IntakeClean

Document intake for small law firms
Generated 2026-05-04

Privacy Policy

How we collect, use, share, and protect information. Covers both firm representatives (controller scope) and uploaded end-client documents (processor scope).

IntakeClean — Privacy Policy

Last updated: `[YYYY-MM-DD]` **Effective:** `[YYYY-MM-DD]`

This Privacy Policy explains how `[LLC NAME]`, a New Jersey limited liability company ("**IntakeClean**," "**we**," "**us**," or "**our**"), collects, uses, shares, and protects information in connection with the IntakeClean software-as-a-service product, websites, and APIs (collectively, the "**Service**").

> **Two roles, important difference.**
>
> - When IntakeClean handles information about a **Customer's** representatives (e.g., a law-firm administrator who creates an account, signs in, manages billing), IntakeClean is acting as a **business / controller**. This Privacy Policy applies directly.
> - When IntakeClean handles information about a Customer's **End-Clients** (the people whose documents are uploaded through the Service), IntakeClean is acting as a **service provider / processor** on behalf of the Customer. The Customer's own privacy notice — not this one — is the primary notice to End-Clients. We process End-Client data only as instructed by the Customer under our Data Processing Addendum. End-Clients with questions about their data should contact the Customer (their attorney or the firm) first.

---

1. Information we collect

1.1 Information you provide

- **Account information:** name, email, password (hashed), firm name, phone, billing address.
- **Billing information:** payment method tokens (we do not store card numbers; payments are tokenized via Stripe).
- **Communications:** messages you send to support, sales, or via in-app chat.
- **Configuration:** firm settings (AI provider preferences, escalation thresholds, document-type vocabulary, document request templates).

1.2 Information collected automatically

- **Log data:** IP address, browser type and version, operating system, referring URL, pages viewed, timestamps, and actions taken in the Service.
- **Device data:** device identifiers and approximate location derived from IP.
- **Cookies and similar technologies:** see `05-cookie-notice.md`.

1.3 Customer Content (uploaded documents)

When a Customer or End-Client uploads a document, the Service stores the document file, derived images, OCR transcripts, classification labels, quality flags, and processing metadata. This data is **Customer Content**, and we process it on the Customer's behalf under the Data Processing Addendum. We do not access Customer Content except as reasonably necessary to operate, secure, or troubleshoot the Service or as required by law.

1.4 Information from third parties

- **Authentication providers** (e.g., Supabase Auth, Google OAuth) provide your name and email when you sign in.
- **Payment processor** (Stripe) provides billing-status updates.
- **Marketing partners** (if applicable) may share information about your interest in the Service.

2. How we use information

We use information to:

- (a) provide, operate, secure, and improve the Service;
- (b) authenticate users, process payments, and send transactional notices;
- (c) communicate with you about updates, security alerts, and support;
- (d) detect, investigate, and prevent fraud, abuse, and security incidents;
- (e) comply with legal obligations and enforce our Terms; and
- (f) with your consent, send marketing communications (which you can unsubscribe from at any time).

We do not use Customer Content to train any general-purpose AI model. When a Customer enables the optional AI integration, prompts and document content are sent to the configured inference provider for the duration of that request only, in accordance with the DPA and the Subprocessor List.

3. Legal bases for processing (EEA/UK)

Where the General Data Protection Regulation or the UK GDPR applies, we rely on the following legal bases:

- **Contract** — to provide the Service to you under your subscription.

- **Legitimate interests** — to secure the Service, prevent abuse, and improve the Service, where those interests are not overridden by your fundamental rights.
- **Consent** — for marketing emails and certain cookies.
- **Legal obligation** — to comply with tax, accounting, and legal-process requirements.

4. How we share information

We share information only as described below:

- **Subprocessors.** We share information with vetted third-party providers that perform services on our behalf. The current list, with the categories of data each receives, is at `07-subprocessor-list.md`.
- **Within Customer organizations.** Information is visible to other Authorized Users of the same Customer account, consistent with the roles set by the account administrator.
- **Legal and safety.** We may disclose information if we believe in good faith that disclosure is necessary to comply with law, lawful process, or governmental request; to protect the rights, property, or safety of any person; to investigate fraud or abuse; or to enforce our Terms.
- **Business transfers.** If IntakeClean is involved in a merger, acquisition, or asset sale, information may be transferred subject to a contractual commitment by the recipient to honor this Privacy Policy or to provide equivalent or greater protections, with notice to affected Customers.
- **With your direction.** We share information when you direct us to (e.g., when you enable an integration like Resend, Twilio, or a Hugging Face Inference Endpoint).

We do **not** sell Personal Information for money. We do not "share" Personal Information for cross-context behavioral advertising as those terms are defined under the California Consumer Privacy Act / California Privacy Rights Act (CCPA/CPRA).

5. Data retention

- **Account information:** retained for the life of the account and for **up to 24 months** after deletion to address legitimate business needs (audit, dispute, fraud prevention) and legal obligations.
- **Customer Content:** retained according to the Customer's configuration. After termination of a subscription, Customer Content is available for export for **60 days** and is then deleted from active systems within **30 days**, with backup-system removal within **90 days** thereafter, except as required by law.
- **Logs:** typically **30–90 days**; security and audit logs may be retained up to **two (2) years**.
- **Billing records:** retained for **seven (7) years** to comply with tax law.

6. Security

We use administrative, technical, and physical safeguards designed to protect information, including encryption in transit (TLS 1.2+) and at rest, role-based access controls, multi-tenant isolation enforced via row-level security, audit logging, principle-of-least-privilege access for personnel, and routine review of subprocessors. **No system is perfectly secure.** Promptly report suspected security issues to `[security@CONTACT EMAIL]`.

7. International transfers

Our servers and certain subprocessors are located in the United States. If you access the Service from outside the U.S., your information will be transferred to and processed in the U.S. and other countries that may have different data-protection laws than your jurisdiction. Where required, transfers from the EEA, UK, or Switzerland are subject to the European Commission's Standard Contractual Clauses (SCCs) and the UK Addendum.

8. Your privacy rights

Subject to applicable law, you may have the right to:

- **Access** the personal information we hold about you.
- **Correct** inaccurate personal information.
- **Delete** personal information.
- **Port** personal information to another service.
- **Restrict or object to** certain processing.
- **Withdraw consent** at any time, where processing is based on consent.
- **Opt out** of "sale" or "sharing" of personal information for cross-context behavioral advertising — note: we do not engage in such sale or sharing, but you may submit a confirming request.
- **Limit use** of "sensitive personal information" under the CCPA/CPRA — note: we use sensitive information only for the disclosed purposes of providing the Service.
- **Lodge a complaint** with a supervisory authority (in the EEA/UK).

To exercise rights with respect to **your account** at IntakeClean, email `[privacy@CONTACT EMAIL]`. We will respond within the time required by applicable law (generally 30–45 days).

To exercise rights with respect to **End-Client data** (documents uploaded through the Service), please contact the Customer (the firm) — they are the controller for that data; we will assist them in fulfilling your request.

We will not retaliate against you for exercising your rights.

8.1 Authorized agents (California)

You may use an authorized agent to submit a request on your behalf. We will require written verification of the agent's authority and may verify the request directly with you.

8.2 Right to no discrimination

We do not discriminate against you for exercising any privacy right.

9. Children

The Service is not directed to children under 13 (or 16 in the EEA/UK), and we do not knowingly collect personal information from such children. If you believe we have collected information from a child, contact `[privacy@CONTACT EMAIL]` and we will delete it.

10. Automated decision-making

The Service performs automated classification and quality flagging of uploaded documents. These outputs are **assistive only** and the Customer's staff makes the final decision on each document. Automated outputs are not used to make decisions that produce legal or similarly significant effects on End-Clients without human review by the Customer.

11. California "Shine the Light"

California residents may request information about the categories of personal information we have shared with third parties for those third parties' own direct marketing purposes. We do not currently engage in such sharing. Requests may be sent to `[privacy@CONTACT EMAIL]`.

12. Changes to this Privacy Policy

We will update this Policy from time to time. The "Last updated" date at the top reflects the most recent change. If we make a material change, we will notify you (via email to the account's billing contact and/or in-product notice) at least thirty (30) days before the change takes effect, except for changes required by law.

13. Contact

`[LLC NAME]` Attn: Privacy `[PRINCIPAL OFFICE ADDRESS]` Email: `[privacy@CONTACT EMAIL]`
