to know the categories and specific pieces of personal information we have collected about you, the categories of sources, the business or commercial purposes for collecting personal information, and the categories of third parties to whom we disclose personal information.

Right to delete personal information we have collected from you, subject to legal exceptions.

Right to correct inaccurate personal information we maintain about you.

Right to limit the use and disclosure of sensitive personal information to purposes specified in California Civil Code section 1798.121.

Right to opt out of the sale or sharing of personal information. Prikme does not sell or share personal information, so no opt-out is necessary; however, if Prikme's practices change in the future, an opt-out mechanism will be provided.

Right to non-discrimination for exercising any of the foregoing rights.

To exercise these rights, contact Prikme at the email or mailing address in Section 12. Prikme will verify your identity before responding, typically by confirming information already

associated with your account. Authorized agents may submit requests on your behalf with appropriate documentation.

7.2 Health Information.

With respect to medical information governed by HIPAA or the CMIA, your rights are administered by the Provider acting as the covered entity. Please contact the Provider directly to exercise rights with respect to your medical record.

7.3 Shine the Light.

Prikme does not disclose personal information to third parties for those parties' direct marketing purposes within the meaning of California Civil Code section 1798.83.

7.4 Account Deletion.

You may delete your Prikme account at any time through the in-app account-deletion function or by contacting us. Account deletion will trigger deletion of associated personal information except as described in Section 5.

8. Children's Privacy

The Platform is not directed to and may not be used by individuals under eighteen (18) years of age. The Platform requires users to confirm their date of birth at registration, and accounts that fail the age check are blocked. Prikme does not knowingly collect personal information from individuals under thirteen (13) years of age. If Prikme learns that it has collected personal information from a person under thirteen (13), Prikme will promptly delete that information.

9. Communications and Notification Preferences

At launch, Prikme sends only transactional communications, including booking confirmations, appointment reminders, intake-form links, password resets, support replies, and administrative notifications. You may manage transactional notification preferences within your account settings to the extent permitted by law and the operational needs of the Platform. SMS recipients may reply STOP to opt out of further SMS messages from Prikme. If marketing communications are introduced in the future, separate consent will be obtained as required by law.

10. International Users

The Platform is designed for users located in the United States and, at launch, is offered only in California. If you access the Platform from outside the United States, you understand that your information will be processed in the United States, which may have different data-protection laws than your country of residence.

11. Changes to This Privacy Policy

Prikme may update this Privacy Policy from time to time. Material changes will be communicated through the Platform or by other reasonable means in advance of the effective date of the change. The “Effective Date” at the top of this Privacy Policy reflects the date of the most recent revision. Your continued use of the Platform after the effective date constitutes acceptance of the updated Privacy Policy.

12. Contact Us

Questions or requests regarding this Privacy Policy may be directed to:

Prikme, Inc.

3555 Valley Meadow Road

Sherman Oaks, California 91403

Email: legal@prikme.com