

Data Processing Addendum

Helmsted, Inc. Version 1.7 · September 19, 2026 helmsted.ai/company/dpa

This Data Processing Addendum ("DPA") is entered into between Helmsted, Inc., a Delaware corporation ("Helmsted"), and the registered investment adviser identified in the Order that incorporates this DPA ("Adviser"). This DPA supplements the Pilot Order, Order Form, Pilot Agreement, or Master Subscription Agreement between the parties (the "Agreement") and forms part of it. Where an Order identifies a version of this DPA, that version governs; a copy of the incorporated version is delivered to Adviser when the Order is executed.

Helmsted processes Adviser Client Data to provide the contracted services. Separately authorized client services and professional sharing are permitted only under this DPA, applicable law, and source restrictions. A client agreement does not itself expand rights in information received for Adviser.

Professionals receiving records for their own client engagements are separate recipients. Providers processing on Helmsted's behalf are subject to the applicable Subprocessor requirements. Client information embedded in a professional contact or referral record remains protected as client information.

The Exhibit A version delivered with the executed Order identifies the initially authorized Subprocessors. Subprocessor changes follow section 5.3; amendments to this DPA follow section 10.2.

1 Definitions

For purposes of this DPA:

- "Adviser Client Data" means any nonpublic personal information, as defined in 17 CFR §248.3(t), relating to Adviser's clients or prospective clients that is provided to or received by Helmsted in connection with the platform.
- "Incident" means unauthorized access to, acquisition, use, disclosure, alteration, loss, or destruction of Adviser Client Data, or a security breach resulting in unauthorized access to a customer information system maintained by Helmsted or a Subprocessor for Adviser.
- "Platform" means the Helmsted software platform and related services provided under the Agreement.
- "Reg S-P" means Regulation S-P: Privacy of Consumer Financial Information and Safeguarding Customer Information, 17 CFR Part 248, as amended.
- "Subprocessor" means any third party engaged by Helmsted to process Adviser Client Data on Helmsted's behalf in connection with the Platform, as listed in Exhibit A.

- "ZDR Agreement" means a verified arrangement with an AI provider prohibiting model training and providing zero retention of customer inputs and outputs for the services used, as required by section 3.3.
- "Usage Data" means technical and operational data generated by use of the Platform (such as feature usage, performance metrics, and error or diagnostic logs) that does not include the content of Adviser Client Data.
- "Structural Knowledge" means knowledge about data formats, file layouts, schemas, and document structures encountered in providing the Platform, excluding any client content or identifiers.
- "De-identified Aggregated Data" means data derived from Adviser Client Data that has been irreversibly de-identified and aggregated across multiple adviser firms such that it cannot reasonably be used to identify Adviser, any client, or any account.
- "Authorized Professional" means a professional or firm, including an adviser, accountant, attorney, or insurance professional, authorized by the client or a legally authorized representative to access designated records for specified services.
- "Client Records" means documents, profile information, and other records supplied by or for a client for the client's services, excluding Firm Work Product and Restricted Feed Data except where the rights applicable to a particular copy permit it to be retained for the client.
- "Firm Work Product" means client-specific professional deliverables and the firm's internal notes, workflows, and configuration. It excludes Helmsted Technology.
- "Restricted Feed Data" means information subject to source-provider limits on use, sharing, retention, or transfer, including applicable custodial and Plaid data.
- "Client Account" means an account established under accepted client terms. A firm-created household record alone does not establish client acceptance.
- "Helmsted Technology" means Helmsted's software, reusable tools, templates, methods, and improvements, excluding client information, firm-confidential material, and client-specific professional deliverables.

2 Scope and Permitted Purpose

2.1 Scope

This DPA applies to all Adviser Client Data that Helmsted receives, accesses, processes, stores, or otherwise handles in connection with providing the Platform to Adviser, including data received passively through communication channel integrations.

2.2 Permitted Purpose

Helmsted may process Adviser Client Data to provide and support the authorized services, including organizing, analyzing, and exchanging information; operating communications, integrations, and workflows; maintaining records and security; and complying with law. Adviser instructs Helmsted to facilitate client-directed sharing and continuing client services only where the necessary rights, notices, and authorizations exist. Such processing remains subject to source restrictions.

A client's relationship with another professional does not alone require Adviser's additional approval. This does not grant rights in another person's records, protected firm materials, or restricted feeds.

2.3 Prohibited Uses

Helmsted will not sell, rent, or transfer Adviser Client Data for unrelated commercial purposes; use it for unrelated marketing; or process it inconsistently with the permitted purposes, instructions, or this DPA. Section 2.4 sets the exclusive operation and improvement permissions and does not authorize model training.

2.4 Service Improvement: Usage Data, Structural Knowledge, and De-identified Data

Helmsted will not sell Adviser Client Data, use it for unrelated marketing, or process it beyond the permitted purposes and instructions. Helmsted may use content-free technical Usage Data, Structural Knowledge excluding client content and identifiers, and permitted De-identified Aggregated Data to operate, secure, and improve its services, subject to source restrictions. De-identified data must not reasonably identify or link an individual, account, or firm; Helmsted will not attempt re-identification.

Adviser Client Data, Usage Data, and De-identified Aggregated Data will not be used to train or fine-tune AI models. Plaid and custodial account content, including derived account content, is excluded from de-identified aggregation and remains subject to its source terms. Client information will not be used for unrelated network marketing or commercial profiling. Any client-specific matching requires the authorized service purpose, applicable disclosures, and source permissions.

Client-specific outputs, analyses, and normalized data remain Adviser Client Data. Rights in those records follow the applicable client and firm rights; Helmsted does not obtain ownership by processing them.

3 Security Measures

3.1 Technical and Organizational Measures

Helmsted will implement and maintain reasonable administrative, technical, and physical safeguards to protect Adviser Client Data, including at a minimum:

- Encryption of Adviser Client Data at rest (AES-256) and in transit (TLS 1.2 or higher);
- Role-based access controls limiting access to personnel who require it to provide the Platform;
- Logging and monitoring of access to systems that store or process Adviser Client Data;
- Regular assessment and remediation of security vulnerabilities; and
- Personnel screening consistent with Helmsted's HR security policy, written confidentiality obligations, and security training for personnel with access to Adviser Client Data.

3.2 Security Program

Helmsted will maintain a written information security program consistent with Reg S-P §248.30. Helmsted's security overview is available at helmsted.ai/security and in the Security Overview document provided at onboarding.

3.3 Zero Data Retention for AI Processing

Helmsted will submit Adviser Client Data to AI providers only under verified arrangements prohibiting model training and providing zero retention of customer inputs and outputs for the services used. Required account and service settings must be maintained. Helmsted's retention of platform records is governed separately by section 6.

Supported text paths mask detected sensitive identifiers before model submission. Images may contain unmasked identifiers, and masking does not remove all personal information.

3.4 Updates

Helmsted may update its technology and security measures while maintaining the protections required by this DPA and law. Material contractual changes follow the amendment procedure.

4 Incident Response and Notification

4.1 Incident Response and Notification

Helmsted will maintain a written program to detect, assess, contain, respond to, and recover from Incidents. Helmsted will notify Adviser in writing as soon as possible and no later than 72 hours after becoming aware of an Incident or reasonably suspecting it has occurred or is reasonably likely to have occurred. Notice will not await confirmation, a completed investigation, or a finding of harm. A shorter applicable deadline controls.

Initial notice will include known facts about the nature, timing, systems, information and persons affected, response measures, and a follow-up contact. Helmsted will send it to the compliance contact with a copy to the primary contact, supplement it promptly, preserve relevant evidence, and reasonably cooperate with investigation, recovery, and required notices.

Adviser remains responsible for ensuring required individual notice, including where delivery is delegated by written agreement. Neither party's independent duties or stricter Plaid or other notice requirements are displaced.

5 Subprocessors

5.1 Authorized Subprocessors

Adviser acknowledges that Helmsted engages third-party Subprocessors to provide infrastructure and related services supporting the Platform. The current list of Helmsted's Subprocessors, including their names, the nature of their services, the data each accesses, and its location, is set forth in Exhibit A, published at helmsted.ai/security/subprocessors with its own version number, effective date, and change history.

5.2 Subprocessor Obligations

Helmsted will conduct risk-based Subprocessor diligence and monitoring, enter into written agreements imposing protections no less protective than this DPA, and remain responsible for Subprocessors' acts and omissions to the same extent as if Helmsted performed the processing directly.

5.3 Changes to Subprocessors

Helmsted maintains the current Subprocessor list at helmsted.ai/security/subprocessors. Publication of an updated list constitutes notice of Subprocessor changes. Adviser may request email notice of changes at security@helmsted.ai. If Adviser objects to a change, Adviser may terminate as provided in the Agreement.

6 Data Retention and Return

6.1 Required Records

Helmsted retains data for authorized services and applicable legal or agreed preservation duties. Contract-covered audit and processing records are retained at least five years from creation, the first two immediately accessible. Longer periods and different legal starting events apply where required. Ending an engagement does not end those duties.

Adviser maintains its required archive; Helmsted honors its express preservation, export, and regulatory-cooperation commitments. Retained compliance copies are restricted to that purpose. Records must not be altered or de-identified in a way that defeats preservation duties.

6.2 Return and Deletion

Subject to lawful preservation and authorized continuity, upon termination or Adviser's written request Helmsted will, within 30 days and at Adviser's election, return the affected Adviser Client Data in a commercially reasonable format or securely delete it, as required by the governing Agreement. Requests are verified without undue delay; shorter applicable deadlines control. Return does not create an independent right to retain or reuse the information.

Restricted backup copies expire under the documented retention schedule and are not used for ordinary service. Applicable deletions and access restrictions are reapplied after restoration. Stricter deletion requirements control. On request, Helmsted provides completion information identifying remaining copies, their basis, and applicable expiry or release conditions.

Helmsted will certify completion upon request, accurately identifying any permitted retained copies and their basis.

6.3 Limited Exceptions

Retention exceptions are limited to the information and period required for their valid basis. Once that basis ends, the records are securely disposed of under applicable requirements. De-identification does not replace a required deletion or preservation obligation.

6.4 Clients and Professionals

Where available under separately accepted service terms, a Client Account may support multiple authorized professional relationships. Ending one relationship does not itself terminate another valid relationship. Helmsted may retain and supplement eligible Client Records only for authorized services or lawful preservation. These permissions do not promise uninterrupted access or a future feature. Firm Work Product, delivered-copy rights, and Restricted Feed Data remain governed by their applicable rights and source agreements.

Retention alone does not authorize ongoing refresh, transfer credentials, or grant another professional access. Access is limited to the relevant authorization, with any post-engagement compliance access restricted to its required purpose. Service availability and account closure follow the applicable service terms.

Clients may request closure and deletion directly from Helmsted. Helmsted verifies authority without undue delay and handles eligible records within the periods required by applicable law and accepted client terms, subject to lawful preservation and source restrictions.

7 Audit Rights and Compliance

7.1 Documentation

Helmsted will maintain records documenting its compliance with this DPA and will make such records available to Adviser upon reasonable written request, subject to appropriate confidentiality protections.

7.2 Security Summary

Helmsted will make relevant compliance documentation and available assurance reports accessible under appropriate confidentiality protections and reasonably cooperate with regulatory and vendor-oversight requests. Current audit status is stated separately.

Helmsted will provide its Security Overview on request and respond to reasonable security and due diligence questionnaires.

7.3 Regulatory Inquiries

If Helmsted receives a regulatory inquiry relating to Adviser Client Data, Helmsted will, to the extent permitted by law, promptly notify Adviser and cooperate reasonably in responding.

8 Representations and Warranties

Each party represents and warrants that it has the authority to enter into this DPA and will comply with all applicable laws governing its processing of Adviser Client Data.

Helmsted additionally represents and warrants that it will process Adviser Client Data only as permitted by this DPA, has implemented and will maintain the safeguards in section 3 including the required verified AI-provider arrangements, and will not use Adviser Client Data to train AI models.

9 Limitation of Liability

Each party's liability arising out of or related to this DPA is subject to the limitations of liability in the Agreement. Nothing in this DPA expands either party's liability beyond what is set forth in the Agreement. For clarity, under the Terms of Service incorporated into the Agreement, Helmsted's liability for claims arising out of an Incident or Helmsted's breach of this DPA is not subject to the general pilot-period cap and is instead capped at the available limits of the insurance described in the Terms of Service, currently two million dollars (\$2,000,000).

10 General Provisions

10.1 Conflicts

In the event of any conflict between this DPA and the Agreement regarding processing of Adviser Client Data or Helmsted's data security obligations, this DPA controls.

10.2 Amendments

Material amendments require at least 30 days' advance written notice to Adviser's compliance contact identifying the changes and effective date. Adviser may terminate before they take effect. Continued use

constitutes acceptance only where permitted; required separate consent remains necessary. New versions do not retroactively expand information rights. Incorporated versions are delivered with the executed Order and retained in the version history.

10.3 Governing Law

This DPA is governed by the laws of the State of Delaware, unless the Agreement specifies otherwise.

10.4 Not Legal Advice

This DPA is a commercial agreement. Nothing in it constitutes legal advice. Adviser is encouraged to have it reviewed by its own legal and compliance team prior to execution.

Helmsted, Inc.

Questions about this DPA or to request a signed copy? legal@helmsted.ai

Exhibit A: Subprocessors

The versioned list at helmsted.ai/security/subprocessors identifies Subprocessors, services, information accessed, and locations. The Exhibit A version delivered with the executed Order applies, subject to subsequent changes made under section 5.3.

AI providers and covered-service descriptions are identified in Exhibit A. Processing must satisfy section 3.3, including the required account and service settings.

Plaid Inc. is engaged for optional, client-initiated account aggregation in the client portal and accesses external account data only when a client chooses to connect an account. Adviser's use of Plaid-powered aggregation is subject to the Plaid End Client Terms at helmsted.ai/company/plaid.

Helmsted provides technology and informational tools, not investment or other professional advice. Professionals remain responsible for their services and review of professional materials.