Privacy Policy

Effective Date: April 30, 2026 **Last Updated:** April 30, 2026 **Version:** 2.0

Porchops, Inc. ("**Porchops**," "**we**," "**us**," or "**our**") respects your privacy and is committed to protecting your personal information. This Privacy Policy describes how we collect, use, disclose, and protect personal information when you use porchops.com, app.porchops.com, and our related products and services (collectively, the "**Service**").

This Privacy Policy applies to:

- **Visitors** to our marketing website (porchops.com)
- **Waitlist subscribers** who request early access
- **Account holders and Customers** who use our product
- **End users whose personal information is processed by our Customers** through the Service (in which case our Customer is the data controller and we act on the Customer's behalf as a data processor)

We have written this policy to be readable and direct. Defined terms used here align with our Terms of Service. If anything is unclear, please contact us at **privacy@porchops.com**.

Table of Contents

---

1. Quick Summary

For people who want the gist:

- **What we collect from visitors:** name and email if you submit our waitlist form, basic privacy-respecting analytics (page views, referrer, approximate location)
- **What we collect from Customers:** account info, billing info, data you connect from third-party services, data you input into the Service
- **What we don't do:** sell your data, share your data for cross-context behavioral advertising, use your data to train general-purpose AI models, use third-party advertising trackers, or use surveillance-style session-replay tools
- **Where your data goes:** to the third-party sub-processors listed in Section 9, including Anthropic for AI processing
- **Your rights:** access, correction, deletion, export, restriction, objection, and (in California) opt-out of automated decision-making; specifics depend on your jurisdiction
- **Sub-processor changes:** we provide at least 30 days' advance notice
- **Breach notification:** without undue delay, typically within 72 hours of becoming aware (where you are a Customer affected by a breach)
- **How to reach us:** privacy@porchops.com

If you want the details, the rest of this policy explains everything.

---

2. Notice at Collection (California Consumer Privacy Act)

This section provides the "**Notice at Collection**" required by the California Consumer Privacy Act ("**CCPA**") and California Privacy Rights Act ("**CPRA**") effective January 1, 2026.

Category of Personal Information	Sources	Business Purpose	Sold/Shared?	Retention
Identifiers (name, email, IP address, account IDs)	You; cookies; sub-processors	Provide and operate the Service; account management; security	**No**	Account life + 90 days
Commercial information (subscription tier, billing history)	You; Stripe	Process payments; manage subscriptions	**No**	7 years (financial records)
Internet/electronic activity (Service usage data, login times, feature interaction)	Automatic collection	Operate, secure, and improve the Service	**No**	24 months (audit logs)
Geolocation (approximate, IP-based)	Automatic collection	Security; localization; fraud prevention	**No**	90 days (raw logs)
Inferences (preferences, derived business metrics)	Derived from your usage	Personalize the Service experience	**No**	Account life
Customer Data you upload (including End User Data)	You; Connected Services you authorize	Provide the Service per your instructions	**No**	Account life + 30 days
Audio/visual (only if you contact support)	You	Customer support	**No**	24 months

We do **not** collect:

- Sensitive personal information as defined in CCPA § 1798.140(ae) without your specific consent
- Biometric information
- Genetic information
- Information about a known child under 13 (or under 16 in jurisdictions with that digital consent age)

We do not sell or share personal information for cross-context behavioral advertising. We do not use third-party advertising trackers. As a result, the CCPA's "Right to Opt Out of Sale or Sharing" mechanism is not applicable to our practices, but you retain that right and may exercise it as described in Section 12.

---

3. Data Controller and Roles

For purposes of European data protection law (GDPR, UK GDPR, Swiss FADP):

- **When you visit our website or sign up as a Customer**, Porchops is the **data controller** of your personal information.
- **When you use the Service to process information about your customers, prospects, or other third parties (your "End Users"), you are the data controller** of that information and **Porchops is a data processor** acting on your behalf. We will execute a Data Processing Addendum (DPA) at your request, which is required if you process Personal Data of EU/UK/Swiss residents.

For purposes of California data protection law (CCPA/CPRA):

- Porchops is a **business** with respect to information we collect about visitors and Customers.
- Porchops acts as a **service provider** to our Customers with respect to End User information processed through the Service.

For purposes of other U.S. state laws (Colorado Privacy Act, Connecticut Data Privacy Act, Virginia Consumer Data Protection Act, Texas Data Privacy and Security Act, Florida Digital Bill of Rights, etc.), our roles map analogously: we are a controller for our own collection and a processor for End User Data we handle on behalf of Customers.

---

4. Information We Collect

4.1 Information You Provide Directly

When you visit porchops.com without creating an account:

- Email address (if you submit the waitlist or contact form)
- Name (if you submit the waitlist or contact form, optional)
- Any information you choose to share via communications

When you create an account:

- Name
- Email address
- Authentication credentials (handled by Clerk, our auth provider)
- Profile information you choose to provide

- Workspace and organization details
- Billing information (when you subscribe; processed by Stripe — we do not store full payment card numbers)

When you use the Service:

- Configuration settings for Connected Services
- Playbook configurations and preferences
- Communications with our support team

When you connect a third-party service (Stripe, Gmail, HubSpot, etc.):

- OAuth tokens or API credentials authorizing our access
- Data accessed through that service per the scope you grant, including but not limited to:
    - Customer records
    - Payment history
    - Email metadata and content (for connected email accounts)
    - Support tickets and customer interactions
    - Subscription and billing information

4.2 Information We Collect Automatically

Website analytics:

- IP address and approximate geographic location (city/country level)
- Browser type and version, operating system, device type
- Pages visited, time spent, referring URLs
- Date and time of visits

We use **Plausible Analytics** and **Vercel Analytics**, both designed to be privacy-respecting and **without cookies or persistent identifiers.**

Service usage data:

- Login times and account activity
- Features and pages accessed within the Service
- Performance metrics (response times, errors)
- Audit logs of actions taken in the Service (by you, by AI Systems, by Connected Services)

4.3 Information We Collect from Third Parties

- **Authentication provider (Clerk):** identity verification and basic profile information when you sign in
- **Payment processor (Stripe):** transaction confirmations, last four digits of card, billing address. We do **not** store full payment card numbers
- **Connected Services:** data accessed under the scope you authorize (Stripe Connect data, email metadata, etc.)

4.4 Information About Your End Users

When you use the Service, you may upload, transmit, or otherwise provide information about your customers, prospects, or other individuals ("**End User Data**"). We process End User Data on your behalf as a data processor. **We do not control what End User Data you provide; that is your responsibility as the data controller.**

End User Data may include names, email addresses, payment information, transaction history, communication content, and other personal information your business handles.

4.5 What We Don't Collect

- We don't collect biometric information
- We don't collect genetic information
- We don't track you across third-party sites
- We don't use device fingerprinting beyond what's necessary for security
- We don't deploy session-replay tools that record your interactions
- We don't request information about your race, ethnicity, religion, sexual orientation, political views, union membership, or health unless you specifically choose to share it for a clear support need

---

5. How We Use Your Information

We use the information we collect for the following purposes:

5.1 To Provide the Service

- Authenticating your account and securing your access
- Processing Connected Services on your behalf
- Generating AI Outputs based on your configuration and Customer Data
- Executing Authorized Actions (such as drafting communications, sending recovery emails) per your configured Playbooks

- Maintaining audit records of every action by users and AI Systems
- Providing customer support
- Processing payments and managing subscriptions

5.2 To Improve the Service

- Analyzing usage patterns to identify product improvements (using only aggregated, statistical metadata that does not include Customer Data, AI Output content, or End User Data)
- Diagnosing and fixing bugs
- Measuring performance of features
- Conducting research and developing new features

We do not use your Customer Data, End User Data, AI Outputs, or your prompts to train, fine-tune, or improve AI models — neither our own models nor any third party's general-purpose AI models. AI Outputs are generated by querying our AI providers (currently Anthropic) at the time you generate an output, subject to the contractual safeguards described in Section 9.1.

5.3 To Communicate With You

- Transactional emails about your account, billing, and the Service
- Responses to your questions and support requests
- Product updates and announcements (you can opt out of marketing emails; you cannot opt out of essential security and service notifications)

5.4 For Legal and Safety Reasons

- Complying with applicable laws and regulations
- Responding to lawful government and regulator requests
- Detecting, preventing, and addressing fraud, security issues, and abuse
- Enforcing our Terms of Service
- Establishing, exercising, or defending legal claims
- Protecting the rights, property, or safety of Porchops, our Users, or others

5.5 Aggregated and Anonymized Data

We may create aggregated, de-identified, or anonymized data from your information that cannot reasonably be used to identify you, any individual, or any specific business. We may use this data for any purpose, including business analysis and product development.

6. AI Systems and Automated Decision-Making

6.1 Use of AI Systems

The Service uses AI Systems (including Anthropic's Claude models) to generate AI Outputs based on your Customer Data and configurations. We disclose this in compliance with EU AI Act Article 50, the CCPA's Automated Decision-Making Technology regulations effective January 2026, and similar transparency requirements globally.

When you receive output from the Service, you are receiving content generated wholly or in part by AI. When the Service sends communications on your behalf, those communications are generated wholly or in part by AI.

6.2 No Training on Customer Data

We do not use your Customer Data, End User Data, AI Outputs, or your prompts to train AI models. Our AI provider (Anthropic) processes data submitted via their commercial API under their Commercial Terms, which prohibit training on customer API data and specify a 30-day deletion window (extended for trust and safety review of policy violations). We do not enroll Customer Data in any AI provider's "data sharing for model improvement" programs.

If we change AI providers, we will only engage providers offering equivalent or stronger no-training commitments for commercial API usage. We will provide at least 30 days' prior notice of any change to this commitment.

6.3 Automated Decision-Making

We do not make solely-automated decisions that produce legal or similarly significant effects on you (the Customer). The Service may generate AI Outputs that influence decisions **you** make about **your** customers, but those decisions are yours, not ours.

If you use the Service in a way that constitutes automated decision-making about individuals, **you (not Porchops) are responsible for** providing required pre-use notices, opt-out mechanisms, access requests, and appeal rights under applicable law (including CCPA's ADMT regulations effective January 1, 2027, GDPR Article 22, Colorado Privacy Act profiling rules, and similar laws). We provide configuration options and audit logs to support your compliance.

---

7. Legal Bases for Processing (GDPR / UK GDPR / Swiss FADP)

For individuals located in the EEA, UK, or Switzerland, we process Personal Data based on the following legal bases:

- **Contract (GDPR Art. 6(1)(b)):** to provide the Service that you have signed up for and to perform our obligations under the Terms of Service
- **Legitimate interests (GDPR Art. 6(1)(f)):** to operate, improve, and secure the Service; to prevent fraud and abuse; to communicate about the Service; balanced against your privacy interests
- **Consent (GDPR Art. 6(1)(a)):** where required, such as for non-essential cookies (none of which we currently use) or for communications requiring opt-in. You can withdraw consent at any time.
- **Legal obligation (GDPR Art. 6(1)(c)):** to comply with applicable laws

For End User Data you provide to the Service, **you (the Customer) are responsible for establishing the appropriate legal basis** under applicable law. We process End User Data on your documented instructions as a data processor.

---

8. How We Share Information

We do not sell your personal information within the meaning of CCPA, GDPR, or other applicable laws. We share information only as described below.

8.1 With Service Providers (Sub-processors)

We share information with the third-party services we use to operate Porchops, listed in Section 9. Each sub-processor is contractually bound to:

- Use the information only for purposes of providing services to us
- Maintain appropriate confidentiality and security
- Comply with applicable data protection law
- Be governed by terms equivalent to those in our DPA (flow-down provisions)

8.2 With Connected Services

When you connect a third-party service, we share information with that service as needed to provide the integration. For example, if you connect Stripe and configure Failed Payment Recovery, we read payment data from Stripe and may write recovery actions back to Stripe per your configuration.

8.3 In Connection with Business Transactions

If Porchops is involved in a merger, acquisition, financing, sale of assets, bankruptcy, or similar transaction, your information may be transferred as part of that transaction. We will notify you of

any such transfer that materially affects your rights and provide an opportunity to opt out where applicable.

8.4 To Comply with Law

We may disclose information when we believe in good faith that disclosure is necessary to:

- Comply with a subpoena, court order, or other legal process
- Comply with applicable law or regulation
- Cooperate with law enforcement investigations
- Protect the rights, property, or safety of Porchops, our Users, or others

We will challenge overly broad requests where appropriate and lawful, and we will notify affected Users where permitted by law.

8.5 With Your Consent

We may share information for any other purpose with your consent or at your direction.

8.6 What We Don't Do

We do **not**:

- Sell your personal information to third parties
- Share your personal information for cross-context behavioral advertising
- Use third-party advertising trackers (Facebook Pixel, Google Ads, etc.) on our website
- Permit our sub-processors to use your information for their own purposes beyond providing services to us
- Use Customer Data, End User Data, AI Outputs, or your prompts to train general-purpose AI models

---

9. Sub-processors

We use the following third-party services to operate Porchops. Each is contractually bound to appropriate security, confidentiality, and data protection obligations. We will provide at least **30 days' advance notice** before adding or replacing any sub-processor that processes Customer Data.

Sub-processor	Purpose	Location	Transfer Mechanism
Anthropic	AI/LLM processing (Claude API)	United States	Standard Contractual Clauses; commercial API terms prohibit training on customer data
Clerk	Authentication and identity management	United States	Standard Contractual Clauses
Cloudflare	DNS, CDN, file storage (R2)	Global	Standard Contractual Clauses
GitHub	Source code repository, CI/CD	United States	Standard Contractual Clauses; Microsoft DPF certification
Inngest	Background job and workflow orchestration	United States	Standard Contractual Clauses
Neon	Managed PostgreSQL database	United States	Standard Contractual Clauses
Plausible Analytics	Privacy-respecting website analytics (no cookies, no persistent identifiers)	European Union	EU-resident processing
Resend	Transactional email delivery	United States	Standard Contractual Clauses
Sentry	Error tracking and monitoring	United States	Standard Contractual Clauses
Stripe	Payment processing and billing	United States	Standard Contractual Clauses; DPF certification
Upstash	Redis cache and rate limiting	Global	Standard Contractual Clauses
Vercel	Web hosting and deployment	Global	Standard Contractual Clauses; DPF certification

The current published list is maintained at **porchops.com/legal/sub-processors**. For Customers with executed Data Processing Addendums, we will provide direct notice of new sub-processors as required by the DPA.

9.1 Data Processing by AI Providers

When the Service generates AI Outputs, your relevant Customer Data is sent to the AI provider (currently Anthropic) for processing. Specifically:

- We use Anthropic's commercial API under Anthropic's Commercial Terms
- Anthropic's Commercial Terms prohibit using customer API data to train models
- Anthropic deletes API request data within 30 days, subject to legal hold or extended retention for trust and safety review of policy violations
- We do not opt in to any AI provider's voluntary data sharing or model improvement programs

We do not log AI prompt and response content beyond what is necessary to operate the Service (such as displaying the AI Output to you, recording audit trails, and tracking costs). AI prompt and response content stored in our system is subject to the same protections as other Customer Data described in this policy.

---

10. International Data Transfers

Porchops is based in the United States. Several of our sub-processors are based in the United States or process data globally. If you access the Service from outside the United States, your information will be transferred to and processed in the United States and other jurisdictions.

For transfers from the EEA, UK, or Switzerland to the United States, we rely on:

- **Standard Contractual Clauses** approved by the European Commission as the transfer mechanism with our sub-processors
- **Supplementary measures** including encryption in transit and at rest, access controls, audit logging, and contractual confidentiality obligations
- **EU-U.S. Data Privacy Framework certifications** of our sub-processors where applicable
- **UK International Data Transfer Agreement** and **Swiss equivalents** where applicable

If you are subject to a data protection law that requires specific transfer mechanisms or notifications, please contact privacy@porchops.com to discuss your requirements.

---

11. Data Retention

11.1 Retention Periods

We retain personal information for as long as necessary to provide the Service and fulfill the purposes described in this policy:

- **Account information:** Retained while your account is active. Deleted within 90 days after account closure, except where retention is required by law (e.g., financial records typically retained 7 years).
- **Customer Data and End User Data:** Retained while your account is active. After account closure, retained for 30 days to allow recovery, then deleted, subject to your account-specific retention preferences for active accounts.
- **AI Output content (within Porchops's systems):** Retained per your retention preferences for active accounts; deleted with Customer Data after closure.
- **Audit logs:** Retained for 24 months for security and compliance purposes, then deleted.
- **Marketing communications data:** Retained until you opt out, then deleted within 30 days.
- **Backups:** Retained for 90 days, then automatically purged.
- **Financial records:** Retained for 7 years per U.S. tax and financial regulations.
- **Legal hold:** Information subject to a legal hold is retained until the hold is lifted, regardless of other retention rules.

11.2 Anthropic API Data

As described in Section 9.1, AI prompt and response data sent to Anthropic via their commercial API is processed under Anthropic's Commercial Terms with a 30-day deletion window (subject to trust and safety review for policy violations).

11.3 Deletion Requests

You can request deletion of your personal information at any time as described in Section 12. We will honor deletion requests subject to legal retention obligations.

---

12. Your Rights

Depending on your jurisdiction, you may have the following rights regarding your personal information.

12.1 Universal Rights (We Honor for All Users)

- **Access:** request a copy of the personal information we hold about you

- **Correction:** request correction of inaccurate or incomplete information
- **Deletion:** request deletion of your information, subject to legal retention obligations
- **Export:** request a portable copy of your information in a commonly used format
- **Account closure:** close your account at any time

12.2 European Economic Area, UK, and Switzerland (GDPR / UK GDPR / FADP)

In addition to universal rights:

- **Restriction:** request that we limit how we process your information
- **Objection:** object to our processing based on legitimate interests
- **Automated decision-making:** request human review of any solely automated decision producing legal effects on you (note that the Service does not make solely-automated decisions about Customers as described in Section 6.3)
- **Withdraw consent:** withdraw consent at any time where processing is based on consent
- **Lodge a complaint:** file a complaint with your local data protection authority

12.3 California (CCPA / CPRA)

In addition to universal rights:

- **Right to know:** specific pieces of personal information collected, sources, purposes, and recipients (much of this is described in this policy and the Notice at Collection in Section 2)
- **Right to delete:** subject to enumerated exceptions in CCPA § 1798.105(d)
- **Right to opt out of sale or sharing:** as described in Section 2, we do not sell or share for cross-context behavioral advertising; you retain this right and may exercise it
- **Right to limit use of sensitive personal information:** we do not use sensitive personal information in ways that would trigger this right
- **Right to non-discrimination:** we will not discriminate against you for exercising your rights
- **Right to opt out of automated decision-making (effective January 1, 2027 for "significant decisions"):** see Section 6.3

12.4 Other U.S. State Laws

We honor rights granted to you under applicable U.S. state privacy laws, including:

- **Colorado Privacy Act** — including profiling opt-out rights
- **Connecticut Data Privacy Act**

- **Virginia Consumer Data Protection Act**
- **Texas Data Privacy and Security Act**
- **Florida Digital Bill of Rights**
- **Indiana, Montana, New Jersey, Oregon, Tennessee, Delaware, and other state laws** as they take effect

These rights generally include access, correction, deletion, portability, opt-out of targeted advertising and sale, and (in some states) opt-out of profiling for "significant decisions."

12.5 Other Jurisdictions

We honor rights under applicable law including Canada (PIPEDA, Quebec Law 25), Brazil (LGPD), Australia (Privacy Act), and other comprehensive data protection laws.

12.6 How to Exercise Your Rights

To exercise any of these rights:

- Email **privacy@porchops.com** with your request
- Include sufficient information for us to verify your identity (typically the email address associated with your account)
- Specify which right you are exercising and what information your request relates to

We will respond within timeframes required by applicable law (generally 30 days for GDPR, 45 days for CCPA, with extensions where allowed). There is no charge for exercising these rights, except in extraordinary circumstances permitted by law.

If we receive a request from a Customer's End User, we will direct that End User to the Customer who controls the data, except where we are required by law to act directly.

12.7 Authorized Agents and Browser Signals

For California residents and others with applicable rights:

- You may use an **authorized agent** to submit a request on your behalf, with proper documentation
- We honor **Global Privacy Control (GPC)** browser signals as opt-out preference signals where required by law
- For automated decision-making opt-outs (CCPA effective January 1, 2027), you may submit requests through methods we provide at that time

---

13. Security

We take security seriously and implement reasonable administrative, technical, and physical safeguards to protect your information, including:

- **Encryption in transit:** all data transmitted to and from the Service uses TLS 1.2 or higher
- **Encryption at rest:** Customer Data is encrypted at rest in our database
- **Access controls:** access to systems and data is limited to personnel who need it for their job functions
- **Authentication:** multi-factor authentication required for administrative access
- **Tenant isolation:** database-level row-level security ("RLS") ensures Customer Data is isolated by Workspace
- **Audit logging:** all actions in the Service are logged for security and compliance purposes
- **Incident response:** we maintain documented procedures for detecting, responding to, and notifying affected parties of security incidents
- **Vendor security:** we assess the security practices of our sub-processors

13.1 No Method is 100% Secure

While we work hard to protect your information, no method of transmission or storage is completely secure. We cannot guarantee absolute security, and you use the Service at your own risk to that extent.

13.2 Breach Notification

If we become aware of a Personal Data Breach affecting your Customer Data:

- **For Customers (where you are the data controller and we are the processor):** we will notify you **without undue delay, and typically within 72 hours** of becoming aware. We will provide information sufficient to enable you to comply with your own breach notification obligations under applicable law (including the GDPR's 72-hour controller notification requirement to supervisory authorities).
- **For information we control (such as your account information):** we will notify affected individuals and regulators in accordance with applicable law.
- We will provide reasonable assistance in your investigation and notification activities

---

14. Children's Privacy

The Service is not directed at children under 13 (or under 16 in jurisdictions where that is the

applicable age of digital consent — including the EU under GDPR Art. 8 in many member states), and we do not knowingly collect personal information from children under those ages.

If you believe we have inadvertently collected information from a child, please contact us at privacy@porchops.com and we will delete it promptly.

If you use the Service to process information about End Users who are children, you are responsible for obtaining required parental consents and complying with applicable child privacy laws (such as COPPA in the United States, the Age-Appropriate Design Code in California and the UK, and similar laws elsewhere).

---

15. Cookies and Tracking Technologies

15.1 What We Use

The Service uses minimal cookies and tracking technologies:

- **Strictly necessary cookies:** required for authentication, security, and basic Service functionality (session cookies, CSRF tokens). These cannot be disabled without breaking the Service.
- **Analytics:** Plausible Analytics and Vercel Analytics, which are designed to be privacy-respecting and **do not** use cookies or persistent identifiers to track users across sites.
- **Preference cookies:** to remember your settings (e.g., dark/light mode). Set only after you change a preference.

15.2 What We Don't Use

We do not use:

- Third-party advertising trackers (Facebook Pixel, Google Ads, TikTok Pixel, etc.)
- Cross-site tracking cookies
- Device fingerprinting beyond what's necessary for security
- Session replay tools that record user interactions
- Cookies for marketing or behavioral advertising

15.3 Your Choices

You can configure your browser to refuse cookies or alert you when cookies are set. If you disable strictly necessary cookies, parts of the Service may not function correctly.

We honor **Global Privacy Control (GPC)** signals where required by applicable law.

---

16. Changes to This Policy

We may update this Privacy Policy from time to time. When we make material changes, we will:

- Update the "Last Updated" date and version number at the top
- Notify Customers and waitlist subscribers via email at least 30 days before changes take effect (except for changes required by law or that do not materially reduce your rights, which may take effect immediately)
- Post a notice in the Service or on porchops.com

Your continued use of the Service after changes take effect constitutes acceptance of the updated policy.

---

17. Contact Us

For questions, concerns, or requests related to this Privacy Policy or our data practices:

Porchops, Inc. Privacy: privacy@porchops.com **General contact:** hello@porchops.com **Security:** security@porchops.com **Legal:** legal@porchops.com **Mailing address:** Porchops, Inc. c/o Registered Agent [Stripe Atlas-assigned registered agent address] Wilmington, DE [ZIP] United States

For data protection authority complaints (EU/UK/Swiss residents), you may lodge a complaint with your local supervisory authority. A list is available at https://edpb.europa.eu/about-edpb/about-edpb/members_en.

For California residents, our toll-free number for privacy requests will be added when we have customers in California with active accounts; until then, please use privacy@porchops.com.

Data Protection Officer

Porchops has designated a privacy contact for data protection inquiries (privacy@porchops.com). We do not currently meet the threshold to require a formally appointed Data Protection Officer under GDPR Article 37, but we maintain GDPR-aligned practices and will appoint a DPO if and when our processing activities require it.

This Privacy Policy is provided to be transparent about how we handle your information. If anything is unclear, please ask. We will work in good faith to address your concerns.