



Privacy Policy

Effective date: September 8, 2026 · **Last updated:** October 12, 2026

This Privacy Policy explains how **ACE Applications**, doing business under the Alden Data Solutions brand (“Alden,” “we,” “us,” or “our”), handles information through aldendatasolutions.com, its public sample demonstration, and separately contracted client systems.

1. Scope and Important Service Distinction

This Policy applies to visitors, prospective clients, and authorized users of a contracted Alden system.

Public website and sample demonstration

The public document-intake workspace is a deterministic demonstration. It uses a built-in catalog of sample documents and sample outputs. It does not provide an open upload function for a visitor’s own documents, does not require a user account, and does not process payments.

Contracted client systems

Alden Data Solutions is a DBA owned by ACE Applications. This Policy covers both Done for You pipeline implementation and the separate Subscription offer. A production system is designed separately for each business client. Depending on the written scope, it may include private accounts, client-provided documents, extracted data, review queues, integrations, migration, and billing. The signed order form, statement of work, blueprint, or data-processing agreement identifies the selected offer, contracting party, and deployment-specific processing terms. Those agreed terms control where they differ from this Policy; browsing an offer does not authorize client-document processing.

Discovery and validation samples

Before sending samples, agree in writing on their purpose, eligible data types, transfer method, authorized access, providers, processing locations, retention period, and return or deletion arrangements, including logs and backups. Use synthetic or redacted representative documents where possible and share only what is needed. Do not send confidential or sensitive documents merely to request a quote. Discovery samples are not automatically approved for production use or other purposes.

Automated extraction requires typed PDFs with embedded, machine-readable text. OCR is not supported. Handwriting is not supported. Photos and image-only scans are not supported. Any possible manual data-entry work must be separately discussed and scoped; it is not included or promised available.

2. Information We May Collect

Category	Examples	When it may be collected
Inquiry and business contact data	Name, company, business email, message content, requested workflow, and documents voluntarily shared during discovery.	When a person emails us, requests a blueprint discussion, or communicates about services.
Basic technical data	IP address, browser/device type, request time, page or resource requested, and security or diagnostic logs.	When the website or a hosted service is accessed. Hosting and security infrastructure may create these records automatically.
Client account data	Name, business email, role, permissions, authentication identifiers, and activity records.	Only when a contracted client system includes authenticated access.
Client document and operational data	Uploaded or connected documents, extracted fields, validation results, exception-review decisions, output files, and migration records.	Only within a contracted production workflow or during authorized testing using client-provided samples.
Commercial and payment data	Selected tier, invoice status, transaction reference, billing contact, and limited payment metadata. Full card details are handled by the applicable payment provider, not Alden.	When a client purchases services or pays an invoice.

We do not knowingly seek sensitive personal information unless it is necessary for an agreed business workflow and appropriate safeguards have been addressed in writing. Clients must not submit regulated or unusually sensitive data unless Alden has expressly accepted that data type in the applicable agreement.

3. How We Use Information

We may use information to:

- respond to inquiries, evaluate fit, prepare scopes, and communicate with prospective or current clients;
- configure, test, operate, maintain, secure, and support contracted document-automation systems;
- extract, validate, review, transform, migrate, or deliver data as directed by the client;
- administer accounts, permissions, invoices, payments, processing allowances, and service renewals;
- detect abuse, investigate failures, maintain security, and comply with legal obligations; and
- improve reliability using aggregated or de-identified operational information where appropriate.

We do not sell or rent client data. Any AI processing must be identified in the agreed workflow before client data is sent. Provider training or secondary-use rules depend on the selected service, account terms, and configuration; this Policy does not promise a universal non-training policy for third parties.

4. Cookies and Local Storage

The current public demonstration may use browser session storage for limited interface preferences, such as remembering that an orientation tip was dismissed during the session. We do not currently describe the public demo as using advertising cookies or cross-site behavioral advertising. A contracted system or future site feature may use

strictly necessary cookies or similar storage for authentication, security, and session continuity; material changes will be reflected in this Policy.

5. Service Providers and Data Sharing

We disclose information only as reasonably necessary to provide, secure, support, or collect payment for services; comply with law; protect rights and safety; or complete a business transaction with appropriate protections. Providers may differ by client deployment and written scope.

Provider	Function and information involved
Google Firebase	May provide authentication, application hosting, database, storage, or related cloud functions for a contracted system. It may receive account, technical, or client workflow data when that system is configured to use Firebase.
Stripe	May process card payments, billing events, fraud-prevention signals, and transaction records. Stripe receives payment and billing details needed to complete the transaction; Alden does not receive full card numbers.
Payoneer	May facilitate invoices, payment transfers, or other business-payment services and receive billing, transaction, and identity information required by Payoneer.
Client-designated services	When expressly scoped, data may be sent to the client's chosen storage, accounting, ERP, CRM, spreadsheet, database, or API destination. The client controls and authorizes those destinations.

These providers operate under their own terms and privacy notices. The named providers are conditional examples, not a verified provider list for a particular engagement. Hosting, storage, automation, or AI/model providers may also receive the data needed for their scoped function. Before accepting client samples or production data, the parties must identify the actual providers, data sent to each, processing locations, access arrangements, and applicable retention and secondary-use terms in writing. A provider change affecting these arrangements must be addressed with the client before using it for client data. API access alone does not establish confidentiality, deletion, non-training, or regulatory compliance guarantees.

6. Client Instructions and Responsibilities

For client documents and operational data, the business client generally determines what data is submitted, why it is processed, who may access it, and where output is sent. Alden processes that information to provide the contracted service. Clients are responsible for having appropriate authority, notices, consents, and lawful grounds for the data they direct Alden to process and for configuring access to client-designated destinations.

7. Retention and Deletion

Retention depends on the type of information and the contracted workflow:

- Public demo:** The demo uses built-in samples. It does not accept a visitor's own document upload. Limited technical logs may be retained for security, diagnostics, and service operation.
- Inquiry and commercial records:** We may retain communications, proposals, contracts, invoices, and transaction records for business, tax, dispute, and legal purposes.

- **Discovery and validation samples:** Agree a retention period and return or deletion procedure before transfer, covering originals, extracted outputs, temporary copies, logs, provider-held copies, and backups. Do not assume immediate deletion or a fixed retention period that has not been agreed.
- **Production workflow data:** Client files, extracted data, caches, logs, and backups are retained according to the applicable written scope, operational need, provider backup cycles, and legal requirements. Some workflows process files transiently; others require agreed storage, review queues, migration, or audit records.

Authorized clients may request deletion or return of eligible data. We may retain information that is required for legal compliance, fraud prevention, security, billing, dispute resolution, backup integrity, or enforcement of agreements. Deletion from backups may occur on the applicable provider's normal rotation schedule.

8. Security

Security measures must be assessed for the scoped deployment and recorded in the applicable agreement. Depending on the deployment, these may include encrypted transport, authenticated access, role-aware permissions, provider security controls, monitoring, and restricted administrator access; this list is not verification that every control is implemented. This Policy does not assert a compliance certification, suitability for regulated data, or an absolute confidentiality or security guarantee. No internet transmission, storage platform, or software system can be guaranteed completely secure. Clients must protect credentials, limit user access, maintain secure destination systems, and promptly report suspected compromise.

9. International Processing

Alden and its providers may process information in the United States and other locations where they operate. Those locations may have different privacy laws from the user's location. Any required client-specific transfer mechanism or regulated-data arrangement must be agreed in writing before that data is processed.

10. Children's Privacy

The website and services are directed to businesses and are not intended for children under 18. We do not knowingly collect personal information from children through the public website.

11. Privacy Choices and Requests

Depending on applicable law and the relationship to Alden, a person may request access, correction, deletion, restriction, or a copy of eligible personal information. We may need to verify identity and authority before acting. If the information is controlled by an Alden business client, the request should usually be directed to that client; we will assist the client as required by the applicable agreement and law.

12. Changes to This Policy

We may update this Policy as services, providers, or legal requirements change. The "Last updated" date will identify the current version. Material changes may also be communicated through the website, a contracted system, or direct client notice when appropriate.

13. Contact

Privacy questions or requests may be sent to:

ACE Applications, doing business as Alden Data Solutions

Email: info.alddatasolutions@gmail.com

Website: alddatasolutions.com

General template notice: This document provides general information about Alden's current practices and is not legal advice or a guarantee of compliance with every law. Client-specific, regulated, or multi-jurisdictional processing may require additional terms and review by a qualified attorney.

© 2026 Alden Data Solutions · Owned and operated by ACE Applications