Jubal Privacy Policy

Effective date: December 14, 2026

Version: 2026-12-14

This Privacy Policy explains how Jubal Inc ("Jubal," "we," "us") handles personal information in connection with the website at jubal.law (the "Site") and the Jubal desktop and web applications and related services (the "Service").

Jubal is software for law firms. This policy treats three kinds of information differently.

1. Website information. Information about people who visit the Site, fill in a form, or use the free Cite Checker. Section 2.
2. Account information. Information about the lawyers and staff who use the Service under a firm's account. Jubal decides how this is used, as described here. Section 3.
3. Customer content. The documents, text, chats, and other material a law firm puts into or creates with the Service. This will often contain personal information about the firm's clients and others. Section 4. Jubal processes customer content on the law firm's behalf and on its instructions, as its service provider. The law firm decides what goes into the Service and is responsible for its own privacy obligations to its clients. If you are a client of a law firm that uses Jubal, contact that firm about your information.

1. Our core commitments about customer content

- We do not use customer content to train AI models. We configure our model providers not to train on it. Whether written no-training terms are on file is stated, for each provider that receives customer content, in the Subprocessor List. Where that list says the written terms are not on file, or not confirmed, this policy does not say that the provider's agreement prohibits training.
- We do not sell personal information, and we do not share it for cross-context behavioral advertising. The Site runs no advertising trackers.
- We use customer content only to provide the Service to the firm that owns it, and we share it only as Section 5 describes.
- We store customer content in the United States, encrypt it at rest and in transit, and scope it to the firm and to each matter.
- Naming a model provider in this policy, including X.AI LLC (xAI), does not decide whether a firm must obtain its client's informed consent before using the Service on that client's matter. That judgment is the firm's.

2. Website information

2.1 What we collect

When	What we collect	Why
You visit any page	We count page views ourselves: the page's path, the domain of the site that referred you (if any), and the country your connection appears to come from (derived by our host from your IP address), with a timestamp. We do not store your IP address, browser details, a cookie, or any identifier with this record. Our host, Vercel, also counts visits for us with its cookie-less Web Analytics.	To see which pages people read and where visitors come from, in aggregate.
You fill in a referral or contact form	Your name, email, and optionally your firm name, phone number, and message; the referral code and landing page you came from; campaign tags in the link; and whether you asked us to follow up about a trial.	To follow up with you, and to credit the person or group that referred you.
You request a free trial	Your name, work email address, and role at the firm; your firm's name, primary state, size, and practice areas; what you want Jubal to do first, in your own words; and how you heard about us. Optionally, your phone number, your firm's website, and who referred you. We also record the page and button you used, any referral code, whether you confirmed your address by an emailed link or by signing in with Google, and the city, region, and country your connection appears to come from (derived by our host from your IP address).	So a person at Jubal can review and approve the request, confirm the firm is real, contact you, and credit a referral.
You tell us more about your firm after signing in	Every question is optional: your firm's name, website, size, practice areas, and phone number; your role at the firm; the AI tools your firm uses today; a note on what you would most want help with; your bar number and bar admission state; and your LinkedIn and X profiles.	To review your request, confirm that the firm is real and that you are a practicing attorney, and contact you. Your bar number is never published.
You use the Cite Checker	The text you paste, or the text of the file you choose. The file itself stays in your browser. The text is processed in memory on our server to find citations, and is not stored or logged. Only the citations are sent to the legal research services the tool uses. Your IP address is used briefly in memory to rate-limit the tool.	To check your citations.

2.2 Cookies and similar technologies

The Site does not use advertising or analytics cookies. If you sign in, we set strictly necessary cookies that keep you signed in and secure. See Section 3.2. We also set one preference cookie that remembers your chosen text size. If you tick "remember my email" at sign-in, your email is stored in your own browser.

3. Account information

3.1 What we collect

- Identity and sign-in. Name, email address, profile picture, and email-verification status from our sign-in provider (WorkOS, or Google if you choose “Sign in with Google”). If you register a passkey, its public key and a coarse device label (for example, “Mac · Safari”). We never receive your Google password.
- Profile details you choose to add. Title, phone, website, mailing address, avatar, and a personal working profile that Jubal’s agent uses to tailor its work for you.
- Firm and role. The firm or firms you belong to, your role, seat, and plan, who invited you, and invitation details.
- Acceptance records. When you accept our Customer Terms, Acceptable Use Policy, or this Privacy Policy, we record which document and version you accepted, a fingerprint of its text, when, on which platform, where in the Service, and the IP address and browser or device information reported at the time, so that we can show what was agreed. We keep acceptance records after an account is deleted, for the life of the firm’s account plus the applicable limitations period. They contain no customer content.
- Device and app information. For the desktop app, the app version, operating system and version, and processor architecture, and the date you were last active.
- Usage and billing. Records of your use of AI features (for example, which model and how much), used for your firm’s usage allowance, billing, and cost reports; billing contacts; and Stripe customer and subscription identifiers. Payment card details are entered on Stripe’s pages. Jubal never receives card numbers.
- Communications and feedback. Messages you send us, and ratings and comments you give in the app. If, and only if, you tick the box to include it, a copy of the conversation or a screenshot you choose to send with feedback.
- Security and error information. Sign-in and security events (for example, passkey enrolment and use), and error reports from the app. See Section 3.3.

3.2 Cookies in the web application

Strictly necessary, httpOnly, secure cookies: a sealed session cookie (up to 7 days), a device cookie for passkey sign-in (30 days), and short-lived cookies used during sign-in and when handing sign-in to the desktop app (2 to 5 minutes). They are not used for analytics or advertising.

3.3 Error reporting

The web and desktop apps send error reports to Sentry so that we can find and fix bugs. They are configured not to send user identities. The desktop app additionally strips request details and activity trails before sending. Error reports contain technical details such as the app and

operating-system version and the error itself.

3.4 How we use account information

We use account information to provide, secure, and support the Service; to authenticate you and prevent fraud and abuse; to bill your firm; to send service messages (sign-in codes, invitations, deadline digests you can turn off, usage and billing notices, and notices about changes to our terms); to respond to you; to improve the Service using aggregated usage information that does not include customer content; and to comply with law and enforce our terms. We do not send marketing newsletters to account users. We do not use account information for targeted advertising.

4. Customer content

4.1 What it is

Everything a firm and its users put into or create with the Service: uploaded documents and files (including their text, images, embedded metadata such as photo location and camera details, and audio and video), matter and client details (which can include names, contact details, dates of birth, and other information about clients, parties, and witnesses), chats and prompts, dictation audio, notes, tasks, calendar entries, memory, generated documents, and information about people outside the firm that a user enters — for example, the name and email of someone asked to upload files through a file-request link.

4.2 Our role

We process customer content on the firm's behalf to provide the Service to it, under the Jubal Customer Terms of Service. The firm is responsible for having the right to upload it and for any notices or consents its clients or others are owed. We do not use customer content for our own purposes, except as needed to secure the Service, prevent abuse, and comply with law.

4.3 Medical records and health information

A firm may upload medical records and other health information that the firm or its client lawfully holds for a representation, and that the firm has the right to process with the Service and its subprocessors. A firm may not upload protected health information in the capacity of a HIPAA covered entity or business associate unless Jubal and the firm have signed a business associate agreement covering that use. Jubal will enter into a business associate agreement with a firm that asks for one, by writing to legal@jubal.law.

A matter that is not marked as containing protected health information is treated as not containing it, except that a personal-injury matter is treated as containing it unless the firm states that it does not. The firm is responsible for marking matters that contain protected health information. Marking a matter does not make the Service suitable for protected health information.

A firm must not upload psychotherapy notes, or substance-use disorder treatment records it is not authorized to redisclose, without Jubal's prior written agreement. Jubal may decline that agreement.

4.4 Where customer content goes

- Storage. Documents are stored in Jubal's Amazon S3 storage in the United States, encrypted with keys managed in AWS KMS. The rest of the matter record (extracted text, summaries, chats, memory, and other data) is stored in our application database (Convex). A working copy of each matter a user opens is kept on that user's computer so the desktop agent can work with it.
- AI processing. When you use AI features, the content a request needs — which can include document text and page images — goes through Jubal's model gateway in our AWS account to the AI model providers in our Subprocessor List. Those providers are Amazon Bedrock and xAI. Whether a given request goes to xAI depends on a deployment-wide setting controlled by Jubal, not on a separate consent by the firm. Scanned pages are read by Amazon Textract. Audio and video are transcribed by Amazon Transcribe.
- Dictation. If you use voice dictation, your audio is streamed directly from your computer to our speech-to-text provider (Deepgram). Dictation is available to paying and trial accounts. Marking a matter as containing protected health information does not change dictation.
- Lookups. When you or Jubal's agent looks something up — a case, a statute, a business address, or a web search you ask for — a short query, not your documents, is sent to the research service. It may include a name or other detail from your request. Every such call is logged.
- Email. Some service emails contain customer content — for example, matter names and deadlines in deadline digests, client names in statements, and file-request emails to the people you invite.
- Jubal staff. See Section 5.3.

5. How we share information

5.1 Service providers (subprocessors). We share information with the providers that host and operate the Service for us, under contracts that restrict their use of it. The current list, with what each receives and whether written no-training terms are on file, is our Subprocessor List at jubal.law/legal/subprocessors. Before a new subprocessor begins processing a firm's customer content, we will email the firm's owner and billing owner and update that page. We will not start that processing until 30 days after the email, unless a shorter period is required by law or to address a security incident. A firm that objects may cancel and receive a refund of prepaid fees for the unused part of the billing period, as the Customer Terms describe.

5.2 Within your firm. Customer content is visible to the people your firm authorizes, according to the permissions your firm sets, and to guests your users invite to a matter.

5.3 Jubal personnel. Our staff do not access customer content except to provide support your firm has requested through the in-app support-access feature (which your firm's administrators are notified of and can revoke at any time), to set up a firm at its request, to review feedback you chose to send with content attached, to investigate security incidents, abuse, or technical problems, or where the law requires. An activated support grant runs until it is revoked, unless the firm sets an earlier expiry. Read-only viewing under a grant is not separately audited. We do not promise that every access is logged.

5.4 Legal requirements. We may disclose information if we believe in good faith that the law, a court order, or legal process requires it. If we receive legal process seeking a firm's customer content, we will, where the law allows, notify the firm promptly so that it can assert privilege or object, and we will direct the requester to the firm where practicable.

5.5 Business transfers. If Jubal is involved in a merger, acquisition, financing, or sale of assets, information may be transferred as part of that transaction, subject to this policy.

5.6 With your direction. We share information when you ask us to.

We do not sell personal information, and we do not share it for targeted advertising.

6. Retention

The periods below match the Customer Terms.

Information	How long we keep it
Customer content	For as long as the firm keeps it in the Service. A deleted matter can be restored for 30 days and is then permanently deleted. A firm owner can delete a matter permanently at once. The Service does not delete trial content, or content after the Customer Terms end, on a timer. We will not delete it until we have emailed the firm's owner, stated a deletion date at least 30 days after that email (and, after the Customer Terms end, at least 30 days after the export period ends), and the date has passed. We will not send that email for a trial account before 90 days after the trial ends. After the Customer Terms end, the firm keeps read-only access for at least 30 days to export.
Backups	Encrypted database backups are kept for up to 35 days (daily) and 12 months (monthly). Deleted database records can persist in backups until those copies expire. Backups are used only for disaster recovery. If a backup is restored, deletions are re-applied. Document files are deleted from storage when a matter is permanently deleted and are not kept in these backups.
Confirmation of deletion	We do not remove a single firm's content from a backup before that backup expires. On a firm's written request, we will confirm in writing what was deleted from our active systems, and what remains in backups and until when.

Information	How long we keep it
Working copies on users' computers	Removed by the desktop app when a matter is deleted or access ends, the next time the app signs in or runs its periodic clean-up. Signing out does not remove them. A computer on which the app is not run again will keep them.
Account information	For as long as the account exists. A firm's owner can delete the firm, and any user can delete their own account, in the Service (Settings, Security, Delete, or jubal.law/account). When an account is deleted we delete the user record, memberships, passkeys, memory, and personal chats. When a firm removes a member, that member's personal workspace data is deleted 30 days later.
Audit, security, usage, and billing records	Kept after deletion for security, audit, billing, and legal purposes, and in any event not longer than 7 years unless a longer period is required by law. Audit records can include document file names and party names.
Acceptance records	Kept after account deletion, for the life of the firm's account plus the applicable limitations period. They contain no customer content.
Website page-view counts	Until deleted. They contain no personal identifiers.
Referral and contact forms, and trial requests	Until you ask us to delete them, or 24 months after our last contact if you do not become a customer.

7. Security

We protect information with measures including encryption of stored documents with AWS KMS keys and encryption in transit; server-enforced access controls scoped to each firm and each matter; short-lived upload and download links; audit logging of privilege-relevant actions; time-limited sign-in sessions and optional passkeys; sign-in tokens on Mac sealed by the device's Secure Enclave; and a sandbox that keeps the desktop agent's command shell off the network. No system is perfectly secure.

If we become aware of unauthorized access to, or acquisition, disclosure, or loss of, customer content in our or our subprocessors' systems, we will notify the affected firm without undue delay, and in any event within 10 days after determining that a breach of security has occurred, with the information reasonably available to us, and we will take reasonable steps to contain and remediate it. The firm is responsible for any notices to its clients, affected individuals, and regulators that the law requires of it. We will assist. A notice by us is not an admission of fault. Where the law requires notice to individuals or to a regulator, we will give that notice as well.

8. Where information is processed

Jubal is based in the United States, and we store customer content in the United States. Where a service provider's processing location has been verified, the Subprocessor List states it. The Service is intended for law firms in the United States. If Jubal accepts firms outside the United States, this policy will be updated with international-transfer terms before that happens.

9. Children

The Site and the Service are for professionals and are not directed to children under 16. We do not knowingly collect personal information from children for our own purposes. Customer content that a law firm uploads may concern minors. That content is processed on the firm's behalf. Section 4.

10. Your choices and rights

10.1 Everyone. You can ask us for a copy of the personal information we hold about you as a website visitor or account user, ask us to correct it, or ask us to delete it, by writing to privacy@jubal.law. We will verify your request and respond within 30 days, or within any shorter period the law that applies to the request requires. We will not discriminate against you for making a request. The commitments in this Section 10 are voluntary except where a law requires them.

10.2 Account users. You can update your profile in the app. You can delete your account yourself under Settings, Security, Delete, or at jubal.law/account; a firm's owner must delete the firm or transfer ownership first. If you belong to a firm, some information about your work belongs to the firm's customer content and may be kept by the firm.

10.3 Customer content. If your request concerns information in a law firm's customer content — for example, you are a client or opposing party in a matter — we will refer you to the firm, which controls that information, and will assist the firm as our contract with it requires. A firm that wants its own content deleted may delete documents and matters in the Service, or ask us to delete the firm, as Section 6 describes.

10.4 Email. You can turn off deadline digests in the app. Service messages about your account, security, and billing cannot be turned off while you have an account.

10.5 State privacy laws. We do not sell personal information. We do not share it for cross-context behavioral advertising. If a state privacy law applies to a request, we will honor the rights it gives. We do not add statute-specific notices for laws whose thresholds Jubal does not meet.

11. Changes to this policy

We will post any change here with a new version and effective date. A change in how customer content is used or shared is material, and we will say so in the notice before we publish it. We treat every published change as material: we email account holders at least 30 days before it takes effect and ask for acceptance before continuing, as the Customer Terms describe. The binding act for a firm is its owner's acceptance. Every version of this policy remains available at a permanent address.

12. Contact

Jubal Inc

c/o Ken Ronan, 750 S Dixie Hwy, Boca Raton, FL 33432

Privacy questions and requests: privacy@jubal.law

Security: security@jubal.law

Everything else: hello@jubal.law