<!-- !!! ATTORNEY REVIEW REQUIRED BEFORE PUBLICATION This Data Processing Addendum template was drafted by Capstone Horizon LLC as a working draft. It has not been reviewed by licensed legal counsel. Do not present to enterprise customers as a binding addendum until reviewed and approved by a qualified attorney. Date of draft: April 21, 2026
!!! -->

Data Processing Addendum

Effective Date: [Insert Effective Date of MSA or separate DPA execution date]
Version: v1.0.0
Template Last Updated: April 22, 2026
Parties: Capstone Horizon LLC ("Processor") and [Customer Legal Name] ("Controller")

This Data Processing Addendum ("DPA") is entered into between Capstone Horizon LLC, an Arizona limited liability company doing business as DeployReady ("Processor"), and the customer entity identified in the applicable Master Subscription Agreement or order form ("Controller"). This DPA supplements the Master Subscription Agreement or Terms of Service between the parties (the "Agreement") and governs Processor's processing of Personal Data on behalf of Controller.

In the event of a conflict between this DPA and the Agreement, this DPA controls with respect to data processing matters.

Article 1: Definitions

"Personal Data" means any information relating to an identified or identifiable natural person that Controller submits to the Service.

"Processing" means any operation performed on Personal Data, including collection, storage, use, disclosure, transfer, and deletion.

"Data Subject" means the natural person to whom Personal Data relates.

"Controller" means the entity that determines the purposes and means of processing Personal Data. Under this DPA, Controller is the Customer.

"Processor" means the entity that processes Personal Data on behalf of the Controller. Under this DPA, Processor is Capstone Horizon LLC.

"Subprocessor" means any third-party engaged by Processor to process Personal Data on Controller's behalf.

"Technical and Organizational Measures" ("TOMs") means the security controls Processor implements to protect Personal Data, as described in Annex II.

"Service" has the meaning given in the Agreement.

"Breach" means a confirmed security incident resulting in unauthorized access to, disclosure of, or destruction of Personal Data.

Article 2: Scope and Roles

2.1 Controller. Controller is the data controller of Personal Data that Controller submits to the Service. Controller determines the purposes and means of processing that Personal Data.

2.2 Processor. Processor processes Personal Data solely on behalf of Controller, in accordance with Controller's documented instructions as set forth in the Agreement and this DPA, and for no other purpose.

2.3 Nature and Purpose of Processing. Processor processes Personal Data to provide the DeployReady solicitation analysis and proposal generation platform, including authentication, data storage, AI-assisted content generation, audit logging, and customer support.

2.4 Categories of Personal Data. The Personal Data processed under this DPA includes: account holder names and email addresses, company personnel names and roles included in the company profile, and any other personal data Controller chooses to include in uploaded content.

2.5 Data Subjects. Data Subjects include: Controller's employees and end users who access the Service, and individuals whose information Controller includes in the company profile (e.g., personnel listed for proposals).

2.6 Term of Processing. Processor processes Personal Data for the duration of the Agreement, and thereafter only as required to complete deletion as specified in Article 7.

Article 3: Processor Obligations

3.1 Documented Instructions. Processor processes Personal Data only on Controller's documented instructions. The Agreement and this DPA constitute the entirety of documented instructions. If Processor receives a legal order requiring processing beyond these instructions, Processor will notify Controller before complying, unless prohibited by law.

3.2 Confidentiality of Authorized Personnel. Processor ensures that all personnel authorized to process Personal Data are subject to confidentiality obligations and are trained on data protection requirements.

3.3 Technical and Organizational Measures. Processor implements and maintains the TOMs described in Annex II. Processor may update TOMs over time to reflect improvements, provided that updates do not materially reduce the overall level of protection.

3.4 Subprocessors. Processor engages Subprocessors only as listed in Annex III. Processor will give Controller at least 30 days' written notice before adding or replacing a Subprocessor. If Controller reasonably objects to a new Subprocessor on data protection grounds, Controller may notify Processor in writing during the notice period. If the parties cannot resolve the objection within 30 days, Controller may terminate the Agreement without penalty, with pro-rata refund for any prepaid unused term. Processor remains fully liable for Subprocessors' acts and omissions under this DPA.

3.5 Data Subject Assistance. Processor will assist Controller in responding to Data Subject access, correction, deletion, portability, restriction, and objection requests, using the technical capabilities of the Service. Requests directly received by Processor will be forwarded to Controller within 5 business days.

3.6 Breach Notification. Processor will notify Controller at the security contact on file within 72 hours of confirming a Breach. The notification will include: (a) a description of the nature of the Breach; (b) categories and approximate volume of Personal Data affected; (c) likely consequences; and (d) measures taken or proposed to address the Breach. Processor will provide updates as more information becomes available.

3.7 Return or Deletion. Upon termination of the Agreement, Processor will delete Controller's Personal Data within 30 days, subject to the audit log retention exception described in the Data Handling Policy. Upon

written request, Processor will provide written confirmation of deletion. If Controller requests return of data, Processor will provide a machine-readable export before deleting.

3.8 Compliance Assistance. Processor will make available to Controller, on request, information reasonably necessary to demonstrate compliance with this DPA, including a copy of the FAR 52.204-21 Self-Attestation document (Annex II basis).

Article 4: Controller Obligations

4.1 Legal Basis. Controller represents and warrants that it has a lawful basis under applicable law to submit Personal Data to the Service and to instruct Processor to process it as contemplated by the Agreement and this DPA.

4.2 No Prohibited Data. Controller represents and warrants that it will not submit Prohibited Data (as defined in Terms of Service Section 4) to the Service. Controller acknowledges that Processor's security architecture is not designed for FCI, CUI, or classified information processing.

4.3 Data Subjects' Rights. Controller is responsible for informing Data Subjects about the processing of their Personal Data and for receiving and routing Data Subject requests to Processor where Processor's assistance is needed.

Article 5: Subprocessors (Annex III)

The following Subprocessors are authorized to process Personal Data:

Subprocessor	Purpose	Personal Data Categories	Location
Railway	Application hosting, database storage and compute	All customer data at rest and in transit	AWS us-east-1, USA
Stripe	Payment processing, billing	Billing name, billing address, payment method metadata	USA
OpenAI	LLM inference for proposal generation	Solicitation content and company profile data included in prompts	USA
Anthropic	LLM inference for proposal generation	Solicitation content and company profile data included in prompts	USA
xAI (Grok)	LLM inference for proposal generation	Solicitation content and company profile data included in prompts	USA
Resend	Transactional email delivery	Account email address, name (for salutation)	USA

Not Product Subprocessors: Google Workspace (used for Capstone Horizon company email only) and Instantly.ai (used for Capstone Horizon outbound sales outreach only) do NOT process DeployReady customer data and are not listed above.

Processor will give 30 days' advance notice to Controller before adding any new product Subprocessor.

Article 6: Technical and Organizational Measures (Annex II)

The following TOMs describe Processor's security controls for Personal Data:

Control Area	Implementation
Encryption at rest	AES-256 via Railway Postgres (default).
Encryption in transit	TLS 1.2 minimum on all ingress via Railway HTTPS.
Access control	Server-side session authentication required for all data-bearing routes. Role-based permissions (owner/admin/member).
Tenant isolation	Application-layer tenant_id binding on every query. Postgres Row-Level Security policies on 19 tenant-scoped tables where DB role permits.
Authentication	Email + password with scrypt (N=16384, 64-byte key, per-user random salt). Constant-time comparison. 5-attempt-per-15-minute lockout.
Audit logging	audit_logs table captures: user, tenant, action, resource, IP address, user agent, timestamp on every logged action.
Physical security	Inherited from Railway / AWS us-east-1 (SOC 2, ISO 27001). No Capstone physical infrastructure.
Backup	Railway daily automated Postgres snapshots, 7-day retention, AES-256.
Vulnerability management	Manual npm audit; CI integration on roadmap (Q3 2026). Drizzle ORM prevents SQL injection. TypeScript strict-mode.
Breach notification	Controller notified within 72 hours of confirmed Breach per Article 3.6.
Incident response	Documented Incident Response Plan maintained at capstonehorizon.com/legal/.
Personnel confidentiality	All personnel with data access are subject to confidentiality obligations.
Subprocessor management	Subprocessors under contractual data protection obligations; 30-day advance notice to Controller before changes.

Detailed mapping to FAR 52.204-21 controls is available in the FAR 52.204-21 Self-Attestation document, provided to Controller on request.

Article 7: Audit Rights

7.1 Self-Assessment. Processor will make available to Controller, upon written request with 30 days' notice, its most recent FAR 52.204-21 Self-Attestation and any available third-party audit reports or certifications.

7.2 On-Site Audit. Controller may, no more than once per year and with at least 30 days' written notice, conduct or commission an audit of Processor's data processing practices. Any auditor must execute a non-disclosure agreement acceptable to Processor before commencing the audit. Audits are conducted at Controller's cost. Processor may decline an audit if it is disruptive, unreasonably broad, or presents a security risk, and will propose alternative means of demonstrating compliance.

7.3 Cooperation. Processor will cooperate with reasonable audit requests and provide relevant documentation, records, and personnel access consistent with the scope agreed in writing.

Article 8: Term

This DPA takes effect on the date of the Agreement (or the date both parties sign this DPA, if executed separately) and remains in force for the duration of the Agreement. Obligations under Articles 3.7 (deletion), 7 (audit), and this Article 8 survive termination.

Article 9: Liability

9.1 DPA Liability Cap. Processor's total liability arising from or related to this DPA is subject to the liability limitations in the Agreement.

9.2 Processor Responsibility. Processor is responsible for Subprocessors' acts and omissions with respect to Personal Data to the same extent Processor would be responsible if performing the processing directly.

Article 10: Governing Law

This DPA is governed by the laws of the State of Arizona, Pima County, consistent with the Agreement. Any disputes under this DPA are subject to the dispute resolution provisions of the Agreement.

Signatures

Processor (Capstone Horizon LLC):

Signature: ————————————————————————
Name: David Diaz
Title: Founder / CEO
Date: ————————————————————————

Controller ([Customer Legal Name]):

Signature: ————————————————————————————

Name: ————————————————————————————

Title: ————————————————————————————

Date: ————————————————————————————