

Privacy Policy

Effective June 4, 2026 · Version 1

ProcessModel, Inc. ("ProcessModel", "we", "us") respects your privacy. This policy explains what personal information we collect, how we use it, who we share it with, and your choices. It covers our website, the ProcessModel desktop application, the licensing and activation services that the application connects to, and the optional ProcessModel AI features.

1. Opt-In Methods

On our website, we ask for personal information from those who download and/or install our trial or evaluation software, subscribe to communications, or contact us. Providing this information is voluntary.

2. Methods Where We Need Information (Not Opt-In)

To place an order, register a product, create an account, activate a license, or participate in beta testing, certain information is required. ProcessModel has always reserved the right to limit free technical support to registered users.

3. Anonymous Information Collection

We collect general, non-identifying usage statistics about visitors to our website to analyze traffic patterns and improve the site.

4. About Cookies

Our website uses cookies to collect general information. Cookies cannot read information from your hard drive or read information from other cookies. You may disable cookies in your browser and still access the website.

5. Use of Personal Information

We use the personal information we collect to: process and fulfill orders; register products and maintain accounts; provide and validate software licenses; deliver technical support and determine support eligibility; send service notices (e.g. order confirmations, license and expiry notices); analyze website traffic; conduct surveys; and — where you have not opted out — send product news and offers.

6. Product Registration

Personal information you provide during registration or account creation is maintained in ProcessModel's database unless you direct otherwise or request deletion (see §A.10).

7. How ProcessModel AI Protects Your Information

When you use the optional ProcessModel AI features, your data remains strictly confined to your secure workspace. Your business plans, process logic, and simulation parameters are never used to train the AI models. We use enterprise-grade agreements with our AI providers (OpenAI Enterprise/API) and maintain encryption standards including TLS 1.2+ in transit and AES-256 encryption at rest.

A. Licensing & Activation Data

This section discloses the personal data collected by ProcessModel's licensing and activation system, which lets you sign in, purchase a license, and bind that license to your computer. The application contacts ProcessModel's licensing server to activate a license and to periodically confirm it (a "heartbeat").

A.1 Account and Sign-In (email + magic links)

When you create a ProcessModel account, we store your **email address** as your sign-in identity, together with the date the account was created.

Sign-in is **passwordless**: you request a sign-in link, and we email you a one-time **magic link** that is valid for a short period (currently about 15 minutes). We do **not** store a password. To operate this flow we store a **hashed, one-time token** (never the link itself in plain text) and the time it was issued and used. If single-sign-on is offered, we may also store the identity-provider reference for your account.

Administrative staff accounts (ProcessModel employees who operate the back office) use the same email-magic-link model and may optionally register a passkey (a WebAuthn security credential). These are internal staff accounts, not customer data, and are listed here only for completeness.

A.2 Machine Fingerprint and Machine Name

A paid license is bound to a specific computer. To do this, the application computes a **machine fingerprint**: a **one-way hash** (SHA-256) derived from a combination of stable hardware and system identifiers on your computer — for example its network hardware (MAC) address, hostname, and machine GUID (and, conceptually, identifiers tied to components such as the CPU, motherboard, or disk).

We store only the resulting hash. We do **not** store the raw hardware identifiers from which it is computed, and the hash is not reversible into them. The fingerprint is used solely to (a) bind a license to one machine, (b) recognize the same machine on later launches, and (c) prevent abuse of the free trial (see §A.4).

We also store a **machine name** — a human-readable computer name (for example, "MacBook-Pro-Brendan") — captured at activation so that your account page can show which computer a license is bound to without exposing the hash.

A.3 License, Activation, Heartbeat, and Binding History

For each license associated with your account we store:

- the **license tier / type** (for example trial, a Pro term license, student, or complimentary);

- the **expiry date** (if the license is time-limited);
- the **currently-bound machine** (by fingerprint) and that machine's name;
- **activation and heartbeat timestamps** — the application periodically contacts our server (roughly daily) to confirm the license is still valid on the bound machine; we record the time of the most recent successful heartbeat;
- a **binding history**: an append-only log of binding lifecycle events — when a machine was first bound, when a new machine displaced a prior one ("whoever signs in wins"), when you released a computer, and when a binding was automatically cleared after an extended period without a heartbeat. Each entry records the event type, the machine fingerprint it concerns, a timestamp, and an optional reason.

This data lets you see and manage which computer your license is on (including releasing a computer so you can move your license), and lets support diagnose activation issues.

A.4 Trial Anti-Abuse Markers

To prevent the same computer from repeatedly resetting its free trial, we store a **first-seen marker** per machine — the **machine fingerprint hash** and the date it was first seen — and, where a trial extension is granted, a **one-per-machine trial-extension record** tying that extension to one account.

For these anti-abuse markers we store **only the fingerprint hash**, never the underlying hardware identifiers. The first-seen marker is **not linked to any account**. These records are automatically purged after a period of inactivity (currently about 180 days).

A.5 Technical Request Metadata (IP, Browser)

When you request a sign-in link, sign in, or maintain an active session, we record standard technical metadata for security and abuse-prevention: your **IP address** and your **browser/device user-agent string**, together with timestamps for session creation and last use. Active sessions are stored server-side so they can be listed and revoked, and they expire on a schedule (web sessions currently up to 90 days; staff sessions are short-lived).

A.6 Audit Logs and Support Notes

We keep an **audit log** of administrative actions taken on accounts and licenses (for example issuing or revoking a license, adjusting a tier, or applying a tag). Each entry records who performed the action, what action was taken, the affected target, and a timestamp. Support staff may also attach free-form **account notes** (for example "refund issued" or "student verification requested") to your account. This information is used for support, security, fraud prevention, and record-keeping.

A.7 Payment Information (handled by Stripe)

Purchases (for example the Pro 1-, 2-, and 3-year term licenses and the Student license) are processed by our payment processor, **Stripe, Inc.** Stripe collects and processes your payment details (including card information) under **its own privacy policy and PCI-compliant systems**.

ProcessModel does not store your full card number. We store a **Stripe customer reference** (an identifier that links your account to your Stripe customer record) and **purchase records** — for example the amount, the

license duration purchased, the Stripe transaction/identifier, and the purchase date. Your Stripe customer email is kept in sync with your account email so receipts go to the right address.

A.8 Marketing (ActiveCampaign)

Where permitted, we sync your **contact email** to our marketing and CRM platform, **ActiveCampaign, LLC**, together with **tags** (for example which product or license type you have) so we can send relevant product communications. You may opt out of marketing email at any time (every marketing message includes an unsubscribe link); opting out does not affect transactional/service email such as receipts and license notices.

A.9 Retention of Licensing Data

We retain your **account, license, and purchase records** while your license is active. **Once a license has been expired for 12 months, we delete the associated account together with its license and local purchase records.** Renewing or extending your license resets this period — your data is kept while you hold an active (or recently-active) license. **Administrative and security audit logs are retained for 365 days and then deleted.** Trial anti-abuse markers are purged after a period of inactivity (currently about 180 days); sign-in tokens are short-lived and sessions expire on the schedules noted in §A.5. Independently of our systems, our payment processors (**Stripe** and **Paddle**) and our accounting records retain transaction information as required for financial and tax purposes.

A.10 Your Choices; Account Deletion; Data Subject Requests

You may review and update your account information, see which computer your license is bound to, and release that computer, from your account page. You may opt out of marketing email at any time.

To request **access to, correction of, or deletion of** your personal information — including your account, license, and associated data — contact us using the details in §10. We will respond consistent with applicable law (including the GDPR and the CCPA/CPRA where they apply). Note that some records (for example audit, purchase, and tax records) may be retained where we are legally required or permitted to keep them.

8. Citizens of the European Union (EU)

ProcessModel is based in the United States. Any information that you provide to ProcessModel will be transferred out of the EU to the United States. By providing your information, you consent to that transfer.

Personal data processed for licensing, payments, and marketing is shared with the following US-based service providers (sub-processors): **Stripe** (payment processing), **ActiveCampaign** (marketing/CRM), and our transactional email provider (magic links and receipts). See §B for the consolidated list. Where the GDPR applies, our legal bases include performance of the license contract with you (account, activation, license enforcement), our legitimate interests (security, fraud and trial-abuse prevention, audit logging), your consent (marketing email), and compliance with legal obligations (tax and accounting records). Credit card details are handled by Stripe and are retained by it only as long as necessary; ProcessModel does not retain full card numbers.

9. Additional Use of Information for Citizens of the European Union

Personal information may be shared with EU-based technical-support subcontractors and distributors for the purpose of product support and upgrade notifications.

B. Third-Party Service Providers (Sub-processors)

Provider	Role	Data shared
Stripe, Inc. (US)	Payment processing for purchases	Name/email and payment details (collected by Stripe); we store only a customer reference + purchase records
ActiveCampaign, LLC (US)	Marketing / CRM	Contact email + tags
Transactional email provider (e.g. Postmark / ActiveCampaign Postmark) (US)	Delivery of sign-in magic links and receipts	Email address + message content
OpenAI (US) — *only if you use ProcessModel AI*	Optional AI-assisted features	See §7 — not used to train models

Our hosting/infrastructure providers process data on our behalf under appropriate agreements.

10. Security of Information

We take reasonable technical and organizational precautions to protect personal information from loss, misuse, and unauthorized access, disclosure, or alteration. Sensitive values are protected in transit (TLS) and, where applicable, at rest; sign-in tokens and machine fingerprints are stored only in hashed form; full payment card numbers are never stored by ProcessModel.

11. Changes to This Policy

We may update this policy from time to time. Material changes will be reflected in the "Last Updated" date above and, where appropriate, communicated to account holders.

12. Contact Us

ProcessModel, Inc. Eagle Mountain, UT 84005, USA Phone: (801) 356-7165 Email: support@processmodel.com

See also our [End-User License Agreement](#) and [Refund Policy](#).