Privacy Policy — Pipeit (Plumbing Copilot)

Last updated: April 8, 2026

This Privacy Policy describes how Pipeit (“we,” “us,” or “our”) collects, uses, discloses, and protects personal information when you use our public website (including pages describing Pipeit and Plumbing Copilot), our account and license management areas, our APIs used by the Pipeit desktop add-in for Autodesk Revit, and related services (together, the “Services”).

By using the Services, you agree to this Privacy Policy. If you do not agree, please do not use the Services.

---

1. Introduction

Pipeit provides software and online services for MEP design workflows. We process personal information to operate accounts, licenses, subscriptions, support, and security. We do not sell your personal information.

This policy applies to information processed through pipeit.co and our related web applications and APIs. The desktop add-in communicates with our servers only for authenticated features we describe below (for example, license verification and optional issue reporting); we do not use the add-in to collect your Revit project files, models, or design content.

The Services are not directed at children under 16, and we do not knowingly collect personal information from children under 16.

---

2. Information We Collect

2.1 Information you provide directly

- Account and profile: When you register or manage an account, we collect information such as your name, email address, and password (stored using secure hashing; we do not store your password in plain text).
- Email verification and security: We process data needed to verify email addresses, reset passwords, and maintain session security.

- API access: When you use authenticated features (including the Pipeit add-in), we process credentials and tokens used to authorize API requests to our servers, consistent with your account settings.
- Purchases and billing: When you subscribe or pay for plans, you may provide or confirm billing-related details. Payment card data is handled by our payment processor (Stripe); we do not store full payment card numbers on our servers.
- Team invitations: License holders may invite others by email. We process invitee email addresses, invitation status, and related license metadata to deliver invitations and complete onboarding.
- Support and communications: Information you send when you contact us (for example, by email or through forms), including the contents of your messages.
- Issue reports (in-app): Authenticated users may submit optional text descriptions and attach plain-text diagnostic files (for example, .txt or .log files, subject to size and type limits). Do not include secrets or personal data in attachments unless necessary for troubleshooting.

2.2 Information collected automatically (websites and APIs)

Depending on how you interact with us, we may automatically collect:

- Network and device data: Such as IP address, approximate location derived from IP, browser or client type, operating system, and timestamps.
- Usage and technical logs: Pages or endpoints accessed, HTTP referrer where available, request metadata, and error or diagnostic information recorded in server or application logs.
- Cookies and similar technologies: On our marketing site, we use essential cookies and, where configured and permitted by you, optional analytics cookies (see Section 10).

2.3 License, activation, and product access

To verify eligibility, enforce seat limits, and protect against misuse, we process data associated with license activations, including for example:

- Product identifiers (such as product keys), device identifiers, and optional device names provided by the client.

- Activation and session signals such as activation tokens, activation and deactivation timestamps, heartbeat timestamps, revocation status, and related license metadata.
- IP address and client user-agent strings supplied with activation and heartbeat requests.

When you download a software product version from your account dashboard, we also log download events, including your account identifier (if signed in), product and version identifiers, download timestamp, IP address, and user-agent string. We use this information for security monitoring, fraud and abuse prevention, auditability, troubleshooting, and product operations.

We use this information to operate the license system (including periodic “heartbeat” checks and deactivation of stale activations as configured), not to collect your design files or project content.

2.4 Beta and pre-release access

Where we offer beta or pre-release software versions, we may process email addresses (and related product or version identifiers) to control who may download or access those builds.

---

3. How We Use Information

We use personal information for purposes that include:

- Providing and improving the Services, including hosting, authentication, and customer support.
- Managing accounts, licenses, activations, team seats, invitations, and software version eligibility (including beta access where applicable).
- Processing subscriptions and payments, handling invoices where applicable, and responding to billing inquiries (with payment processing performed by Stripe).
- Sending transactional and service-related emails (such as verification, password reset, invitations, receipts, and important notices about the Services).
- Operating security and fraud prevention, abuse detection, rate limiting, troubleshooting, and audit logging.
- Analyzing how our public website is used when optional analytics are enabled and consented to.
- Complying with legal obligations and enforcing our terms and policies.

We do not use the Services to ingest or store your Revit project content for analytics or unrelated purposes.

---

4. Legal Basis (where the GDPR or UK GDPR applies)

Where European or UK data protection law applies, we rely on one or more of the following legal bases, as appropriate:

- Performance of a contract: Processing necessary to provide the Services you request (for example, account, license, and subscription handling).
- Legitimate interests: For example, securing the Services, preventing abuse, improving reliability, and understanding aggregated website usage where not overridden by your rights.
- Consent: Where required for optional cookies or analytics on our marketing site, or where we expressly ask for your consent for a specific activity.
- Legal obligation: Where we must retain or disclose information to comply with applicable law.

You may withdraw consent where processing is consent-based, without affecting the lawfulness of processing before withdrawal.

---

5. Sharing of Information

We may share personal information in these situations:

- Service providers: With vendors that help us run the Services (for example, hosting, email delivery, payment processing, and security), subject to appropriate contractual safeguards.
- Payment processing: With Stripe for payments, subscriptions, and related webhooks. Stripe processes payment data under its own terms and privacy policy.
- Professional advisers: When necessary, with lawyers, auditors, or insurers under confidentiality obligations.
- Legal and safety: When we believe disclosure is required by law, regulation, legal process, or governmental request, or to protect the rights, safety, and security of users,

the public, or Pipeit.

- Business transfers: In connection with a merger, acquisition, financing, or sale of assets, subject to appropriate protections.

We do not sell personal information as that term is commonly understood in U.S. state privacy laws.

---

6. Data Retention

We retain personal information only as long as necessary for the purposes described in this policy, including to:

- Maintain your account and fulfill subscriptions and licenses.
- Resolve disputes and enforce agreements.
- Meet legal, accounting, and compliance requirements.

Retention periods vary by data type. For example, server logs may be kept for a limited period for security and diagnostics; license and billing records may be kept longer where required for accounting or legal reasons. Issue reports and attachments are stored so we can investigate and improve the product; we delete or anonymize data when it is no longer needed, consistent with operational and legal constraints.

You may request deletion of your personal information subject to Section 9 and applicable exceptions (for example, records we must retain by law).

---

7. Security Measures

We implement reasonable administrative, technical, and organizational measures designed to protect personal information against unauthorized access, loss, or alteration. These measures include, where appropriate, access controls, encryption in transit for our websites and APIs (HTTPS), secure password hashing, and logging for security monitoring.

No method of transmission or storage is completely secure. We cannot guarantee absolute security.

---

8. Third-Party Services

8.1 Stripe

Subscription and payment processing are handled by Stripe, Inc. (and its affiliates as applicable). When you pay for a subscription, Stripe collects and processes payment details according to its own policies. We receive limited billing-related information (for example, customer identifiers, subscription status, and transaction references) needed to provide the Services.

Stripe’s privacy policy: https://stripe.com/privacy

8.2 Google Analytics (optional, marketing site)

When a Google Analytics measurement ID is configured in our environment and you consent through our cookie banner, our public website may load Google Analytics (gtag) to help us understand aggregated traffic and usage. Google may process data such as pages viewed, device and browser information, and IP address (Google may apply IP anonymization depending on configuration).

Google’s privacy policy: https://policies.google.com/privacy

You can use our cookie preferences on the site to decline optional analytics cookies. You may also use browser controls or Google’s opt-out tools: https://tools.google.com/dlpage/gaoptout

If no measurement ID is configured, analytics features are not available in that deployment.

8.3 Scheduling and demos

Our site may link to third-party scheduling tools (for example, Calendly) for booking demos or meetings. If you use those tools, the provider processes your information under its own terms.

8.4 Email delivery

Transactional email may be sent through infrastructure compatible with our configuration (for example, SMTP or cloud email APIs). Those providers process message metadata and content needed to deliver email.

---

9. User Rights

Depending on where you live, you may have rights regarding your personal information, such as:

- Access to the personal information we hold about you.
- Correction of inaccurate or incomplete information.
- Deletion, restriction, or objection to certain processing, subject to legal exceptions.
- Data portability, where applicable.
- Withdrawal of consent where processing is based on consent.
- Lodging a complaint with a supervisory authority (for example, in the EEA or UK).

To exercise these rights, contact us using the details in Section 13. We may need to verify your identity before fulfilling requests.

If you are a California resident, you may have additional rights under the CCPA/CPRA (for example, to know categories of personal information collected, to request deletion, and to opt out of “sale” or “sharing” — we do not sell personal information in the conventional sense). We will not discriminate against you for exercising privacy rights.

---

10. Cookies

We use cookies and similar technologies on our website:

- Essential cookies: Required for basic site operation, security, and preference storage (for example, remembering cookie consent choices in your browser).
- Analytics cookies: Only if a measurement ID is configured and you opt in through our cookie banner or preferences.

You can control cookies through our on-site preferences and your browser settings. Disabling certain cookies may affect site functionality.

---

11. International Transfers

We may process and store information in countries other than your country of residence, including countries that may not provide the same level of data protection. Where we transfer personal information from the EEA, UK, or Switzerland to other countries, we use appropriate safeguards (such as standard contractual clauses or other mechanisms required

by applicable law), where required.

---

12. Changes to This Policy

We may update this Privacy Policy from time to time. The “Last updated” date at the top will change when we do. For material changes, we may provide additional notice (for example, a notice on our website or by email). Your continued use of the Services after the effective date constitutes acceptance of the updated policy, except where prohibited by law.

---

13. Contact Information

If you have questions about this Privacy Policy or wish to exercise your privacy rights, contact us at:

Email: support@pipeit.co

Website: https://pipeit.co