Taproot

Taproot Privacy Notice

Version 3
Effective November 13, 2026

Summary of changes: Names the company as Taproot IO, LLC in our mailing address. Nothing else changes.

This notice explains how Taproot IO, LLC (“Taproot”) collects, uses, discloses, and retains personal data when people use Taproot-operated services, including the Taproot app and the sites that creators publish with Taproot.

Two roles apply. Taproot decides how to handle account, billing, security, abuse-prevention, its own launch waitlist and abuse reports, and platform email data, and is responsible for that data under this notice. When a creator uses a Taproot site to collect information from their own readers — form answers, newsletter subscribers, comments, member lists — the creator decides what to collect and why, and Taproot stores, secures, and delivers that data on the creator's behalf. The creator's own privacy notice should explain the creator's use of it. Taproot also sets some rules that apply to every site, such as the shared email suppression list, abuse limits, and the visit measurement described under “Site analytics” below: Taproot decides what that measurement collects and shows the resulting reports to the site's owner.

Data we process

- Taproot launch waitlist: if you join the waitlist on www.taproot.io , we collect your email address and your answers about what best describes you and what you publish with today. We use your email address, with your consent, to let you know when account signup opens, and the answers to understand which audiences and publishing tools people use. We store the answers, submission time and page, and a record of your email choice (a hash of the consent label and the time) with your entry. The form also records the short-lived network address hash and submission counts described under “Forms and visitor submissions” below. Reports show audience and current-tool totals without identifying individual respondents. Joining displays an on-page confirmation; it does not create an account or newsletter subscription, send a confirmation email, give priority access or guarantee an opening date. To leave the waitlist, contact privacy@taproot.io from the address you submitted; no Taproot account is needed.
- Abuse reports: if you use the report form on www.taproot.io , we collect the address of the page you report, the kind of problem you choose, your description, your email address, and a record of your agreement that we may store the report and contact you about it (a hash of that label and the time). We use them to look into the report, act on it under our Terms and Community Guidelines, and contact you about it. The form also records the short-lived network address hash and submission counts described under “Forms and visitor submissions” below. Sending a report does not create an account or newsletter subscription.
- Account and profile data: name, email address, and optional profile details you choose to add (display name, tagline, bio, location, website, social links, and image). Taproot uses passwordless sign-in codes sent to your email address; we never store a password for you . Your profile is public. When you create an account Taproot publishes a profile for you as public files. The published profile includes the first and last name you gave at sign-up, your display name, and the other details you have added. The people you follow and the people who follow you are published as public lists too.
- Creator and site data: site configuration, content, collaborators and invitations, publishing history, custom domains and verification records, support requests, and moderation activity. When a creator searches for a place, the search text and an approximate (city-level) location are sent to Google to

rank results; the location is not stored, and the place the creator selects is stored with their content. Everything a creator publishes on a site is public unless the creator makes a page member-only (see “Member-only pages” below).

- 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. For a payment method we store the card brand, last four digits, expiration, and a one-way fingerprint of the card number that lets us notice when several accounts use the same card; 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.
- Forms and visitor submissions: when a creator publishes a form, what a visitor submits is stored for the creator: every answer, the contact email address if the form asks for one, the page it was sent from, the time, a record of which consent boxes were ticked (a hash of each consent label and the time), and a keyed hash of the visitor's network address that we delete after 30 days. A count of submissions per site (site and time only) is kept for 90 days to apply the licence's monthly limit. Taproot does not add its own privacy notice to a creator's form; the creator is responsible for telling visitors how the answers are used.
- Newsletter data: a creator can run a newsletter. For each person who signs up or whom the creator imports, Taproot stores the email address, name, subscription status, the consent wording and version agreed to, where and when it was agreed, and a history of changes to the subscription. For an import, Taproot also stores the creator's statement that the list was not purchased, rented, or scraped and that the creator can provide the original consent evidence. Every address is confirmed by email before it receives a newsletter. Each newsletter email contains a small image and rewritten links that let Taproot record whether, and when, each recipient opened the email or clicked a link; this is recorded against the recipient and shown to the creator. Open and click recording is part of how newsletters work today and cannot be switched off; you can unsubscribe at any time.
- Usage, device, and security data: server request logs, session records, and error information. Cloudflare request logs can include the request URL and path, request headers containing a visitor IP address, referrer, browser description, request identifiers, and network and approximate location information. URLs may contain query strings. These operational records help us investigate failures, abuse and delivery costs; they are separate from the creator analytics described below. We do not promise that all headers, query strings or cookies are excluded from these records. Account sign-up and published forms use Taproot's own bot challenge, which runs from Taproot's servers and sends nothing to a challenge vendor. To limit repeated sign-ups and form submissions, Taproot keeps short-lived counters keyed by a hash of the visitor's network address (for example ten minutes for forms) and refuses sign-ups from known disposable-email domains.
- Site analytics: described in the next section.
- Communications and community data: emails we send you and their delivery status, comments you post (published as public files together with your user id, so they display your public profile name), reports you file (a moderator sees the reporter's display name), a creator's per-site standing for you as a commenter (trusted, suspended, or banned, with the creator's reason), 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; for a creator who connects Google Search Console, the search performance data Google reports for that site (see “Google Search Console”); and, for a creator who connects a Google Business Profile, the details and reviews Google reports for the location they choose (see “Google Business Profile”).

Taproot's own pages and templates load no third-party advertising or analytics scripts or pixels, and sign-in is first-party only — there is no social login. A site's map page requests map tiles from OpenFreeMap

when you open that page, which gives OpenFreeMap your IP address. Creators can add embedded video (YouTube or Vimeo, loaded only after you press play) and install integrations that load their own scripts on their sites; those services have their own practices (see the Cookie Notice).

Site analytics

Taproot measures visits to published sites for each site's owner. The measurement runs at Taproot's edge network (provided by Cloudflare, see the Subprocessor List) and, where the sections below say so, with one short-lived visit cookie and one small script (and, only where a site asks first, one cookie that remembers your choice). It is part of the service and is available to the owner of a Grow or Scale site; Starter sites have no creator analytics. Operational request logs can still record requests to Starter sites and profiles, independently of creator analytics availability or analytics opt-out. Taproot's creator analytics collections are:

- Page-view events. Analytics events include page path, the previous page of the same site, referrer domain, country and region, device, browser and operating system family, and language. When a visit arrives through a link tagged with a recognised source or medium, or with a campaign key the site registered, Taproot also stores that tag; any other tag value is discarded. Analytics events do not include raw IP address, user-agent string or precise location. Taproot's summaries and reports store movement between pages only as counts of page pairs, never as a record of one person's browsing. Our edge provider keeps the individual analytics events behind those summaries, which carry the identifiers below, for up to three months; they are not shown to anyone.
- Daily identifier. To count daily traffic, Taproot derives an internal identifier from request data (a keyed hash of the network address and browser description, not either of them). It changes every day (UTC), is never combined with another site's data or with any account, customer, or advertising ID, and is not shown to anyone.
- Monthly identifier. To estimate how many different people read a site over a week or month, Taproot derives a second identifier from request data that is specific to one site and changes at the start of each calendar month. Our edge provider keeps it with the analytics event for up to three months. It is used only to produce estimated counts, is never combined with another site's data or with any account, and is not shown to anyone.
- Visit cookie. Taproot sets one short-lived first-party cookie, taproot-visit , on published sites. It lasts 30 minutes after your last page view (Taproot stops using it at midnight UTC), holds no persistent identifier, and records which link brought you, the page you started on and how many pages you have read in this visit, so site owners can see what leads readers deeper. Taproot adds those three facts to the analytics events for the visit. The Cookie Notice lists the cookie and the choice cookie described below.
- Engagement script. Pages include a small first-party script that reports how long a page was open and how far it was read, and which external link or button was clicked (the destination site, the link label the site owner added to it, or the button text only). The report holds no visitor identifier and our edge provider keeps it for up to three months. The script stores nothing on your device.
- Link labels. Site owners can register link labels, short identifiers they put in their own links; when a visit arrives through a link carrying a registered label, the label is stored with the page view. Labels name links, not people; any other value is discarded.

Consent prompt. A site owner whose readers are in places where the law requires asking first can turn on a prompt that asks before visits are counted with the cookie. On that site the cookie is set, and the engagement script reports, only if the reader accepts, and the choice is remembered in a second cookie. The prompt is off by default. Where it is off, the cookie is set without asking. The prompt does not hold back the daily or monthly identifiers.

Global Privacy Control. Taproot honors the Global Privacy Control signal by leaving the visit cookie, the monthly identifier and the script out for that request. The page view itself is still counted in the site's totals, without those. A reader's browser that sends the signal is not shown the prompt.

Opt-out for site owners. A site's owner can keep their own browser out of the count with a preference described in the Cookie Notice.

Who sees this. Analytics reports are shown to people who have permission to view analytics on that site. Taproot does not sell this data and does not use it for advertising.

Retention. Analytics events are held by our edge provider for up to three months. Daily summaries are kept for 90 days on Grow sites and 365 days on Scale sites. Monthly count summaries and the estimated-reader counts built from the monthly identifier are kept until the site is deleted. Counts of requests we excluded from measurement, such as automated traffic, are kept for 400 days. Deleting a site or account removes our summaries of its analytics; the provider's individual events cannot be deleted earlier and expire on its schedule.

Google Search Console

A site's owner can connect Google Search Console to see how the site performs in Google Search. If they do, Taproot asks Google for read-only access to that site's search data. Taproot stores the access tokens Google issues, encrypted, and imports the queries, pages, clicks, impressions, and average positions Google reports for that site; the data contains no visitor identifiers. Daily data is kept for 90 days and monthly data for 16 months. Taproot shows the data only to people with permission to view that site's analytics, uses it only to provide this feature, does not use it for advertising, and does not sell it or share it with anyone else except to provide the feature or as the law requires. Taproot's use and transfer of information received from Google APIs adheres to the Google API Services User Data Policy, including the Limited Use requirements. When the owner disconnects Search Console, or the site or account is deleted, Taproot deletes the imported data and keeps the encrypted grant only until Google confirms that it has been revoked.

Google Business Profile

A site's owner can connect the site to one Google Business Profile location that they manage. If they do, Taproot asks Google for permission to manage that profile. Taproot stores the refresh token Google issues, encrypted, and reads the details Google reports for the location the owner chooses: the business's name, address, phone number and website, Google's place identifier, and the links Google gives for the location on its maps and for leaving a review. While the owner is choosing, Taproot holds the same details for each location the signed-in Google account manages for up to about an hour, then deletes that list.

Taproot also keeps a copy of the location's reviews so the owner can choose which ones the site shows. For each review it stores the text, the star rating, the dates, the owner's reply and, when the reviewer is not anonymous, the reviewer's display name and profile photo. Taproot refreshes the copy once a day and removes it if Google has not been read successfully for 21 days. A published page can show the reviews the owner selects, with each reviewer's name and photo; Taproot serves the photo itself, so visitors' browsers never contact Google to load it. Published pages are rebuilt when a review changes or is removed, and an earlier copy of a page is deleted a day after it is replaced, so a published review is never kept for more than 30 days after Google last returned it.

Taproot changes the profile only when a person with permission to manage the site asks it to and confirms exactly what will be sent: posting a published page to the profile, with a summary, an optional image from the page and a link to it, or replying to a review. Taproot sends nothing to the profile on its own.

Taproot shows the location's details and reviews to people with permission to manage or view that site, uses this data only to provide this feature, does not use it for advertising, and does not sell it or share it with anyone else except to provide the feature or as the law requires. Taproot's use and transfer of information received from Google APIs adheres to the Google API Services User Data Policy, including the Limited Use requirements, and Google's Business Profile APIs policies. When the owner disconnects, when the site or account is deleted, or when the site's licence no longer includes the feature, Taproot

deletes the location's details and the copy of its reviews, and keeps the encrypted grant only until Google confirms that it has been revoked.

Member-only pages

A creator can publish a page for members only. Taproot encrypts the page when it is published and releases the key only to a signed-in person whose membership is current. The site's owner and its collaborators with the right role, and the page's credited author, can read the page without a membership. Taproot's own systems handle the keys and the content in order to publish it, so Taproot can read member-only content; it is access-controlled, not copy-protected, and a member can copy what they can read. When a membership ends, a member can keep reading for a short time: up to about 15 minutes to open a page, and a page already open stays readable until it is closed or reloaded. A member-only page's title, byline, and dates, and the comments on it, are public, and the page's address stays in the site's sitemap, so search engines can list its title. Taproot keeps the page out of the site's own search.

Why we process it

We process data to provide and secure accounts and sites; publish requested content; administer site licences, memberships, payments, payouts, and taxes; communicate with users; prevent fraud and abuse; moderate content; measure visits for site owners; 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 site licences and memberships); legitimate interests (securing the service, preventing fraud and abuse, giving site owners the visit measurement described above, moderating content, improving the service); legal obligation (tax, accounting, and lawful requests); and consent for optional communications you subscribe to, for the visit cookie and script where a site asks first, and for the other optional choices this notice describes. You can withdraw consent 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. Newsletter consent is given to a specific creator's site, is recorded with the wording shown at the time, and is confirmed by email. 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: from any newsletter email by its unsubscribe link (which works without signing in), from your newsletter subscriptions and notification preferences in your account, 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, membership status, and period and access dates — not the member's payment-method details or billing address. A creator also receives what their own readers give them through the site: newsletter subscribers (with the consent record and a CSV export the creator can download), form submissions, comments and reports on the site, and per-recipient open and click status for newsletters. People a creator has given a role on the site — for example a Site Moderator — can see member names and email addresses and can read form submissions, as the creator's role settings allow.

Some data is published publicly by design: profiles, the follow lists, comments, and the content of published sites.

We do not sell personal data, and we do not share it for cross-context behavioral advertising. Taproot's own pages and templates use no third-party advertising, cross-site tracking, or analytics scripts or pixels. Our measurement is Taproot's own, and the providers that store or process it for us act on our instructions, 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;
- analytics: as stated under “Site analytics” above;
- launch-waitlist entries, including the email-consent record, are kept for 365 days from receipt, then removed by scheduled cleanup. You may ask us to delete your entry earlier at privacy@taproot.io . If you withdraw, we remove all waitlist responses associated with the address you submitted before sending any later launch email. This initial waitlist keeps no separate mailing list or exported copy of responses;
- abuse reports, including the consent record, are kept for 365 days from receipt, then removed by scheduled cleanup. You may ask us to delete a report you sent earlier at privacy@taproot.io ;
- form submissions follow the retention period saved for that form. The creator chooses within the site's applicable licence ceiling; lowering that ceiling does not shorten a longer period already saved on a form. If the creator changes the saved period, expiry is recalculated for submissions still stored from the date each was received, so shortening it can bring deletion forward. Scheduled cleanup removes expired submissions. The creator can delete them earlier, and they are removed with the site. The hash of the visitor's network address is deleted after 30 days; the separate site-and-time submission counts used for the monthly allowance are kept for 90 days;
- newsletter subscriber records, including the consent record, are kept until the subscriber erases themself, the creator removes the address, the account that owns the address is deleted, or the site is deleted; unsubscribing keeps the record so the withdrawal is remembered. Newsletter delivery and open-and-click records are kept with the site;
- a bounce or spam complaint places the address on Taproot's shared email suppression list, which stays until a Taproot administrator clears it or the account that owns the address is deleted;
- comments are kept until their author, a moderator, or the site's owner removes them, or the site is deleted;
- delivery records for emails we have sent are kept and the address on them is replaced when the account is deleted; Taproot does not currently delete the processing-queue copy of sent messages automatically; it stays after the account is deleted, apart from newsletter copies removed with their site;
- billing, tax, and transaction records are kept as required for tax, audit, and dispute periods (typically seven years);
- audit and safety records are kept while relevant to investigate abuse or satisfy legal obligations; legal-acceptance records are deleted when your account is deleted;
- application logs and traces held by Honeycomb are kept for 60 days, and its summary metrics for 13 months;
- Cloudflare Workers request logs are kept for up to seven days;
- database backups are kept for seven days.

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. Deleting your account cancels your subscriptions immediately with no

refund or credit for prepaid time, takes your sites offline, and cancels the memberships that members hold on your sites (see the Creator and Commerce Terms). Deleting a single site cancels the memberships on that site. Deleting either also removes the site's form submissions, newsletter subscribers, and analytics summaries.

We retain what the law requires or a legitimate purpose demands:

- financial and tax records (Stripe also keeps invoices for deleted customers) and records of payments to affiliates;
- audit and safety logs;
- referral records in which you were the referred person; these still hold the IP address, user-agent string, and referring page recorded when you arrived, linked only to an identifier that no longer resolves to you;
- moderation records for comments that remain, and comments you left on other people's sites (disassociated from your identity and shown as a deleted member, although the text of the comment stays);
- pages you wrote on other people's sites, which stay on those sites credited under the name the site already shows;
- processed copies of emails we sent you that sit in our processing queue.

Stripe connected accounts used for payouts are not deleted automatically; we close them by hand. Individual analytics events held by our edge provider, and logs held by our monitoring provider, expire on their own schedules as stated above.

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

You can withdraw your Taproot launch-waitlist email choice and ask us to delete your entries by emailing privacy@taproot.io from the address you submitted. You do not need to create or sign in to a Taproot account. This contact route is separate from the unsubscribe links offered by creator newsletters.

Account settings provide self-service access to correction, a data export, notification preferences, and account deletion. The export is a ZIP of your profile, content, media references, comments, memberships, billing summary, legal acceptances, site analytics summaries, and, for your sites, form submissions. It does not include image or video files, raw analytics events, secrets, or raw email. The only personal details of other people it contains are what visitors submitted through your sites' forms; a few records also carry other people's account ids, such as the authors of pages on your sites and the accounts you referred as an affiliate. It does not include member lists, newsletter subscriber lists, or other people's comments. A site's owner can export the site's newsletter subscribers as a CSV file from the newsletter page. 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. If your request is about information a creator collected on their site, such as a form answer or a newsletter subscription, we will refer you to the creator or pass the request on, and help where the law requires us to. 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 anyone under 18, and people under 18 may not create accounts. Contact us if you believe someone under 18 supplied data contrary to this notice and we will delete it.

Taproot's main systems — its application servers, database, and file storage — run in the United States,

and our email provider is configured to send from a United States region. Our edge provider, Cloudflare, serves requests worldwide and stores some data on its global network: cached copies of published sites, routing records, analytics events, and video files. We have not restricted where it stores that data. If you use the service from Canada or elsewhere, your data is transferred to and processed in the United States and possibly other countries, 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 IO, LLC, 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.