Privacy Policy

Effective May 22, 2026 · Terms of Service → · privacy@invup.me

---

This Privacy Policy explains what personal information invup collects, why, who we share it with, and the choices you have. It applies to the invup website at `invup.me`, the product at `app.invup.me`, and any other product or service we provide that links to this policy.

invup is operated by **INVUP INC.**, an Ontario, Canada corporation. In this policy, "invup," "we," "us," and "our" mean INVUP INC.

Who this policy is for

invup serves three kinds of people:

- **Members** — people who sign up to use invup to run their service business (the firm).
- **Clients** — the firm's own clients, who may receive invoices from invup on the firm's behalf and pay them through our client portal.
- **Visitors** — people who visit `invup.me` without signing up.

For members and visitors, we are the **controller** of your personal information — we decide what we collect and why. For clients, the firm is the controller and we are the **processor** acting on the firm's instructions. If you are a client and want to exercise privacy rights over data the firm has entered about you, please contact the firm directly. We will help the firm respond.

What we collect

We collect only what we need to run the product and the business.

From members, when you sign up and use invup:

- Your name, email, and a password (stored hashed, never in plain text).
- Your organisation's name, address, currency, time zone, working days, and logo.
- Your subscription details — plan, seat count, billing cycle, billing-history records, and a payment-method token issued by Stripe. We do not see or store your card number.
- The work you log in invup — time entries, projects, services, rates, clients you add, invoices you create.
- If you connect Slack, the identifiers and tokens needed to send daily prompts and accept slash commands.
- Activity logs of significant actions, with timestamps and IP address, for security and audit purposes.

From clients, on behalf of the firm:

- Whatever the firm enters about you — name, organisation, email, phone, address, additional contacts.
- The invoices the firm sends you and your payment status. If you pay through the client portal, Stripe records the payment and we record only the payment intent ID, amount, and status.
- Email delivery events (delivered, bounced, opened) for invoices we send you, returned by our email provider.

From visitors to `invup.me`:

- Nothing beyond what is strictly necessary to serve the page. We do not run analytics, marketing pixels, or advertising trackers on our marketing site.

Automatically, when you use the app:

- Server logs — request paths, timestamps, IP address, user agent.
- Session metadata and "last seen" timestamps for account security.
- Error reports when something breaks, so we can fix it.

What we do not collect

We do not collect government IDs, health information, biometric data, or children's data. invup is a business tool and is not directed to children under 13; we do not knowingly accept sign-

ups from them. If you believe a child has signed up, contact us and we will close the account and delete the data.

How we use what we collect

- **To run the product** — authenticate you, render the workspace, track time, generate and send invoices, accept payments.
- **To bill you** — process subscription payments through Stripe and send receipts.
- **To support you** — respond to your questions and help you recover access.
- **To keep the product secure** — detect abuse, investigate incidents, enforce our Terms of Service.
- **To improve the product** — understand which features get used and where things break. We do not sell your data and we do not use it to train machine-learning models you have not asked for.
- **To meet our legal obligations** — tax records, accounting, responses to lawful requests.

We rely on the legal bases of contract performance, our legitimate business interests, and your consent where consent is required. In Quebec, we rely on your consent for the collection and use of personal information as required by Law 25.

The platforms invup runs on

invup is built on infrastructure operated by other companies, typically called cloud services. Your personal information lives on those platforms as a necessary part of how the product works — they process it on our behalf, on our instructions, and only for the purpose of running invup for you. They are not separate recipients of your data. Each is listed below, with what they handle and where they process it.

Service provider	Purpose	Where they process
Railway Corp.	Hosting for the invup application — the backend, the customer portal, the PDF service, and the production database	United States
Amazon Web Services, Inc.	Encrypted database backups, static files (built application assets, uploaded files such as logos and invoice PDFs)	Canada (Montreal region)
Stripe, Inc.	Payment processing for subscriptions and client invoices	United States
Slack Technologies, LLC	Slack integration, when you choose to connect it	United States
Postmark (ActiveCampaign, LLC)	Sending transactional and invoice email	United States

When we may disclose personal information

We may disclose personal information when required by law, when responding to a valid legal request, when defending our legal rights, or in connection with a business transaction such as a merger or acquisition. If a business transaction would change who controls your personal information, we will notify you in advance.

We do not sell your personal information. We do not disclose it to advertisers.

Where your data lives, and the cross-border reality

The invup application — the backend that runs the product, the customer portal, the service that turns invoices into PDFs, and the production database — is hosted in the **United States** by Railway. The other service providers listed above also process data in the United States. Our encrypted database backups and static files (built application assets, uploaded files such as logos and invoice PDFs) are stored in **Canada (Montreal)** with AWS.

In practice, this means your personal information is **primarily stored and processed in the United States today**, with a Canadian footprint limited to backups and static files. It is subject to the laws of both jurisdictions, including U.S. laws that may permit government access in ways different from Canadian law.

We intend to move the live application tier to Canadian-resident infrastructure over time. Until that change is complete, this is the honest state of affairs.

How long we keep it

- **Active accounts:** for as long as your account is open.
- **Free-plan data:** the product hides records older than 30 days and purges them after 189 days, per the Free-plan limits.
- **Cancelled accounts:** we keep your data for 30 days after cancellation so you can change your mind. After that, we delete or de-identify it, except for records we are required to keep for tax, accounting, or legal reasons (typically up to seven years).
- **Backups:** copies in our backups roll off on the backup retention schedule and are not actively used.

If you want your data deleted sooner, contact us using the address below.

Your rights and choices

You can:

- **Access** the personal information we hold about you.

- **Correct** anything that's wrong — most fields you can edit directly in the product; for the rest, contact us.
- **Export** your data — invoices and time entries are exportable from the product; for a broader export, contact us.
- **Delete** your account and the personal information associated with it, subject to the retention exceptions above.
- **Withdraw consent** to any processing that depends on consent. Some withdrawals will mean we can no longer provide the product.
- **Complain** to a privacy regulator. Federally, that's the Office of the Privacy Commissioner of Canada; in Quebec, the Commission d'accès à l'information du Québec; in your province, your provincial regulator.

To make a request, email us at the address in the **Contact** section. We respond within 30 days. If we cannot, we will tell you why and when we expect to.

If you are in Quebec, you also have the right to information about any automated decision-making that significantly affects you. We do not currently use automated decision-making in that sense — your account decisions are made by people, not algorithms.

If you are a client (not a member) and want to exercise rights over data the firm has entered, please contact the firm. They are the controller of that information. We will assist them in responding.

How we keep it safe

We use encryption in transit (TLS) and at rest, access controls, audit logging, and the security tooling provided by our infrastructure providers. Members are responsible for keeping their account credentials safe — use a strong password and a unique one. If you believe your account has been compromised, contact us right away.

No system is perfectly secure. If a security incident affects your personal information, we will notify you and the relevant regulators as required by the *Personal Information Protection and Electronic Documents Act* (PIPEDA), Quebec Law 25, and any other applicable law.

Cookies and similar technology

The product uses the cookies it needs to keep you signed in and to keep the app working — what's commonly called "strictly necessary" cookies. The marketing site does not use marketing or analytics cookies. If that changes, we will update this policy and put a clear notice on the site.

Changes to this policy

When we change this policy, we will update the **Effective** date at the top and post the change at `invup.me/privacy`. If the change is material — a new category of data, a new sub-processor that handles a new category of data, a change in cross-border processing — we will give you reasonable advance notice, including by email when appropriate.

Contact

Questions, requests, or complaints about your personal information:

INVUP INC. Attn: Privacy Officer Email: `privacy@invup.me`

We respond within 30 days.

Version history

EFFECTIVE	WHAT CHANGED
May 22, 2026	Initial version.