Privacy Agreement &
Data Processing Addendum

Effective Date: April 20, 2026

1. Scope and Roles

This Privacy Policy explains how Technology Coast Partners LLC ("Fluent," "we," "us," "TCP") collects, uses, shares, and otherwise processes information when you (a) visit our websites, landing pages, forms, and related online properties (the "Site"), and (b) use the Fluent platform and related services (the "Service").

For personal data contained in Customer Data processed through the Service, Customer is the controller, business, or equivalent primary decision-maker under applicable law, and Fluent acts as a processor, service provider, or equivalent contractor processing such Customer Data only on Customer's documented instructions and as further described in the DPA. For personal data collected directly by Fluent through the Site, demo requests, sales interactions, and service administration, Fluent is typically the controller.

To the extent applicable under U.S. state privacy laws, including the California Consumer Privacy Act, Fluent acts as a "service provider" or "contractor" with respect to Customer Data processed on behalf of customers and does not sell or share such personal data for cross-context behavioral advertising.

2. Information We Collect

Site Information

We may collect contact details you submit, such as name, company, email address, phone number, title, and any other information you provide in forms, scheduling requests, meeting requests, chat interactions, or correspondence. We may also collect communications content, device and usage data such as IP address, browser type, operating system, referring pages, interactions with the Site, approximate location derived from IP, and information collected through cookies or similar technologies used for analytics, functionality, and performance.

Service Information

We may collect and process account and billing information for administrators, authentication and access logs, implementation and support communications, usage telemetry, configuration information, and Customer Data submitted to or through the Service, including documents, records, emails, attachments, and integration data.

3. How We Use Information

We use information to provide, operate, host, maintain, support, secure, troubleshoot, and improve the Service; process Customer Data and generate Output as directed by Customer; manage billing, subscriptions, and service administration; respond to inquiries and schedule demos; communicate transactional, operational, or service-related

notices; send marketing communications where permitted by law; monitor performance, abuse, fraud, and security incidents; enforce our agreements; comply with law; and protect rights, property, and safety.

4. How We Share Information

We do not sell personal data. We may disclose information to service providers, subprocessors, contractors, hosting providers, infrastructure providers, AI processing vendors, logging and monitoring providers, analytics tools, customer support tools, implementation partners, and professional advisors that assist us in providing or supporting the Site or Service, subject to appropriate contractual protections. We may also disclose information when Customer enables integrations or directs transfers to integration partners or third-party systems; to comply with legal obligations, lawful requests, court orders, or government investigations; to enforce agreements or protect rights and safety; and in connection with a financing, due diligence process, merger, acquisition, corporate transaction, or sale of assets.

Where required, Fluent may maintain and provide an up-to-date list of material subprocessors or a mechanism to obtain that list.

5. AI Processing

The Service may use AI and machine learning systems, including third-party providers, to process Customer Data and produce Output. Such processing may involve document ingestion, optical character recognition, classification, extraction, summarization, transformation, or workflow-related analysis. Output may be probabilistic and may contain errors. Unless explicitly agreed otherwise in writing, Fluent does not use Customer Data to train public or shared models.

6. International Transfers

If personal data is transferred across borders, including outside the jurisdiction in which it originated, Fluent will implement appropriate safeguards as required by applicable law, which may include contractual protections such as Standard Contractual Clauses or comparable legal transfer mechanisms.

7. Data Retention

We retain information only for as long as reasonably necessary for the purposes described in this Privacy Policy, including to provide the Service, support customers, maintain business and financial records, resolve disputes, enforce agreements, and comply with legal obligations. Retention, deletion, and return of Customer Data are further described in the applicable agreement, retention policy, and/or DPA.

8. Security

We use reasonable administrative, technical, and organizational safeguards designed to protect personal data and Customer Data, such as encryption in transit and at rest, access controls, monitoring, and incident response processes. No system is 100% secure, and no method of transmission or storage can be guaranteed to be completely secure.

9. Your Choices and Rights

You may opt out of marketing communications using unsubscribe links or by contacting us. You may control certain cookies through browser settings and any cookie banner we provide. For requests relating to personal data contained in Customer Data, individuals should generally direct requests to the applicable Customer, which is the controller of that data. Fluent will assist Customers with data subject requests to the extent required by law and contract. For personal data Fluent collects directly through the Site or service administration, you may contact us using the details below regarding access, correction, deletion, or other applicable rights, subject to verification and applicable legal limitations.

10. Children

The Site and Service are not directed to children, and we do not knowingly collect personal information from children.

11. Contact

Email: privacy@fluenterp.com

Address: 2100 Coral Way Suite 603, Miami, Florida 33145

Phone: +1 (305) 854-8900

12. Changes

We may update this Privacy Policy from time to time. The Effective Date above indicates when this Privacy Policy was last updated. Material changes may be communicated by reasonable means.

13. Governing Law (Florida)

To the extent applicable, this Privacy Policy is governed by the laws of the State of Florida, without regard to conflict-of-laws principles.

Data Processing Addendum

This Data Processing Addendum ("DPA") forms part of the agreement between Technology Coast Partners LLC ("Fluent", "Processor") and Customer ("Controller") governing Customer's use of the Fluent platform and related services (the "Service").

1. Roles of the Parties

For purposes of applicable data protection laws, Customer is the Controller, Business, or equivalent regulated party, and Fluent is the Processor, Service Provider, or equivalent contractor. Processor will process Personal Data solely on behalf of Controller and in accordance with Controller's documented instructions, unless otherwise required by applicable law.

2. Subject Matter and Duration

This DPA applies to all Processing of Personal Data carried out by Processor in connection with the Service and remains in effect for the duration of Controller's use of the Service and until return or deletion as described below.

3. Nature and Purpose of Processing

Processor processes Personal Data for purposes including ingesting documents such as invoices and purchase orders; extracting, classifying, transforming, routing, and structuring data; generating draft outputs for ERP and workflow-related processes; supporting integrations with third-party systems as directed by Controller; and operating, maintaining, supporting, securing, troubleshooting, and improving the Service. Processing is limited to what is necessary to provide the Service and meet Processor's contractual and legal obligations.

4. Categories of Data Subjects

Personal Data processed may relate to Controller's employees, contractors, administrators, end users, vendors, suppliers, customers, business partners, and individuals referenced in financial, procurement, operational, or business documents contained in Customer Data.

5. Categories of Personal Data

Personal Data may include names, business contact details, email addresses, phone numbers, business identifiers, job titles, invoice and payment information, transactional and financial data, document metadata, login and access logs, and other Personal Data contained in Customer Data or support interactions.

6. Controller Instructions

Processor will process Personal Data only: (a) on documented instructions from Controller; (b) as necessary to provide, support, secure, and improve the Service in a manner consistent with the agreement and Documentation; and (c) as required by applicable law. If Processor is required by law to process Personal Data outside Controller's instructions, Processor will inform Controller where legally permitted to do so.

7. Confidentiality and Personnel

Processor will ensure that personnel authorized to process Personal Data are bound by appropriate confidentiality obligations and receive training appropriate to their roles regarding data protection, privacy, and security practices.

8. Security Measures

Processor implements appropriate technical and organizational measures designed to protect Personal Data, including, as appropriate, encryption in transit and at rest, role-based access controls, least-privilege principles, secure cloud infrastructure, monitoring, logging, anomaly detection, backup and recovery processes, and incident response procedures. No security program can guarantee absolute security, and security is a shared responsibility that depends in part on Controller's identity and access management, endpoint controls, and configuration decisions.

9. Subprocessors

Processor may engage Subprocessors to provide the Service. Processor will maintain an up-to-date list of Subprocessors or a mechanism to access that list; ensure such Subprocessors are contractually bound to data protection obligations substantially consistent with this DPA; and remain responsible for Subprocessors' performance of relevant obligations. Processor will notify Controller of new or replacement Subprocessors where required, and Controller may object on reasonable grounds related to data protection. If the parties cannot resolve the objection in good faith, Controller may terminate the affected Service(s) in accordance with the agreement.

10. International Transfers

Where Personal Data is transferred outside its jurisdiction of origin, Processor will implement appropriate safeguards as required by applicable data protection laws, which may include Standard Contractual Clauses, comparable transfer mechanisms, or equivalent safeguards.

11. Data Subject Rights; Assistance

Processor will assist Controller, to the extent reasonably possible and legally required, in responding to data subject requests relating to access, correction, deletion, restriction, objection, portability, or similar rights. If Processor receives a request directly from a data subject relating to Customer Data, Processor will, to the extent legally permitted, direct the request to Controller.

12. Personal Data Breach Notification

Processor will notify Controller without undue delay after becoming aware of a Personal Data Breach affecting Customer Data. To the extent available, such notification will include the nature of the breach, likely consequences, and measures taken or proposed to address and mitigate the breach.

13. Data Deletion and Return

Upon termination or expiration of the Service, Processor will delete or return Customer Data, including Personal Data, at Controller's election where available under the Service and technically feasible, subject to applicable retention requirements, backup lifecycle limitations, and Processor's need to retain data where required by law or reasonably necessary for security, dispute preservation, or compliance purposes.

14. Audit Rights

Processor will make available information reasonably necessary to demonstrate compliance with this DPA. Any audits or assessments must be reasonable in scope and frequency, conducted no more than once annually unless required by law or following a confirmed material security incident, subject to advance notice, confidentiality obligations, and appropriate security controls, and must not unreasonably disrupt Processor's operations. Where available, Processor may satisfy audit requests by providing third-party assurance reports, certifications, summaries, or audit responses, such as SOC 2 reports, in lieu of an on-site audit.

15. Additional Legal Terms

Limitation of Liability

To the maximum extent permitted by law, Processor's total aggregate liability arising out of or related to this DPA will not exceed the total fees paid or payable by Controller for the Service in the twelve (12) months preceding the event giving rise to the claim, unless applicable data protection laws require otherwise.

Indemnification

Controller shall indemnify, defend, and hold harmless Processor from and against claims, damages, liabilities, and expenses arising from Controller's use of the Service, violation of the agreement, or violation of applicable law, subject to the terms of the main agreement.

Termination / Suspension

Processor may suspend or terminate access to the Service for breach of the agreement. Upon termination, Controller's access will cease and Customer Data will be handled in accordance with the agreement, Privacy Policy, and this DPA.

Governing Law (Florida) and Venue

This DPA shall be governed by the laws of the State of Florida, without regard to conflict-of-law principles. Any disputes shall be resolved exclusively in the state or federal courts located in Florida, consistent with the venue clause in the main Terms.

Modifications

Processor may update this DPA from time to time to reflect changes in the Service, law, or subprocessors. Continued use of the Service constitutes acceptance of the updated DPA, except where applicable data protection laws require a different process.