

LEG-002 / CURRENT PUBLIC VERSION

Privacy Policy

How SideOf collects, uses, discloses, retains, and protects personal information.

EFFECTIVE DATE	ISSUED BY	CONTACT
26 September 2026	LIBRASIDE TECHNOLOGIES LLC d/b/a SideOf	support@sideof.app

READ THIS FIRST

SideOf uses data to provide an adult social and connection service with separate Sides, coarse-location discovery, messaging, safety controls, and optional billing. The phone apps are ad-free for everyone during the launch period. Any advertising SideOf shows, on any platform and at any time, is non-personalized and appears only on the Social and Dating Sides for free accounts; SideOf+ stays ad-free. SideOf does not sell personal information or use it for cross-context behavioral advertising. See Section 10 for full advertising details.

Contents

- | | |
|--|---|
| 1. Scope and controller | 2. Information you provide |
| 3. Information collected through use | 4. Sources of information |
| 5. Location and maps | 6. Sensitive and consumer health data |
| 7. Purposes of processing | 8. Legal grounds where required |
| 9. When information is disclosed | 10. Sale, advertising, and tracking |
| 11. Ranking and automated processing | 12. Retention |
| 13. Security and biometrics | 14. Your choices |
| 15. Access, correction, export, deletion, and appeal | 16. Your U.S. state privacy rights |
| 17. Children | 18. International processing |
| 19. Changes and contact | |

1. Scope and controller

This Policy applies to SideOf applications, websites, APIs, support, safety, and related services that link to it. LIBRASIDE TECHNOLOGIES LLC d/b/a SideOf is responsible for the processing described here. Separate provider policies apply when you use an app store, payment provider, map provider, identity service, or other third-party service.

2. Information you provide

SideOf may receive account contact and age information; profile names, photos, short profile videos (a SideOf+ feature), prompts, interests, identity and relationship preferences; separate Social, Dating, and Private settings; messages and connection activity; trusted contacts and safety choices; reports, blocks, appeals, support communications, survey responses, transaction references, and account-rights requests.

Do not provide information you do not want processed for the feature you select. Private Side information remains subject to strict access controls but is not made risk-free by being private.

3. Information collected through use

SideOf may collect session identifiers, authentication state, device and app version, language, time zone, IP-derived security signals, coarse location, permissions state, navigation and feature events, crash and performance information, message delivery metadata, moderation signals, and transaction status. Private content, Safety Share details, precise device-location information, and message content are excluded from product analytics.

4. Sources of information

Information comes from you; your device and permissions; people who interact with or report an account; payment, identity, communications, app-store, map, security, moderation, and hosting providers; and lawful public or governmental sources when needed for safety, fraud, or legal compliance.

5. Location and maps

With device permission, a precise sample may be used transiently to derive a coarse area. SideOf stores and displays coarse discovery information rather than routine precise-location history and does not make a person's exact location public. You may use a manual city, hide distance, disable map visibility by Side, or withdraw device permission.

The discovery map shows approximate areas only. A spot you choose to share in a conversation is the one exact point SideOf carries. It is sent only to that person, shown on SideOf's own map, and never sent to a map provider.

6. Sensitive and consumer health data

Some profile and compatibility choices may reveal or permit inferences about sexual orientation, relationships, intimacy preferences, safer-sex conversations, or other sensitive matters. SideOf processes these choices only when you provide or activate them for the selected feature, with separate Side controls. The Consumer Health Data Privacy Notice gives additional disclosures and rights where applicable.

7. Purposes of processing

SideOf processes information to create and secure accounts; verify eligibility; operate profiles and separate Sides; provide discovery, matching, messaging, Outside events, maps, and safety tools; remember settings; provide support; fulfill transactions; detect fraud and abuse; moderate content; respond to rights requests; maintain reliability; enforce policy; comply with law; and improve features using minimized product signals.

8. Legal grounds where required

Depending on location, processing may rely on performance of a contract, consent, legitimate interests such as safety and service integrity, compliance with law, or protection of vital interests. You may withdraw consent for future optional processing through the relevant setting or permission, without affecting earlier lawful processing. SideOf does not rely on consent where another lawful basis is required or more appropriate.

9. When information is disclosed

Information is shown to other members only according to the profile, Side, connection, message, attendance, and privacy choices that apply. Service providers process information on SideOf's behalf to host the service and its database, store and deliver media, screen automated sign-ups, deliver email and text messages, monitor errors, and, where you allow it, run the automated photo check described below. Each service provider is bound by written data-processing terms that permit it to use personal information only to provide its services to SideOf, prohibit it from selling that information or using it for advertising, and require it to keep that information confidential and secure. In those respects, those terms require the same or equal protection that this Policy provides. A service provider may retain its own delivery, security, and abuse-prevention records for the period its terms permit; the list of services described below identifies where that applies. Professional advisers, such as lawyers and accountants, receive information subject to professional duties of confidentiality. Other companies handle information under their own privacy policies, as Section 1 notes: Apple and Google when you purchase through the App Store or Google Play; Expo, and then Apple or Google, when they deliver a push notification to your device; Stripe when you pay or complete an age check on the web; Eventbrite when you register for an event through Eventbrite; and Google when the website loads its fonts or, where advertising is shown, serves an ad as Section 10 describes. SideOf gives those companies only what the transaction or delivery requires, such as a purchase reference or the text of a notification, which never includes message content or location. SideOf does not give them your messages, Private Side information, or location. SideOf keeps a plain-language list of the services it uses at <https://sideof.app/service-providers> - for each one, what it handles, what it does with the information, how long it is kept, and a link to that provider's privacy policy where naming the provider is appropriate - and updates it when a provider changes. Uploaded photos may also be checked by a third-party artificial-intelligence service, currently OpenAI, which flags possible prohibited content for SideOf's moderators; a person at SideOf makes every approval or rejection. Videos and identity-check selfies are not sent. SideOf sends your photos to that service only if you allow it when you first upload. If you choose Not now, only SideOf's moderators review them, and you can change your choice at any time in Settings. Under OpenAI's API terms, OpenAI does not use the photos to train its models and may keep them for up to 30 days to detect abuse of its service before deleting them.

SideOf discloses information to a government agency or law enforcement when legal process such as a subpoena, court order, or search warrant compels it; when it believes in good faith that an emergency involving danger of death or serious physical injury requires disclosure without delay; when the law requires a report, such as a report of apparent child sexual abuse material to the National Center for Missing & Exploited Children; and when it refers serious misconduct on the service to the authorities, as the Terms of Service allow and the law permits. SideOf reviews each request for legal validity and discloses only what the request requires. It discloses the content of messages only in response to a search warrant, in an emergency as described above, with the consent of a person who sent or received them (for example, when a member reports a conversation), or as federal law otherwise permits. When SideOf receives a request to preserve records, it preserves them for 90 days, and for 90 more if the agency renews the request; once legal process is served, it holds them for as long as the matter requires. SideOf may also disclose information to protect people or the service, to investigate abuse, to enforce its agreements, or in a merger, financing, reorganization, or asset transaction subject to applicable safeguards. SideOf does not disclose one Side's private fields to another Side merely because the same account owns both. The one link SideOf makes between Sides is this: when two members matched on Social or Dating are both active on the Private Side,

each can see that the other is on Private, so either can invite the other to share Private profiles; neither sees the other's Private profile unless an invitation is accepted.

10. Sale, advertising, and tracking

SideOf does not sell personal information or consumer health data. The phone apps are ad-free during the launch period: the Google Mobile Ads SDK is not built into the iOS or Android binary, no advertising identifier is collected, and no advertising provider receives any request from those apps. When non-personalized advertising is shown, free-tier accounts may see it through Google's advertising services (AdMob in the phone apps, AdSense on the web) on the Social and Dating Sides only; these ads will not be based on your SideOf profile, activity, messages, or location, and SideOf will not send that information to the advertising provider. SideOf does not authorize AdMob, AdSense, or any other third-party SDK to use an advertising identifier to combine SideOf activity with activity across unrelated businesses. Advertising never appears on the Private Side, in messages, or alongside sensitive or consumer health data. SideOf+ membership stays ad-free. When advertising is on, the advertising provider's servers receive standard technical connection information (such as IP address, device type, and a non-personalized advertising identifier) needed to deliver an ad; this Policy's other commitments about your profile, activity, and sensitive information are unaffected. The advertising is non-personalized for everyone, everywhere, so SideOf does not build an advertising profile of you and does not ask you to consent to one. If SideOf ever offers personalized advertising, it will ask first and refusing will be one choice on that request rather than something you have to go looking for. Every core account right, safety control, export, and deletion request stays free either way.

11. Ranking and automated processing

Discovery uses rules and scoring involving eligibility, member choices, coarse distance, activity, compatibility, and safety signals. Automated processing helps order or filter results and detect risk, but SideOf does not use it to make decisions that produce legal or similarly significant effects without appropriate review and rights required by law. An automated check of an uploaded photo only flags it for a moderator; it never approves or rejects anything on its own.

12. Retention

Retention depends on the data and purpose. Profile information is kept while your account is open. Messages are kept while the connection they belong to is active, meaning you and the other member are still matched on that Side. Private messages also follow the chat-history rule below. Precise location samples are discarded after coarse conversion. Operational server logs are kept up to 30 days. Audit and moderation logs recording administrative actions are kept up to two years. Notification and message-delivery records are kept up to 90 days. Security signals and rate-limit events are kept up to 90 days, and sign-in records up to 90 days after the session ends; a signal awaiting a staff decision is kept until it is decided, then up to 90 days. Audit, notification, security and sign-in records about a member can be kept longer while a legal hold covers that member. When an account is deleted, after deletion SideOf keeps a closed list and nothing else: payment, billing and tax records, which carry a one-way hash of the account rather than your name; records under a legal hold or a lawful preservation request, including a child-safety case and anything preserved with it; a request you made to remove an intimate image, kept as the record of how SideOf met its legal duty to remove it, with your name, email address, and signature encrypted, a one-way hash of your contact details, and no longer linked to your account; a one-way hash that records that the deletion happened; reports you filed about other people, with your name removed; reports filed about you, with your account identified only by a one-way hash; and the conversation preserved with a report, for the period stated for report copies in the Privacy Policy; an internal administrative log of actions taken on the account, which records what was done and when rather than what you wrote; and product-usage counts that identify the account only by a one-way hash. A deletion request can be delayed by up to 30 days while a safety review is completed, or for as long as a legal hold applies. Everything else, including photos, identity-check captures, messages, Private message requests, trusted contacts and Safety Share records, is deleted.

Private messages follow the chat-history setting each member chooses on the Private Side. Each message is governed by the setting of the person who received it, so nobody can shorten their own setting to reach into what was said to someone else. Because a message is one record shared by both people, a message you sent is deleted on your recipient's clock, which means it leaves your view of the conversation at the same time it leaves theirs. The countdown for a message begins when its recipient opens it. A message that is never opened is kept at least thirty days from the day it was sent, whatever setting applies, because SideOf holds a conversation open for a reply and does not send a notification when a Private message arrives. Choosing to keep your chat history means messages you received are not deleted on a timer at all.

When a connection ends. A connection ends when either of you unmatches, blocks or reports the other, or when SideOf removes or restricts an account. From then on, neither of you can open the conversation in the app, though Download my data still includes the messages you sent in it (Section 15). SideOf keeps it sealed so either of you can still report a concern, then deletes it for both of you 90 days after the connection ended. On the Private Side, a chat-history setting can delete messages sooner, and a 'Keep' setting stops applying when the connection ends. If either of you deletes your account, the conversation is deleted when that deletion completes. Deletion is postponed only while, and only for as long as, one of these applies: an open report about the two of you; a legal hold; a preservation request from law enforcement; or a report to the National Center for Missing & Exploited Children, which federal law requires SideOf to preserve for one year. SideOf keeps a record that two members were connected, on which Side and when it ended, without any messages, for 12 months, so it can act on a late report and send safety notices the law requires. The other person's name

is removed from that record after 90 days. A block or unmatch keeps two members apart for as long as both accounts exist. Deletion removes messages from live systems; encrypted backups roll off as described below.

When a member reports someone, SideOf saves a copy of up to the 500 most recent messages of that conversation, on the Side the report is about, from before the connection ended. Messages already deleted cannot be saved. SideOf keeps the copy for 12 months, or until 60 days after the case closes if that is later; if the report is dismissed, the copy is deleted 90 days after dismissal. It is kept longer only under a legal hold or a legal duty to preserve. Reporting on one Side does not copy the same pair's conversation on another Side. SideOf does not tell the reported person who reported them, unless the law requires it.

Live records and uploaded media are usually deleted within a few days. Encrypted backups roll off on their own schedule: the frequent copies within about 35 days, and a smaller daily copy within six months. A restored backup is never used to restore a deleted account.

13. Security and biometrics

SideOf does not collect, capture, store, use, or disclose a biometric identifier or biometric information, and it does not run face recognition, face matching, face geometry, voiceprint, fingerprint, iris or retina scanning, or any comparable measurement of your body. Photo approval, selfie verification, and the ID check for posting explicit photos are done by a person looking at the images. The age check for viewing explicit photos reads the barcode on your ID automatically; no person looks at it, and nothing about your face is measured. Where a check asks whether a face matches a selfie, that is a trained reviewer's own judgment recorded as a yes or no; SideOf does not generate, derive, store, sell, lease, trade, or otherwise profit from a template, faceprint, or other representation of a face used to identify or compare people, and it does not ask any provider to. The automated photo check described in the Privacy Policy looks for prohibited content; it does not identify anyone, compare faces, or return anything about a face. Images submitted for an identity or age check are deleted once the check is decided. They are kept longer only while a legal hold described in Section 12 covers the account or the image is part of an intimate-image removal case, and a selfie you also use as a photo stays while it is on your profile or in a message. SideOf does not ask you to consent to biometric processing because it does not do any.

In the SideOf iPhone app on iOS 26 or later, each time you sign in, including when you create your account, SideOf asks Apple for your age range. Apple may ask you before it shares it, and you can decline. If you decline, or Apple gives no answer, nothing is sent to SideOf and your date of birth decides, as it does for everyone. If Apple says you are 18 or older, nothing is sent either. If Apple says you are under 18, the app tells SideOf only that, and your account is held: you are signed out, your profile is hidden, and your matches end. SideOf keeps a record that Apple reported you as under 18 and that your account was held, and this iPhone will not offer a new account for 30 days. SideOf never stores the age range itself and uses Apple's answer only to keep SideOf for adults. If you are 18 or older, you can appeal by writing to support@sideof.app with "Account Appeal" in the subject. If Apple has your age wrong, correct it with Apple, because SideOf asks again each time you sign in on iPhone.

SideOf uses administrative, technical, and organizational safeguards including access controls, encryption for sensitive content, purpose-separated identifiers, session controls, audit records, rate limits, and provider restrictions. No method is completely secure. Report suspected security issues through the published security policy and do not include unnecessary personal data.

14. Your choices

You can manage Side activation, discovery availability, profile fields, map and distance visibility, permissions, trusted contacts, blocks, and communications through available controls. Device permissions can be withdrawn in operating-system settings. Withdrawing a permission may disable the related feature but does not remove unrelated core access.

Email. SideOf sends marketing email only to people who asked for it, for example by ticking the box to get launch updates when joining the waitlist. Every marketing email says it is from SideOf, includes SideOf's postal address, and has an unsubscribe link, and SideOf stops sending within 10 business days after you unsubscribe. Unsubscribing does not stop the messages SideOf needs to send to run your account, such as sign-in codes, security and safety notices, and billing receipts and renewal reminders.

15. Access, correction, export, deletion, and appeal

Depending on law, you may request access, correction, deletion, portability, restriction, objection, withdrawal of consent, or an appeal. You can download a copy of your information and delete your account in the app, in Settings, then Account. You can also email support@sideof.app with "Privacy Request" in the subject line, including if you cannot sign in or your account is suspended. SideOf verifies each request, responds within the time Section 16 states, and provides information through a protected channel.

Download my data. Download my data makes a file of your information straight away and saves it to your device; if you last signed in a while ago, you sign in again first. The file is in JSON, a common format most apps can open. It includes your account and sign-in details, with only the last four digits of your recovery phone number; your profile and each Side with its settings; your compatibility and Private answers, and when you gave or withdrew consent for Private; the policies you accepted; your location and notification settings, with your approximate city and area; your photos and videos; your matches and the conversations you can see in the app; the messages you sent in a conversation that ended in the last 90 days, while SideOf still keeps them; the Direct Introductions, Private message requests, and likes you sent; the people you blocked and the profiles you saved; the category and date of each report you filed; your purchases, memberships, and credits; your trusted contacts, with their contact details partly hidden; your check-ins; and your events. Other members appear only by the name the app shows you. Your photos and videos are included as private links that work for 24 hours; a photo or video still in review is listed without a link until it is approved. Download the file again for new links. You can download the file up to three times a day, including while your account is waiting to be deleted. Anyone you share the file with can read it and use its links.

What the file leaves out. The file does not include your email address, because SideOf keeps only a one-way code of it and cannot read it back; your full recovery phone number, which protects your sign-in; or your precise location, which SideOf does not keep, although a location you or a match shared in a chat appears as it does there. It also leaves out the other person's messages in a conversation that has ended; reports other members made about you, the evidence and staff notes on any report, and the signals SideOf uses to detect abuse and keep accounts secure, because sharing them could put other people at risk or help someone get around SideOf's safety systems; and internal codes and record numbers. Other records, such as your sign-in history and decisions SideOf made about your account or your verification, are not in the file, and you may ask for them. The file lists what it leaves out. To ask for anything SideOf holds about you that is not in the file,

email support@sideof.app with "Privacy Request" in the subject line. SideOf will send what the law requires through a protected channel and, unless the law prevents it, will tell you what it withheld and why.

A deletion request immediately removes the profile from ordinary discovery and revokes active sessions. The verified workflow then deletes your primary records and uploaded media from our systems, usually within a few days; encrypted backups roll off on their own schedule: the frequent copies within about 35 days, and a smaller daily copy within six months. Limited records may remain when legally permitted or required. Deleting the account does not cancel a SideOf+ subscription. Cancel it first: in Settings, then Manage SideOf+, then Manage membership for a web membership, or in the App Store or Google Play for a store membership.

16. Your U.S. state privacy rights

In short: you can ask SideOf what it has about you, fix it, get a copy, or delete it, wherever you live. Some states give you more, and SideOf honors those rights as the law of your state requires.

State laws. California (the California Consumer Privacy Act, as amended by the California Privacy Rights Act), Colorado, Connecticut, Delaware, Indiana, Iowa, Kentucky, Maryland, Minnesota, Montana, Nebraska, New Hampshire, New Jersey, Oregon, Rhode Island, Tennessee, Texas, Utah, and Virginia give their residents privacy rights, and other states may do so. Which rights apply, and whether a law applies to SideOf at all, depends on your state and on thresholds in each law. SideOf accepts the requests below from every member, wherever you live.

Your rights. Depending on your state, you may ask SideOf to: confirm whether it processes your personal information and give you access to it, including the specific pieces it holds; correct inaccurate information; delete information; give you a copy in a portable format; tell you the categories of information it has collected, the sources, the purposes, and the categories of recipients; and give you a list of the specific third parties it has disclosed your information to, where your state provides that right. You may also have the right to opt out of the sale of personal information, of "sharing" or targeted advertising, and of profiling that produces legal or similarly significant effects, and to limit the use of sensitive personal information. SideOf does not sell personal information, does not share it for cross-context behavioral advertising or use it for targeted advertising, and does not use profiling to make decisions with legal or similarly significant effects, as Sections 10 and 11 explain. SideOf uses sensitive personal information, such as Private Side answers and information that reveals sexual orientation, only to provide the features you ask for, to keep the service secure, and for the other purposes the law permits, and it asks for your consent where the law requires, as Section 6 and the Consumer Health Data Privacy Notice explain.

Opt-out preference signals. Because SideOf does not sell or share personal information or use it for targeted advertising, there is currently nothing for an opt-out preference signal, such as Global Privacy Control, to switch off. If that ever changes, SideOf will treat a Global Privacy Control signal from your browser or device as a valid request to opt out, as the law requires, before any sale, sharing, or targeted advertising begins.

How to make a request. Use Download my data and Delete account in the app (Section 15 explains what the file includes and leaves out), or email support@sideof.app with "Privacy Request" in the subject line, including if you cannot sign in or your account is suspended. In the app, your recent sign-in verifies the request. For an emailed request, SideOf verifies it by matching it to the account, usually by confirming control of the account's email address, and asks only for what it needs to do that. An authorized agent may make a request for you where the law allows. SideOf may ask the agent for proof of your permission and may ask you to confirm your

identity directly. SideOf responds within 45 days. Where the law allows, it may take up to 45 more days if it tells you why within the first 45. Requests are free, except that SideOf may decline, or charge a reasonable fee for, requests that are manifestly unfounded or excessive, where the law permits.

Appeals. If SideOf declines all or part of your request, it will tell you why. You may appeal by emailing support@sideof.app with "Privacy Appeal" in the subject line within 60 days of the decision. A person at SideOf will review the appeal and tell you the outcome in writing within 45 days. If the appeal is denied, SideOf will tell you how to contact your state's Attorney General.

No discrimination. SideOf will not deny you the service, charge you a different price, or give you a different level of service because you exercised a privacy right.

17. Children

SideOf is not directed to children and does not permit anyone under 18 to create or use an account. If SideOf learns that a minor provided personal information, it may restrict the account, preserve information needed for safety, and delete information as appropriate. In the iPhone app, SideOf also asks Apple at sign-in whether a member is under 18 and holds the account if Apple says so, as Section 13 explains. Report an underage concern through the in-product report flow or support@sideof.app.

18. International processing

SideOf is operated from the United States and providers may process information in other jurisdictions. Where required, SideOf uses lawful transfer mechanisms and safeguards. Local law may provide additional rights that cannot be limited by this Policy.

19. Changes and contact

SideOf may update this Policy as practices or law change. The current version shows its effective date, and material changes receive notice or renewed consent where required. Privacy questions, rights requests, and appeals may be sent through in-product controls or to support@sideof.app with 'Privacy Request' or 'Privacy Appeal' in the subject line.