Data Processing Addendum

Helmsted, Inc. · Template v1.2 · [Month Day, Year]

TEMPLATE. This document is a template provided for review purposes and is not an executed agreement. It must be reviewed and approved by legal counsel, and completed with the bracketed terms, before use. Where a Pilot Agreement or other written agreement between the parties addresses the same subject matter, that agreement controls.

1. Parties and Purpose

This Data Processing Addendum ("DPA") is entered into between Helmsted, Inc. ("Helmsted") and [Adviser Firm legal name] ("Firm"), effective as of [Effective Date], and supplements the [Pilot Agreement / Master Services Agreement] between the parties (the "Agreement").

This DPA governs Helmsted's processing of Adviser Client Data in connection with the Helmsted platform, and is intended to support the Firm's service provider oversight obligations under Regulation S-P (17 CFR §248.30) and applicable state privacy laws.

2. Definitions

"Adviser Client Data" means nonpublic personal information and other data relating to the Firm or its clients that Helmsted processes on the Firm's behalf, including client financial documents, planning outputs, communications, portal inputs, and AI-derived outputs.

"Security Incident" means a confirmed or reasonably suspected unauthorized access to, or acquisition, use, or disclosure of, Adviser Client Data.

"Subprocessor" means a third party engaged by Helmsted to process Adviser Client Data in delivering the platform.

3. Roles; Processing Instructions

Helmsted acts as a service provider and data processor on behalf of the Firm. Helmsted processes Adviser Client Data only to provide and support the platform in accordance with the Agreement, this DPA, and the Firm's documented instructions, and for no other purpose. Helmsted does not sell Adviser Client Data and does not use it to train artificial intelligence models.

All Helmsted personnel with access to Adviser Client Data are bound by written confidentiality obligations.

4. Security Measures

Helmsted maintains administrative, technical, and physical safeguards designed to protect the security, confidentiality, and integrity of Adviser Client Data, as described in the Helmsted Security Overview (as updated from time to time), including: encryption in transit (TLS 1.2+) and at rest (AES-256); role-based access controls with multi-factor authentication for Helmsted personnel access to production systems; logical segregation of each firm's data; append-only audit logging; and zero-data-retention agreements with Helmsted's third-party AI API providers.

Audit logs are retained for a minimum of five (5) years, with the most recent two (2) years immediately accessible, to support the Firm's books and records obligations under Advisers Act Rule 204-2.

5. Subprocessors

5.1 Authorization. The Firm provides general authorization for Helmsted to engage the Subprocessors listed in Exhibit A.

5.2 Flow-Down. Helmsted binds each Subprocessor to a written agreement imposing data protection obligations no less protective than those in this DPA, including the obligation to notify Helmsted of Security Incidents without undue delay. Helmsted remains responsible for its Subprocessors' acts and omissions.

5.3 Changes; Right to Object. Helmsted will provide the Firm at least thirty (30) days' advance written notice of any material change to Exhibit A. The Firm may object in writing on reasonable data protection grounds within that period, and the parties will work in good faith to resolve the objection before the change takes effect.

6. Security Incident Notification

6.1 Timeline. Helmsted will notify the Firm's designated compliance contact in writing without undue delay, and in any event no later than seventy-two (72) hours, after becoming aware of a Security Incident.

6.2 Content. The notice will describe, to the extent known: the nature and scope of the incident, the categories of Adviser Client Data involved, the measures taken or planned to contain and remediate it, and a contact for further information. Helmsted will supplement the notice as the investigation develops and will cooperate with the Firm's own notification obligations, including its customer notification obligations under amended Regulation S-P.

7. Data Return and Deletion

7.1 During the Term. Helmsted will honor the Firm's reasonable requests to correct, export, or delete Adviser Client Data.

7.2 Upon Termination. Upon termination or expiration of the Agreement, Helmsted will, at the Firm's election, return Adviser Client Data in a commonly used format and will delete or de-identify raw Adviser Client Data within thirty (30) days of termination, except where retention is required by law. Deletion events are logged with timestamp and reason.

8. Audits and Diligence

Upon the Firm's reasonable written request, no more than once annually absent a Security Incident, Helmsted will make available information reasonably necessary to demonstrate compliance with this DPA, including its then-current Security Overview, subprocessor list, and available third-party attestations. Helmsted will complete the Firm's reasonable security diligence questionnaires.

9. Data Residency

Helmsted stores and processes Adviser Client Data in [the United States / North America — confirm scope with Helmsted before execution; see the Security Overview and subprocessor list for storage locations].

10. General

This DPA is incorporated into the Agreement. In the event of a conflict between this DPA and the Agreement with respect to the processing of Adviser Client Data, this DPA controls. This DPA terminates automatically upon termination of the Agreement, provided that obligations relating to deletion and confidentiality survive.

Signatures

HELMSTED, INC. By: _____ Name: _____ Title: _____ Date: _____

[ADVISER FIRM] By: _____ Name: _____ Title: _____ Date: _____

Exhibit A — Subprocessors

The current list of Helmsted subprocessors, including each subprocessor's service, data accessed, and storage location, is published at helmsted.ai/security/subprocessors and is incorporated into this DPA by reference as of the Effective Date. The list as of July 28, 2026 comprises thirteen (13) subprocessors.