DATA PROCESSING ADDENDUM ("DPA")

This Data Processing Addendum (“**DPA**”) forms part of the Master Subscription Agreement (“**MSA**”) and sets out the terms on which the Steward AI, Inc or its affiliates will process Personal Data on behalf of Customers.

Section	Description
1. Subject Matter & Duration	Processing of Personal Data as necessary to provide the Services and perform the Steward’s obligations under the MSA from the Effective Date until deletion or return of Personal Data in accordance with this DPA. “**Personal Data**” for the purposes of this Schedule, means information relating to an identified or identifiable natural person that is processed by Steward, where such information is Customer information.
2. Nature & Purpose of Processing	Automated identity verification, sanctions & PEP screening, adverse-media monitoring, transaction risk scoring, workflow management and audit-trail generation for AML/KYC compliance and fraud prevention.
3. Categories of Data Subjects	End-customers, beneficial owners, directors, authorised signatories and employees of the Customer; counterparties and other individuals whose data is required for AML/KYC checks.
4. Types of Personal Data	Identification data (name, date of birth, gender, nationality, national ID number), contact details (address, email, phone), government-issued documents (passport, driving licence), biometric identifiers (liveness/video selfie, facial geometry) where enabled, sanctions and watch-list data, adverse-media references, IP addresses, device fingerprints, transactional metadata, financial data, investment data, wealth and taxation information.
5. Special Category Data	Biometric data processed for the purpose of uniquely identifying a natural person, processed only with the Customer’s explicit instruction and subject to appropriate safeguards under UK GDPR / EU GDPR.
6. Processing Instructions	The Steward shall process Personal Data only on documented instructions from the Customer, including instructions provided via the Platform’s configuration settings and APIs.

7. Security Measures	Without prejudice to the Steward's general obligations, the Steward shall implement and maintain the following (non-exhaustive) technical and organisational measures: encryption of data in transit and at rest; strict access controls based on least privilege; multi-factor authentication; segregation of duties; ISO 27001; SOC Type II; annual penetration testing; regular vulnerability scans; 24×7 security monitoring and alerting; business continuity and disaster-recovery plans.
8. Sub-processors	The Steward maintains a current list of authorised sub-processors (including data-centre providers), which is listed at the end of this addendum. The Steward shall provide a mechanism to notify Customers of new sub-processors. Steward shall provide at least ten (10) days' notice of any intended addition or replacement of sub-processors and the Customer may object on reasonable, data-protection-related grounds. If the Customer does not subscribe to such notifications, Customer waives any right to receive prior notice of new sub-processors.
9. Audit & Inspection Rights	On written request no more than once per year, Steward shall provide a copy of its most recent independent SOC 2 Type II or ISO 27001 certification report. Where such report is not sufficient, the Customer may, at its own cost and subject to reasonable confidentiality and security measures, conduct an on-site audit or appoint an independent auditor; provided that (i) the Customer gives at least thirty (30) days' notice, (ii) audits are limited to once per year and (iii) the audit does not unreasonably disrupt Steward's business.
10. Data Subject Rights	Taking into account the nature of the processing, Steward shall implement appropriate measures to assist the Customer in responding to data-subject requests (access, rectification, deletion, objection, restriction, portability) through self-service features or, where such features are not available, via support tickets.
11. International Transfers	Steward shall not transfer Personal Data outside the United States, the European Economic Area, the United Kingdom, or Switzerland unless it has ensured a valid transfer mechanism and shall, on request, provide evidence of such mechanism.

12. Deletion & Return	Within thirty (30) days of termination or expiry of the MSA, Steward shall, at the Customer's choice, return all Customer Data and securely delete all copies except for (a) archived back-ups maintained for disaster-recovery purposes (automatically overwritten within ninety (90) days) and (b) logs retained to the extent required by applicable law.
13. Liability	The parties' respective liabilities arising under this DPA are subject to the limitations and exclusions set out in Clause 9 of the MSA.

Sub-processors

Name	**Service Provided**	**Location**
AWS	Cloud service provider	US and EU
OpenAI	AI model provider for text analysis and automation	US and EU
MongoDB	Managed database hosting and storage	US and EU
Entrust (Onfido)	Identity verification and document authentication	US and EU
ComplyAdvantage	Screening (PEP, Sanction, Adverse Media) data vendor	US and EU
Kyckr	Corporate registry and company verification data	US and EU
Datadog	Monitoring, logging, and application performance management	US and EU
Auth0	Authentication and user identity management	US and EU
Slack	Internal communications and collaboration	US and EU
Google Workspace	Document, Worksheet and Drive storage services	US and EU
Pipedrive	CRM services on customer data	US and EU