



Privacy Notice

Version 1

Effective August 21, 2026

This notice explains how Taproot IO, LLC (“Taproot”) collects, uses, discloses, and retains personal data when people use Taproot-operated services. A creator may separately control data collected through that creator's site; the creator's own privacy notice should explain that processing.

Data we process

- Account and profile data: name, email address, and optional profile details you choose to add (display name, tagline, bio, location, website, and social links). Taproot uses passwordless sign-in codes sent to your email address; we never store a password for you .
- Creator and site data: site configuration, content, collaborators and invitations, publishing history, custom domains and verification records, support requests, and moderation activity.
- Membership and commerce data: product selections, membership status, billing cadence, transaction and invoice references, billing country, and — for creators — Stripe connected-account and payout status. We store only the card brand, last four digits, and expiration of a payment method; full payment-card details are collected directly by Stripe and never stored by Taproot.
- Legal-acceptance evidence: when you accept an agreement, we record the document version, time, method, your browser's user-agent string, and a keyed hash of your IP address, so we can prove which version you accepted.
- Referral data: if you arrive through an affiliate link, we record the referral code, referring page, IP address, and user-agent string to attribute the referral and prevent fraud.
- Usage, device, and security data: server request logs, session records, and error information. Published-site analytics are aggregate and privacy-preserving: we count visits using a visitor identifier that is re-derived every day from a rotating key and cannot be linked across days; we store page path, referrer domain, country, and device category — never your IP address, precise location, or full browsing history.
- Communications and community data: emails we send you and their delivery status, comments you post, reports you file, email-suppression records (bounces and complaints), notification preferences, and information supplied to support.
- Data received from providers: payment, payout, tax, and fraud signals returned by Stripe for accounts and creators using commerce features.

Taproot does not use third-party advertising or analytics scripts anywhere on its services, and sign-in is first-party only — there is no social login.

Why we process it

We process data to provide and secure accounts and sites; publish requested content; administer plans, memberships, payments, payouts, and taxes; communicate with users; prevent fraud and abuse; moderate content; comply with law and provider requirements; enforce agreements; keep records; and improve the service.

Where a legal basis is required, we rely on: performance of a contract (operating accounts, publishing sites, administering plans and memberships); legitimate interests (securing the service, preventing fraud and abuse, aggregate analytics, moderating content, improving the service); legal obligation (tax, accounting, and lawful requests); and consent for optional communications you subscribe to, which you

can withdraw at any time.

For Canadian users, consent under PIPEDA works as follows: consent is implied for the processing that is necessary to deliver the service you asked for and that this notice describes, and we obtain express consent separately — through a distinct opt-in — for optional communications and for any sensitive processing. We do not treat merely continuing to use the service as consent to anything beyond what is necessary to provide it. You may withdraw consent at any time, subject to legal and contractual limits, through notification preferences, by deleting your account, or by contacting privacy@taproot.io.

Sharing

We disclose data to service providers and subprocessors that host, secure, deliver, measure, communicate, or process payments for the service; to creators and members as needed for their membership relationship; to professional advisers; in a corporate transaction; and to authorities or other parties when reasonably necessary to comply with law, protect rights or safety, investigate abuse, or enforce agreements. The current vendor inventory is in the Subprocessor List .

Stripe receives payment and connected-account data under its own notices and agreements. A creator receives the member information reasonably needed to deliver and support the creator's membership: the member's display name, email address, plan, price, and membership status and dates — not the member's payment-method details or billing address.

We do not sell personal data, and we do not share it for cross-context behavioral advertising. Taproot runs no third-party advertising, tracking, or analytics technology, so no “sale,” “sharing,” or targeted-advertising opt-out under US state privacy laws currently applies.

Retention and security

We retain data for as long as needed for the purposes above. Representative periods:

- sign-in verification codes expire after 10 minutes; sessions expire with their refresh token (1–30 days, configurable, default 7);
- self-service data-export archives are deleted after 7 days;
- raw analytics events are kept 0–30 days depending on plan; daily summaries 30–365 days depending on plan; only non-identifying monthly aggregates are kept longer;
- billing, tax, and transaction records are kept as required for tax, audit, and dispute periods (typically seven years);
- legal-acceptance and safety/audit records are kept while relevant to prove acceptance, investigate abuse, or satisfy legal obligations;
- backups are deleted on their normal provider cycle.

When you delete your account, an automated deletion process removes your profile, content, images, sessions, and related records — usually within about 15 minutes — and provides a public status page you can check without signing in. We retain what the law requires or a legitimate purpose demands: financial and tax records, audit and safety logs, records of payments to affiliates, and comments you left on other people's sites (disassociated from your identity and shown as a deleted member).

Taproot uses administrative, technical, and organizational safeguards, including encryption in transit, role-based access control, short-lived session tokens, and least-privilege infrastructure access, but no system can guarantee absolute security.

Choices and rights

Account settings provide self-service access to correction, a full data export, notification preferences, and account deletion. You may also contact privacy@taproot.io. Depending on where you live, you may have rights to access, correct, delete, restrict, object, port, withdraw consent, opt out, or appeal a decision; we honor these rights as applicable law requires. We may verify your identity before acting on a request and may retain data when legally permitted. We will not discriminate against you for exercising a privacy

right. If you are dissatisfied with our response, you may complain to your local supervisory or privacy authority — in Canada, the Office of the Privacy Commissioner of Canada or your provincial authority.

Children and international transfers

Taproot is not directed to children under 13, and people under 13 may not create accounts. Contact us if you believe a child supplied data contrary to this policy and we will delete it.

Taproot stores and processes data in the United States (our infrastructure providers operate US regions), and our edge network processes requests globally in transit. If you use the service from Canada or elsewhere, your data is transferred to and processed in the United States, where privacy laws may differ from those of your jurisdiction; we protect it as this notice describes wherever it is processed and use appropriate safeguards where the law requires them.

Contact and changes

Privacy questions and requests: privacy@taproot.io , or by mail at Taproot I/O, 6824 19th Street W #633, University Place, WA 98466. Taproot IO, LLC is the entity responsible for personal data processed under this notice. For the purposes of Quebec law, the person in charge of the protection of personal information is Taproot's Privacy Officer, reachable at privacy@taproot.io .

We will publish changes with an effective date and provide additional notice when required. A changed notice is not recorded as consent.