

FETCHLINE

CONSULTANCY LLC

ENTERPRISE ADDENDUM

DATA PROCESSING ADDENDUM

Personal Data Protection Terms Under the Master Service Agreement

Version 1.0
August 5, 2026

CONFIDENTIAL — PREPARED FOR INTERNAL AND CLIENT USE

Table of Contents

1. Introduction and Scope

This Data Processing Addendum (this “DPA”) forms part of the Master Service Agreement (the “MSA”) between Fetchline Consultancy LLC (“Fetchline” or “Processor”) and the client identified in the signature block (“Client” or “Controller”). This DPA applies whenever Fetchline processes Personal Data on Client's behalf in connection with the Services. In case of conflict between this DPA and the MSA regarding Personal Data processing, this DPA controls.

1.1 Definitions. “Personal Data” means information relating to an identified or identifiable natural person processed by Fetchline on Client's behalf under the MSA, such as resident names, contact details, communications, and account records. “Processing,” “Data Subject,” “Controller,” and “Processor” have the meanings given under applicable data protection laws, including U.S. state privacy laws and, where applicable, the EU/UK GDPR. “Subprocessor” means a third party engaged by Fetchline to process Personal Data on Client's behalf.

2. Roles and Instructions

2.1 Roles. As between the parties, Client is the Controller (or a processor acting for another controller) and Fetchline is the Processor of Personal Data processed under the MSA.

2.2 Controller Responsibilities. Client is responsible for: the accuracy and lawfulness of Personal Data it provides; establishing a lawful basis for processing; providing required notices to and obtaining any required consents from Data Subjects (including residents); and issuing lawful processing instructions.

2.3 Processor Responsibilities; Instructions. Fetchline will process Personal Data only on Client's documented instructions — including the MSA, applicable SOWs, and this DPA — unless required to do otherwise by law, in which case Fetchline will inform Client unless legally prohibited. Fetchline will promptly inform Client if it believes an instruction violates applicable data protection law.

2.4 Purpose Limitation. Fetchline will not sell Personal Data, share it for cross-context behavioral advertising, use it to train AI models, or process it for any purpose other than performing the Services and complying with law, consistent with the data handling principles of the MSA.

3. Confidentiality and Personnel

3.1 Personnel. Fetchline ensures that all personnel authorized to process Personal Data are bound by confidentiality obligations and receive appropriate data protection training, and that access is limited to personnel who need it to perform the Services.

4. Security Measures

4.1 Technical and Organizational Measures. Fetchline will implement and maintain appropriate technical and organizational measures to protect Personal Data against accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access, appropriate to the risk, including:

- Least-privilege, role-based access with unique credentials per person;

- Multi-factor authentication on accounts with access to Personal Data where supported;
- Encryption of Personal Data in transit; encryption at rest where Fetchline controls storage;
- Secure, vaulted storage of credentials and secrets;
- Deployment of automations within Client's own infrastructure whenever practical, so Personal Data remains in Client's custody;
- Prompt revocation of access upon project completion or personnel change;
- Logging and monitoring appropriate to the systems involved.

4.2 Updates. Fetchline may update its measures from time to time, provided the updates do not materially reduce the overall protection of Personal Data.

5. Subprocessors

5.1 Authorization. Client provides general authorization for Fetchline to engage Subprocessors to support the Services. Fetchline will: (a) maintain a current list of Subprocessors with access to Personal Data, available on request; (b) provide notice of new Subprocessors before granting them access, giving Client a reasonable opportunity to object on legitimate data protection grounds; and (c) impose data protection obligations on Subprocessors no less protective than this DPA. Fetchline remains liable for its Subprocessors' performance.

5.2 Objections. If Client reasonably objects to a new Subprocessor and the parties cannot agree on a solution, Client may terminate the affected SOW as to services that cannot be provided without that Subprocessor, with a pro-rata refund of prepaid, unused fees.

6. International Transfers

6.1 Transfer Mechanisms. Fetchline processes Personal Data in the United States. Where Personal Data subject to the EU/UK GDPR or similar laws is transferred internationally, the parties will implement an appropriate lawful transfer mechanism, such as the applicable standard contractual clauses (incorporated by reference upon execution) or another recognized safeguard, and will cooperate to complete any required documentation.

7. Data Subject Requests and Assistance

7.1 Assistance. Taking into account the nature of the processing, Fetchline will assist Client through appropriate technical and organizational measures in responding to Data Subject requests (access, correction, deletion, portability, objection) and in meeting Client's obligations regarding security, breach notification, and data protection assessments. If Fetchline receives a request directly from a Data Subject, it will promptly forward the request to Client and not respond except to direct the Data Subject to Client, unless legally required.

8. Personal Data Breach Notification

8.1 Notice. Fetchline will notify Client without undue delay, and in any event within seventy-two (72) hours, after becoming aware of a Personal Data Breach affecting Personal Data processed under this DPA. The notice will describe, to the extent known: the nature of the breach, categories and approximate volumes of affected data and Data Subjects, likely consequences, and measures taken or proposed. Fetchline will reasonably cooperate with Client's investigation, remediation, and any required notifications. Fetchline's notice is not an admission of fault.

9. Deletion and Return

9.1 End of Processing. Upon termination or expiration of the Services, or upon Client's written request, Fetchline will, at Client's choice, return or delete Personal Data in its possession or control, and delete remaining copies within ninety (90) days, except where retention is required by law or the data resides in routine encrypted backups scheduled for deletion, which remain protected under this DPA until deleted. Because Fetchline deploys within Client systems whenever practical, in most engagements Fetchline holds little or no Personal Data at project end; deletion then consists of revoking Fetchline's access.

10. Audits

10.1 Audit Rights. Fetchline will make available to Client information reasonably necessary to demonstrate compliance with this DPA, including responses to reasonable written security questionnaires and summaries of relevant policies. No more than once per year (except after a Personal Data Breach or where required by a regulator), Client may conduct, at its expense and on at least thirty (30) days' notice, an audit of Fetchline's relevant processing activities, during business hours, subject to reasonable confidentiality and scope protections and without access to other clients' information.

11. Signatures

Executed as part of and subject to the MSA:

FETCHLINE CONSULTANCY LLC

Signature

Name: _____ Title: _____ Date: _____

CLIENT

Company Name: _____

Signature

Name: _____ Title: _____ Date: _____