

PRIVACY POLICY

Knotli · Switchback Ventures LLC

Last Updated: September 6, 2026 | Effective Date: September 6, 2026

1. Introduction and Scope

This Privacy Policy (“Policy”) describes how Switchback Ventures LLC (“Company,” “we,” “us,” or “our”) collects, uses, discloses, retains, and protects personal information in connection with the Knotli mobile application, related websites, and services that link to this Policy (collectively, the “Service”). Knotli is a relationship-focused connection application that pairs you with a partner, allows you to answer questions and exchange responses through a mutual-reveal mechanic, and lets you send messages and share photos and other content with your partner.

This Policy applies to personal information we process about users of the Service worldwide. It does not apply to third-party products, services, or websites that we do not control, even if they are linked from or integrated with the Service. By creating an account or using the Service, you acknowledge that you have read and understood this Policy. If you do not agree with it, do not use the Service.

This Policy is incorporated into and forms part of our Terms of Service. Certain capitalized terms used here have the meanings given in the Terms of Service.

2. Who We Are and How to Contact Us

Business. For purposes of the California Consumer Privacy Act as amended by the California Privacy Rights Act (“CCPA/CPRA”) and other applicable U.S. state privacy laws, the business responsible for your personal information is:

Switchback Ventures LLC

Privacy contact and general support: support@knotliapp.com

The Service is intended for users in the United States. It is not directed to, or offered to, individuals in the European Economic Area (EEA) or the United Kingdom (UK), and we have not appointed a representative under Article 27 of the EU or UK GDPR because we do not offer the Service in those regions. If we later begin offering the Service to users in the EEA or UK, we will appoint any representative required by applicable law and update this Policy accordingly.

3. Notice at Collection (California)

This section, together with Section 4 and the Appendix, serves as the “Notice at Collection” required by the CCPA/CPRA. At or before the point we collect personal information, we inform California residents of the categories of personal information and sensitive personal information

we collect, the purposes for which they are used, whether that information is sold or shared, and how long we retain it.

- **Categories collected:** See Section 4 and the Appendix for the categories of personal information and sensitive personal information we collect.
- **Purposes of use:** See Section 6.
- **Sold or shared:** We do not sell personal information for monetary consideration, and we do not “share” personal information for cross-context behavioral advertising as those terms are defined under the CCPA/CPRA. See Section 8.
- **Retention:** See Section 10 for our retention periods and criteria.
- **Your rights and how to exercise them:** See Section 12.

4. Categories of Personal Information We Collect

We collect the categories of personal information described below. The specific information we collect depends on how you use the Service. The Appendix maps these categories to the statutory categories enumerated under California law.

4.1 Information You Provide Directly

- **Account and registration data:** name or display name, email address, phone number, date of birth, username, and password. We collect your date of birth to confirm you meet the minimum age for the Service and to determine eligibility for age-restricted features, as described in Section 5 and Section 15.
- **Profile data:** profile photo, biography, preferences, and any other details you choose to add to your profile.
- **User content:** question responses, messages, comments, photographs, videos, audio, and other content you create, upload, transmit, or share through the Service.
- **Connection data:** partner or relationship links, invitations, mutual-consent settings, and your interactions and connections with your partner.
- **Transaction and billing data:** subscription tier, purchase history, and billing details. Payment card numbers are collected and processed directly by our third-party payment processors and the platform app stores; we do not store full payment card numbers.
- **Communications and support:** information you provide when you contact us, request support, respond to surveys, or provide feedback.

4.2 Information Collected Automatically

- **Device and technical data:** device model, operating system and version, unique device identifiers, language settings, mobile carrier, and app version.
- **Usage data:** features and screens accessed, actions taken, dates and times of use, session duration, and diagnostic, performance, and crash logs.

- **Approximate and precise location data:** approximate location derived from IP address, and precise geolocation only if you grant the relevant device permission.

Precise location is off by default.

- **Log and connection data:** IP address, access timestamps, and referring/exit pages on any web properties.
- **Cookies and similar technologies:** on our web properties and within the app, we and our providers use cookies, SDKs, pixels, and device identifiers as described in Section 9.

4.3 Information from Third Parties

- **Authentication providers:** if you choose to register or sign in through a third-party login, we receive basic profile and authentication information permitted by that provider and your settings.
- **Payment processors and fraud-prevention services:** transaction confirmations and risk signals.
- **Analytics and infrastructure providers:** aggregated and event-level information about how the Service is used.
- **Your partner:** content and information your partner provides that references or relates to you, and, where you have enabled shared or connection features, certain data or settings your partner is permitted to view or adjust as described in Section 4.4.

4.4 Shared and Partner-Adjustable Data

Knotli pairs you with a partner. Some data and settings are shared between paired users or may be viewed or adjusted by your partner through connection features. Where a feature permits your partner to view or change data or settings associated with your account, we display the current state to you, and you can see and reverse changes and unlink from your partner at any time. Age-restricted content requires the affirmative opt-in of both partners, and either partner can disable it unilaterally at any time. We recommend you only pair with a partner you trust and only share information you are comfortable sharing.

5. Sensitive Personal Information

Because Knotli is a relationship-focused application, some information you choose to provide may constitute “sensitive personal information” under the CCPA/CPRA or “special category data” under the GDPR. Depending on how you use the Service, this may include, but is not limited to:

- Account log-in credentials (username in combination with a password or security information).
- Precise geolocation (only if you enable it).
- The contents of your private messages and responses, where we are not the intended recipient.

- Information you choose to share that may reveal sexual orientation or details about your sex life, racial or ethnic origin, religious or philosophical beliefs, or health.

We process this information only as necessary to operate, secure, and provide the features of the Service that you request, to comply with law, and to protect users' safety. We do not use or disclose sensitive personal information to infer characteristics about you, and we do not sell or share it. Where the GDPR applies, we rely on your explicit consent or another lawful condition for processing special category data. You can choose not to provide sensitive information; however, some features may not function without it. California residents may have the right to limit our use of sensitive personal information, as described in Section 12.

Please do not submit information you do not wish to share, including content depicting other individuals, without their knowledge and any consent required by law.

6. How We Use Personal Information (Purposes and Legal Bases)

We use personal information for the business and commercial purposes listed below. For users in the EEA, UK, and Switzerland, the relevant GDPR legal basis is noted in brackets.

- **Provide the Service:** create and manage your account, authenticate you, enable pairing, question responses, connections, messaging, and content sharing, and operate core features. [Performance of a contract.]
- **Confirm eligibility and operate age-restricted features:** verify that you meet the minimum age for the Service and determine whether you and your partner are eligible for, and have both consented to, age-restricted content. [Performance of a contract; legal obligation; legitimate interests.]
- **Process transactions:** process subscriptions, purchases, renewals, and related billing. [Performance of a contract.]
- **Communicate with you:** send transactional, security, and account messages, respond to inquiries, and provide support. [Performance of a contract; legitimate interests.]
- **Maintain safety, security, and integrity:** authenticate users, secure the Service, detect, investigate, and prevent fraud, abuse, prohibited content, and violations of our Terms, and protect users and the public. [Legitimate interests; legal obligation.]
- **Improve and develop:** understand how the Service is used, debug and improve features, and develop new functionality. [Legitimate interests; consent where required.]
- **Personalize your experience:** remember preferences and present relevant content within the Service. [Legitimate interests; consent where required.]
- **Marketing:** send promotional communications about the Service where permitted, from which you may opt out. [Consent where required; legitimate interests.]
- **Legal compliance and enforcement:** comply with applicable laws, respond to lawful requests and legal process, and establish, exercise, or defend legal claims, including mandatory reporting of child sexual abuse material. [Legal obligation; legitimate interests.]

Where we rely on consent, you may withdraw it at any time without affecting the lawfulness of processing before withdrawal. Where we rely on legitimate interests, you may object as described in Section 12.

7. How We Disclose Personal Information

We disclose personal information only as described below. We do not sell your personal information for money.

- **Service providers and processors:** vendors that perform services on our behalf under written contracts that restrict their use of the information, including cloud hosting and database infrastructure, payment processing, email and notification delivery, analytics, customer support tooling, and content-moderation and safety services.
- **Your partner and recipients you choose:** content and information you choose to share, send, or make visible is disclosed to your partner or the recipients you direct it to. Information shared with another user is outside our control once received by that user.
- **Legal, safety, and law enforcement:** to comply with applicable law, regulation, legal process, or enforceable governmental request; to enforce our Terms; to detect, prevent, or address fraud, security, abuse, or technical issues; and to protect the rights, property, or safety of the Company, our users, or others.
- **Mandatory CSAM reporting:** we report suspected child sexual abuse material and related account information to the National Center for Missing & Exploited Children (NCMEC) and to law enforcement as required by law, and we may preserve related information.
- **Corporate transactions:** in connection with a merger, acquisition, financing, reorganization, bankruptcy, or sale of assets, subject to appropriate confidentiality protections; we will notify you of any such transfer as required by law.
- **With your direction or consent:** for any other purpose disclosed to you at the time we collect the information or with your consent.

7.1 Service Providers and Vendors

We rely on third-party service providers, vendors, and sub-processors to operate, provide, secure, and improve the Service. We may engage, add, replace, or remove these providers at our discretion. We disclose to each provider only the personal information reasonably necessary for it to perform its function on our behalf, and we require them by contract to safeguard personal information, to use it only to provide services to us, and not to sell it or use it for their own purposes. These providers include, but are not limited to, the following categories:

- **Payment processing and billing:** to process subscriptions, purchases, and renewals, manage in-app purchases, and detect and prevent payment fraud.
- **Email, SMS, and push notifications:** to deliver transactional, account, security, and, where permitted, marketing messages.

- **Cloud hosting, storage, and database infrastructure:** to host the Service and store your account data and User Content.
- **Authentication and account security:** to verify identity, secure sign-in, and prevent unauthorized access.
- **Analytics and performance monitoring:** to understand how the Service is used and to detect, diagnose, and resolve errors and crashes.
- **Customer support:** to receive, manage, and respond to your requests and communications.
- **Safety, fraud prevention, and content moderation:** to detect, investigate, and address fraud, abuse, prohibited content, and security threats, including the detection and mandatory reporting of child sexual abuse material.
- **Artificial-intelligence model providers:** to generate the optional relationship insights and trend summaries described in Section 16 from check-in content you and your partner submit. Content is transmitted to the provider solely for that purpose.

Some of these providers may process or store information in countries other than your own, as described in Section 14 (International Data Transfers). For purposes of the CCPA/CPRA, these providers act as our “service providers” or “contractors,” and their processing of personal information on our behalf does not constitute a “sale” or “sharing” of personal information.

7.2 Service Providers and Sub-Processors

We use third-party service providers and sub-processors to operate and support the Service, in the categories described in Section 7.1, including providers of cloud database, storage, and authentication infrastructure; email and message delivery; and in-app purchase and subscription management. We may share personal information with these providers as reasonably necessary for them to perform their functions on our behalf, under contracts that require them to protect the information and use it only to provide services to us. We may add, replace, or remove providers from time to time. Payment card processing for in-app purchases is performed by the applicable app store; we do not receive or store full payment card numbers. 8. “Sale,” “Sharing,” and Targeted Advertising We do not sell personal information for monetary consideration. We do not “share” personal information for cross-context behavioral advertising, and we do not process personal information for “targeted advertising” as those terms are defined under the CCPA/CPRA and other U.S. state privacy laws.

Some U.S. state laws define “sale” or “sharing” broadly to include certain disclosures to analytics or advertising partners even without monetary exchange. To the extent any of our analytics activities were ever deemed a “sale” or “sharing,” you may opt out using the methods in Section 12.3. We have not knowingly sold or shared the personal information of consumers under 16 years of age.

9. Cookies and Tracking Technologies

Our web properties and, in some cases, the app use cookies and similar technologies (such as SDKs, pixels, local storage, and device identifiers) to operate the Service, remember your settings, maintain security, and measure and improve performance. Strictly necessary technologies are required for the Service to function. Where required by law, we obtain consent for non-essential technologies and provide controls through a cookie banner or settings.

You can manage cookies through your browser settings and manage advertising identifiers and certain tracking through your device settings. Many browsers and devices also support opt-out preference signals such as Global Privacy Control (GPC), which we honor for U.S. state opt-out rights where required, as described in Section 12.3.

10. Data Retention

We retain personal information for as long as your account is active and for as long as necessary to provide the Service, and thereafter for the period needed to satisfy the purposes described in this Policy. The criteria we use to determine retention periods include:

- the duration of your account and your ongoing use of the Service;
- the time required to provide the Service and resolve any pending matters such as disputes, refunds, or support requests;
- our legal, accounting, tax, and regulatory obligations; and
- the need to establish, exercise, or defend legal claims and to maintain safety and security records.

As a general matter, we delete or de-identify account data within 90 days of account deletion, and information in routine backups is purged within 90 days. Records relating to safety, abuse, fraud prevention, or the reporting and investigation of child sexual abuse material may be retained for up to 180 days, or for longer where a longer period is required or permitted by applicable law, a preservation request, or legal process. When personal information is no longer required, we delete it or de-identify it. Content you have shared with your partner may remain accessible to that partner after deletion from your account.

11. Data Security

We maintain reasonable and appropriate technical and organizational measures designed to protect personal information against unauthorized access, disclosure, alteration, and destruction. These measures may include, but are not limited to, encryption in transit, access controls, row-level security in our database, authentication safeguards, and monitoring. No method of transmission or storage is completely secure, and we cannot guarantee absolute security. You are responsible for keeping your account credentials confidential and for the security of the devices you use to access the Service. Notify us immediately at support@knotliapp.com if you believe your account has been compromised.

12. Your Privacy Rights

12.1 Rights Available to All Users

Regardless of where you live, you may, through your in-app settings or by contacting us, request to access, update, or correct your account information, request deletion of your account and associated personal information, and manage your communication preferences. You may withdraw consent where processing is based on consent.

12.2 California Residents (CCPA/CPRA)

If you are a California resident, you have the rights described below with respect to your personal information, subject to certain exceptions.

- **Right to know / access:** to request the categories and specific pieces of personal information we have collected about you; the categories of sources; the business or commercial purposes for collecting, selling, or sharing; the categories of third parties to whom we disclose; and the categories of personal information disclosed for a business purpose.
- **Right to delete:** to request deletion of personal information we collected from you, subject to legal exceptions.
- **Right to correct:** to request correction of inaccurate personal information we maintain about you.
- **Right to opt out of sale or sharing:** to direct us not to sell or share your personal information. As stated in Section 8, we do not sell or share personal information.
- **Right to limit use of sensitive personal information:** to direct us to limit our use and disclosure of sensitive personal information to what is necessary to perform the Service and as otherwise permitted by law. As stated in Section 5, we already limit our use of sensitive personal information to these purposes.
- **Right to data portability:** to receive a copy of certain personal information in a portable, readily usable format.
- **Right to non-discrimination:** we will not discriminate or retaliate against you for exercising any of these rights.

How California residents can submit requests. You may submit a request to know, delete, correct, or limit by emailing support@knotliapp.com. We will acknowledge your request within 10 business days and respond within 45 calendar days, with one additional 45-day extension where reasonably necessary and permitted, in which case we will notify you.

Verification and authorized agents. To protect your information, we must verify your identity before fulfilling certain requests, typically by confirming control of the email address or account associated with the information, and we may request additional information where necessary. You may use an authorized agent to submit a request on your behalf; we may require the agent to provide proof of authorization and may require you to verify your own identity directly with us.

Opt-out preference signals and the “Shine the Light” law. Where required, we honor recognized opt-out preference signals such as Global Privacy Control (GPC) as a valid request to opt out of sale or sharing for the associated browser or device. Separately, under California’s “Shine the Light” law (Civil Code Section 1798.83), California residents may request information about our disclosure of personal information to third parties for those third parties’ own direct marketing purposes. We do not disclose personal information to third parties for their own direct marketing. You may direct questions to support@knotliapp.com.

12.3 Residents of Other U.S. States

Residents of states with comprehensive consumer privacy laws, including, as and when applicable, Virginia, Colorado, Connecticut, Utah, Texas, Oregon, Montana, Delaware, Iowa, Nebraska, New Hampshire, New Jersey, Tennessee, Minnesota, Maryland, and others as such laws take effect, may have rights to confirm whether we process their personal data; to access, correct, and delete personal data; to obtain a portable copy; and to opt out of targeted advertising, the sale of personal data, and certain profiling that produces legal or similarly significant effects. To exercise these rights, contact us as described in Section 13. Where a law provides an appeals process, you may appeal a decision regarding your request by contacting support@knotliapp.com; if your appeal is denied, you may contact your state attorney general.

12.4 Nevada Residents

Nevada law permits Nevada residents to opt out of the sale of certain covered information. We do not sell covered information as defined under Nevada law. Nevada residents may submit related requests to support@knotliapp.com.

12.5 EEA, UK, and Switzerland Residents (GDPR)

If you are located in the EEA, UK, or Switzerland, you have the following rights with respect to your personal data, subject to conditions and exceptions under applicable law:

- access to your personal data and information about how we process it;
- rectification of inaccurate or incomplete data;
- erasure of your data (the “right to be forgotten”);
- restriction of processing in certain circumstances;
- objection to processing based on legitimate interests and to direct marketing;
- data portability for data you provided to us where processing is based on consent or contract and carried out by automated means;
- withdrawal of consent at any time where processing is based on consent; and
- the right to lodge a complaint with your local data protection supervisory authority. You may exercise these rights by contacting us at support@knotliapp.com. We will respond within the timeframes required by the GDPR. You also have the right to lodge a complaint with a supervisory authority in your country of residence, place of work, or place of the alleged infringement.

13. How to Exercise Your Rights

To exercise any right described in this Policy, email support@knotliapp.com with the subject line “Privacy Request” and a description of your request. We will take steps to verify your identity before fulfilling certain requests and will respond within the period required by applicable law. We do not charge a fee to process most requests unless your request is manifestly unfounded, excessive, or repetitive, as permitted by law, in which case we will inform you before proceeding.

14. International Data Transfers

We are based in, and process and store information in, the United States, and we may transfer personal information to, and process it in, other countries that may have data-protection laws different from those in your jurisdiction. Where we transfer personal data from the EEA, UK, or Switzerland to a country that has not received an adequacy decision, we use appropriate safeguards, such as the European Commission’s Standard Contractual Clauses and the UK International Data Transfer Addendum, together with supplementary measures where necessary. You may request a copy of the relevant safeguards by contacting support@knotliapp.com.

15. Children’s Privacy and Users Under 18

The Service is intended solely for users who are 16 years of age or older. We do not direct the Service to, and do not knowingly collect personal information from, anyone under 16. If we learn that we have collected personal information from a person under 16, we will delete the information and terminate the account. If you believe that a person under 16 has provided us with personal information, contact us immediately at support@knotliapp.com.

Age-restricted content. Certain mature, age-restricted content is available only where each partner has entered a date of birth indicating they are 18 years of age or older and each partner has affirmatively opted in. This content is not available to users under 18, and either partner may disable it at any time. You represent that the date of birth you provide is accurate.

Heightened protections for users under 18. For users we identify as under 18, we apply heightened privacy protections, which include privacy-protective default settings (precise location and age-restricted content are off unless affirmatively enabled) and limiting profiling, consistent with applicable age-appropriate design requirements such as the UK Age Appropriate Design Code.

We strictly prohibit, and report to NCMEC and law enforcement, any child sexual abuse material as described in Section 7 and in our Terms of Service.

16. Automated Decision-Making, Profiling, and AI-Generated Insights

We use automated systems to help detect fraud, abuse, prohibited content (including suspected CSAM), spam, and security threats, which may result in content removal or account restrictions. We do not make decisions that produce legal or similarly significant effects concerning you based

solely on automated processing without a lawful basis and, where required, human review. You may contact us to request human review of, or to contest, certain automated decisions.

AI-generated insights. If you and your partner use the weekly check-in and insights features, the text of your check-in responses (and, for the trend summary, a limited history of prior check-ins) is sent to a third-party artificial-intelligence model provider, currently Google, solely to generate a summary of trends for the two of you. Generated summaries are shown only to you and your partner, are not used to make decisions about you, and are deleted with your account. You can avoid this processing by not using the insights feature.

17. Third-Party Services and Links

The Service integrates with and may link to third-party services, including authentication providers, payment processors, email and notification providers, analytics providers, cloud infrastructure, and the Apple App Store and Google Play. We do not control these third parties, and their handling of your information is governed by their own privacy policies. We encourage you to review the privacy practices of any third party before providing your information.

We use The Movie Database (TMDB) API to retrieve movie and related media information displayed in the Service. When media information or images are loaded from TMDB, TMDB and its content delivery network may receive technical information such as your IP address and device information. Our use of TMDB is subject to TMDB's terms of use and privacy policy. This product uses the TMDB API but is not endorsed or certified by TMDB.

18. Data Breach Notification

If a breach of security leads to the unauthorized acquisition, access, use, or disclosure of personal information, we will notify affected individuals and the relevant authorities where and to the extent required by applicable law, including, where the GDPR applies, notification to the competent supervisory authority within 72 hours where feasible, and notification to affected individuals without undue delay where the breach is likely to result in a high risk to their rights and freedoms.

19. Accessibility

We are committed to making this Policy accessible. If you have a disability and need to access this Policy in an alternative format, contact us at support@knotliapp.com and we will work with you to provide the information in a suitable format.

20. Changes to This Policy

We may update this Policy from time to time. The "Last Updated" date at the top reflects the most recent version, and the current version will always be available within the Service and at <https://knotliapp.com/privacy>. Your continued use of the Service after changes take effect

constitutes acceptance of the updated Policy, except where applicable law requires that we provide advance notice or obtain your consent before specific changes apply to you, in which case we will comply with those requirements. We encourage you to review this Policy periodically.

21. Contact Us

If you have questions, requests, or complaints regarding this Policy or your personal information, contact us at:

Switchback Ventures LLC

Attn: Privacy

Email: support@knotliapp.com

Appendix A — California Categories of Personal Information

Statutory Category	Collected?	Representative Examples	Disclosed for a Business Purpose To	Sold or Shared?
A. Identifiers	Yes	Name, email, phone number, username, account ID, IP address, device identifiers	Service providers (hosting, email, analytics, support, payments)	No
B. Customer records (Cal. Civ. Code 1798.80(e))	Yes	Name, phone number, and payment/financial information processed by our payment processors	Service providers, payment processors	No
C. Protected classification characteristics	Yes (limited)	Age / date of birth; and information you choose to provide that may reveal sex, sexual orientation, or similar	Service providers	No
D. Commercial information	Yes (if you purchase)	Subscription tier and purchase or transaction history	Payment processors, service providers	No
E. Biometric information	No	Not collected. Photos are not used for unique biometric identification.	—	No
F. Internet/network activity	Yes	App interactions, feature usage, diagnostics, and crash logs	Analytics and infrastructure providers	No
G. Geolocation data	Yes (if enabled)	Approximate location from IP; precise location only with permission	Service providers	No
H. Audio, visual, and similar information	Yes	Photos, videos, and audio you include in your content	Hosting/storage providers; recipients you choose	No
I. Professional or employment information	No	Not collected	—	No
J. Non-public education information	No	Not collected	—	No

Statutory Category	Collected?	Representative Examples	Disclosed for a Business Purpose To	Sold or Shared?
K. Inferences	Yes (limited)	Preferences derived to operate and personalize the Service	Service providers	No
L. Sensitive personal information	Yes	Account credentials; precise geolocation (if enabled); contents of private messages; information revealing sexual orientation or sex life	Service providers; recipients you choose	No