



UMAY ANA

DATA PROCESSING ADDENDUM

Enterprise Data Protection Framework

Version 1.0 | September 2026

ENTERPRISE / CONTRACTUAL DOCUMENT

Enterprise AI & Agricultural Intelligence Services

Banks • Insurers • Reinsurers • Public Institutions • Agribusiness

Important drafting note. This DPA is designed to accompany the Umay Ana Master Services Agreement. It intentionally avoids assuming a specific governing jurisdiction where the Order Form should control.

1. Purpose and Scope

This Data Processing Addendum ("DPA") governs the Processing of Personal Data by Aybil Agricultural Technologies, operating the Umay Ana platform ("Provider"), on behalf of an enterprise customer ("Customer") in connection with the Services. The DPA applies only to Processing performed for the Customer under the applicable agreement and does not replace privacy obligations arising from Umay Ana's direct relationship with end users where Provider acts as an independent controller.

2. Definitions and Roles

Term	Meaning
Applicable Data Protection Law	Privacy and data protection law applicable to the relevant Processing, including the GDPR where applicable.
Customer Personal Data	Personal Data submitted to, generated for, or otherwise Processed by Provider on Customer's behalf under the Services.
Controller / Processor	The roles assigned by Applicable Data Protection Law. Customer is generally Controller and Provider generally Processor for Customer Personal Data unless the parties document another allocation.
Subprocessor	A third party engaged by Provider to Process Customer Personal Data in support of the Services.
Security Incident	A confirmed breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to Customer Personal Data.

3. Processing Instructions

- Provider will Process Customer Personal Data only on documented instructions from Customer, including the MSA, Order Form, Statement of Work, this DPA, and authorized use of the Services.
- Provider may Process data as required by law, provided it informs Customer unless legally prohibited.
- Provider will not sell Customer Personal Data or use it for unrelated advertising.
- If Provider believes an instruction violates Applicable Data Protection Law, it may suspend the affected Processing and request clarification.

4. Processing Details

Category	Typical scope
Subjects	Customer personnel, participating farmers/producers, authorized users, and other persons whose data Customer lawfully provides.
Data	Identifiers or pseudonymous references, contact data where configured, farm/geographic context, crop/livestock data, device/request metadata, uploaded images, usage events, and institutional workflow metadata.
Purpose	Provide agricultural AI services, dashboards, APIs/exports, support, security, auditability, and Customer-requested analytics.
Duration	For the term of the Services plus limited retention needed for security, legal, backup, and deletion workflows.
Special categories	Not intentionally required as a default service input. Customer must not provide special-category data unless expressly agreed and legally permitted.

5. Confidentiality and Personnel

Provider will limit access to Customer Personal Data to personnel and contractors who need access to perform the Services and who are bound by confidentiality obligations. Access will be governed through role-appropriate controls and reviewed in proportion to operational risk.

6. Security Measures

Provider will implement appropriate technical and organizational measures designed to protect Customer Personal Data, taking into account the nature of Processing, available technology, implementation cost, and risk. The current enterprise security posture is described in the Security & Trust Overview and may be supplemented by an Order Form or security schedule.

- Encryption in transit using modern transport security for production interfaces.
- Authentication and authorization controls for administrative and institutional access.
- Logical separation of Customer data and environment-level access controls where applicable.
- Logging, monitoring, backup, vulnerability management, and incident-response processes proportionate to the Services.
- Data minimization and purpose-limited institutional API scopes.

7. Subprocessors

Customer authorizes Provider to use Subprocessors necessary to deliver the Services. Provider will remain responsible for Subprocessor performance to the extent required by the agreement and will impose data protection obligations materially consistent with this DPA. Upon enterprise request, Provider will make available a current Subprocessor list or provide a contractual notification mechanism for material changes.

8. International Transfers

Where Customer Personal Data is transferred internationally and a transfer mechanism is required by Applicable Data Protection Law, the parties will implement an appropriate mechanism, such as the European Commission Standard Contractual Clauses, the UK International Data Transfer Addendum, or another legally recognized mechanism, as applicable. Transfer-specific modules, annexes, and supplementary measures may be incorporated by reference.

9. Data Subject Requests

Taking into account the nature of Processing, Provider will provide reasonable assistance to Customer with requests to exercise data protection rights where Customer cannot fulfill the request through available functionality. Provider may direct a requester to Customer when Customer is the responsible Controller.

10. Security Incident Response

Provider will notify Customer without undue delay after confirming a Security Incident affecting Customer Personal Data and will provide available information reasonably necessary for Customer to meet applicable notification obligations. Notification is not an admission of fault or liability. Provider will take reasonable steps to contain, investigate, and remediate the incident.

11. Assessments, Audits and Compliance Information

Provider will make available information reasonably necessary to demonstrate compliance with this DPA. Any audit will be subject to reasonable confidentiality, scope, frequency, timing, and security constraints. The parties should prefer existing documentation, questionnaires, independent reports when available, and remote evidence review before on-site inspection.

12. Deletion and Return

Upon termination or expiration, Provider will delete or return Customer Personal Data in accordance with the applicable agreement, subject to technically necessary backup cycles and legal retention obligations. Data retained solely in backups will remain protected and will not be restored for ordinary business use except as required for continuity or recovery.

13. Aggregated and De-identified Information

Nothing in this DPA prevents Provider from using information that has been aggregated or de-identified so that it is not Personal Data under Applicable Data Protection Law, including to improve service quality, measure reliability, develop agricultural taxonomies, evaluate model behavior, create statistical benchmarks, and improve risk analytics. Provider will not attempt to re-identify such information except to validate de-identification or as legally permitted.

14. Controller-to-Controller Processing

Where Provider independently determines the purpose and means of Processing - for example, account administration, fraud prevention, security logging, billing, or direct end-user services - Provider may act as an

independent Controller. Such Processing is governed by Provider's applicable privacy notices and law, not by Customer instructions under this DPA.

Acceptance and Relationship to the MSA

This document forms part of the Umay Ana enterprise contracting framework when incorporated by reference into a Master Services Agreement, Order Form, Statement of Work, or other written agreement executed by the parties. If there is a conflict, the order of precedence stated in the applicable agreement or Order Form will apply.

This template is intended to support commercial contracting and enterprise readiness. It should be reviewed by qualified counsel for the governing jurisdiction, the customer's regulatory status, data flows, and negotiated risk allocation before signature or public reliance.