01 / MASTER ENGAGEMENT

Professional Services Agreement + SOW

OMEGANEON Public Sample v1.6 | Based on Common Paper PSA Standard Terms v1.1

PUBLIC CONTRACT SAMPLE — FOR LEGAL REVIEW — NOT AN EXECUTED AGREEMENT

01 Parties & Key Terms

Provider	Omeganeon LLC, a Washington limited liability company, USA. Contract notices: hastersun@zohomail.com.
Customer	[CUSTOMER LEGAL NAME], [STATE / COUNTRY OF FORMATION]. Notice address: [CUSTOMER EMAIL OR POSTAL ADDRESS].
Effective Date	Date of the last signature on the Integrated Cover Page / this PSA Cover Page.
Governing Law	State of Washington, United States.
Chosen Courts	State and federal courts located in King County, Washington.
General Cap Amount	1× the fees paid or payable by Customer under the applicable SOW in the twelve (12) months immediately preceding the claim. This is the parties' aggregate General Cap for the relevant SOW, subject to mandatory legal/DPA/SCC exceptions. Express clarification regarding IP warranties and indemnity defense costs appears below.
Increased Cap	No Increased Claims / separate supercap selected; statutory limitations and DPA/SCC exceptions are not waived.
Covered Claims	**Provider Covered Claims: Third-party claims alleging that Provider-Authored Components of a Custom Deliverable expressly identified in the SOW, as supplied by Provider and used by Customer as authorized, infringe a third party's copyright or misappropriate its trade secrets. Exclude claims to the extent caused by Customer Materials/Input, Customer-procured Third-Party Materials, unauthorized alteration, use outside the SOW or combinations with items not supplied/authorized by Provider that cause the claim. Customer Covered Claims: Third-party claims alleging that Customer Materials, Customer Input or Customer-procured Third-Party Materials supplied for and used as authorized in the Services infringe a third party's copyright or misappropriate its trade secrets. Each party's indemnification is limited to these identified Covered Claims and PSA Standard Terms §9, as clarified by the §8.1/§9 amendment on this Cover Page. No blanket standalone AI Output indemnity is offered. The separate limited IP warranty under amended PSA §6.3(b) applies only to defined Provider-Authored Components.**
Unlimited Claims	**No additional contractual Unlimited Claims or Increased Claims are elected. The parties do not waive or cap any liability that Applicable Law does not permit them to limit, including non-waivable data-subject rights and mandatory EEA/UK transfer-clause obligations where applicable. The agreed 1× General Cap is not a blanket guarantee against liability, and courts may decline to enforce a limitation in particular circumstances.**
Additional Warranties	None beyond the Common Paper PSA Standard Terms §6.
Insurance Minimums	None specified; no representation of current insurance coverage.
Publicity	No use of Customer name, logo, trademarks, testimonial or identifiable public case study without Customer prior written approval.

02 Agreed Changes to PSA Standard Terms

Each change below is intended as an express amendment to the identified Standard Terms section, not an undisclosed replacement of Common Paper text.

§1.5 Subcontractors	Customer pre-approves only the service subcontractors affirmatively named in the SOW Subcontractor Schedule. Any additional or replacement service subcontractor requires Customer prior written approval; Provider remains responsible under §1.5. Data subprocessors are separately governed by the DPA.
§2.1 + §2.3 IP	Time of Assignment for specifically commissioned customer Deliverables is upon payment in full of the Fees attributable to them. Pre-Existing Materials, including EDGEPORT, reusable code, methods, templates, platform components and generally applicable tools, remain Provider-owned. Customer receives the limited license described in PSA §2.3 to use such materials with the paid Deliverables. The warranty in §6.3(b) is separately limited as stated below, and Customer owns standalone AI Output as coordinated in AI Schedule C.
§2.4 Third Party	Provider may use Third-Party Materials only where expressly authorized in writing, with procurement and license responsibility identified in the SOW. No third-party IP assignment is promised.
§2.5 Data Use	Regardless of any broad permission in §2.5, Provider will not use Customer Input, AI Output, Customer Materials, Customer Personal Data, Customer Confidential Information, or non-public client Feedback to train models or improve generally available products. Operational telemetry may be processed only as needed for agreed service operation, security, billing, troubleshooting and legal obligations, subject to the DPA and AI Addendum. No unrestricted reuse of customer-derived Usage Data is granted.
§6.3(b) IP Warranty	Express amendment to Common Paper PSA Standard Terms §6.3(b): Provider warrants that the Provider-Authored Components of each Custom Deliverable expressly identified in the applicable SOW, when supplied by Provider and used by Customer without unauthorized alteration and in accordance with the SOW, do not infringe a third party's copyright or misappropriate its trade secrets. “Provider-Authored Components” means the software, configurations, documentation or other portions of a specifically commissioned Deliverable created by Provider for that SOW; they exclude Customer Materials and Customer Input; Customer-procured Third-Party Materials; separately licensed Third-Party Materials; standalone AI Output that is not expressly designated as a commissioned Deliverable; and Customer/third-party changes not authorized in writing by Provider. This limited warranty does not apply to the extent an alleged infringement results from unauthorized modification, use outside the agreed scope, or a combination with materials/systems not supplied or authorized by Provider that caused the infringement. Provider remains responsible for the licenses and permissions it is required to obtain for Provider-procured Third-Party Materials under PSA §2.4(b), and the distinct rights-to-perform/transfer warranty in PSA §6.3(d) is preserved. No comprehensive non-infringement warranty is given for standalone AI-generated Output.
§8.1 + §9 Cap / Indemnity	For clarity, the aggregate General Cap Amount of 1× the fees paid or payable under the applicable SOW during the twelve (12) months immediately preceding the claim applies, to the maximum extent allowed by law, to claims for breach of the limited warranty under amended PSA §6.3(b) and the defined third-party Provider/Customer Covered Claims under PSA §9. Amounts paid by an Indemnifying Party in defense costs, reasonable attorneys' fees, settlements and awards count toward, and do not independently increase, that same aggregate General Cap. No new Increased Claims or contractual Unlimited Claims are elected. Nothing limits non-waivable liability, rights of data subjects, or liabilities under applicable EEA SCCs / UK Addendum that cannot contractually be limited. The separate warranty in PSA §6.3(d), the performance warranty in §6.3(a)/(c), and the limited remedies stated in PSA §6.4 remain subject to their own express terms

	and applicable law. The §9 indemnity is limited to the expressly described Covered Claims; it does not extend to standalone AI Output by implication.
§4 Fees	Setup Fee: 35% of agreed final discounted Setup Fee must be received before Project Kickoff; remaining 65% invoiced upon actual or deemed acceptance, due 30 days after Customer receives the invoice. Monthly Managed Fees are prepaid, with invoices issued early enough for payment before the covered service period; the standard invoice payment period is Net 30. Refunds upon early termination are limited to documented earned startup fees, with unearned prepayments treated under PSA §5.3 and applicable law. Hosted Cloud infrastructure and AI API usage are included in the Monthly Managed Fee as expressly described in the separate Hosted/BYOC cost-inclusion provision below.
§4 Hosted Cloud / BYOC Fees	Default deployment is OMEGANEON-Hosted Cloud. The Monthly Managed Fee is an all-inclusive, fixed monthly charge for the cloud infrastructure (including applicable compute, storage, network and hosting services), AI model/API calls, routine workflow operations and maintenance necessary to deliver the agreed Services within the Scope and Usage Profile stated in the SOW. Provider obtains and pays its hosted cloud and model/API vendor invoices. There is no separate hosted-cloud fee, token-based charge, per-call AI API charge, automatic usage overage or third-party pass-through for those included items. Included usage is defined by the agreed workflows and service profile; it is not an unlimited commitment to materially expanded services. Any proposed scope, architecture or volume change and prospective price adjustment requires a written Change Order agreed before new fees accrue. Customer remains responsible only for any separately authorized third-party business-system licenses or extras expressly itemized in the SOW. BYOC is optional and applies only when expressly selected; Customer pays its own cloud provider directly, and any BYOC add-on fees and model/API credential or billing arrangements must be separately stated in the SOW.
Late Payment	**Only for undisputed sums remaining unpaid for ten (10) calendar days after the due date, Provider may deliver written notice specifying the overdue amount and a further five (5) Business-Day cure period beginning upon confirmed delivery of that notice. If the amount is still unpaid after the cure period, Provider may suspend only the affected non-critical Managed Services, to the minimum reasonably necessary. Provider must not delete, withhold or corrupt Customer data, revoke Customer control of Customer-Owned Cloud resources, or disable agreed essential security/data-export safeguards. Upon receipt of undisputed overdue sums, Provider will restore suspended services within two (2) Business Days where technically available. A good-faith disputed amount handled under PSA §4.4 is not grounds for suspension. The initial 35% Setup payment remains a pre-Kickoff condition; service need not commence before receipt.**
§12.7 Publicity	No public customer identification or identifiable case study without advance written approval; this also applies to generated customer content or security/operations references.

03 Order of Precedence and Execution

For mandatory data-transfer matters, the applicable EEA Standard Contractual Clauses or UK Addendum prevail to the extent required by law. The DPA controls Personal Data processing; the AI Addendum controls AI Services where consistent with the DPA. The PSA Cover Page and PSA Standard Terms control general legal terms. The SOW controls customer-specific services, scope, deliverables, fees, project dates, and authorized deviations that expressly identify amended sections. A general SOW statement does not silently override Personal Data, AI, security, indemnity or liability provisions. This is an express qualification of the default SOW-controls clause, applicable when agreed in the executed customer agreement.

For a first engagement, the parties may sign a single Integrated Cover Page that expressly incorporates the completed PSA Cover, SOW, DPA Cover, AI Addendum Cover and applicable Security Schedule D, each identified by version and attachment. The separate

pre-sales Mutual NDA is not automatically incorporated. If the parties do not use the completed integrated signing structure, execute each applicable cover separately.

04 Statement of Work (SOW) — customer variables

SOW ID / Project	[SOW ID] / [PROJECT NAME]
Services	[DESCRIBE SETUP IMPLEMENTATION, SYSTEMS, CONNECTORS, WORKFLOW SCOPE, MANAGED OPERATIONS, EXCLUSIONS]
Deployment Model	OMEGANEON-HOSTED CLOUD (DEFAULT) unless BYOC ADD-ON is expressly selected and priced in this SOW. Selected hosting platform: [AWS / AZURE / GCP]; deployment region(s): [REGION(S)]; tenant/isolation design: [ACTUAL ARCHITECTURE]. Hosted environments and service-side model/API credentials are operated by OMEGANEON; Customer still authorizes connections to its business systems. If BYOC: Customer-owned cloud account [PROVIDER/ACCOUNT], access delegation [SCOPE], cloud provider billed directly to Customer; model/API credential ownership and billing [OMEGANEON-INCLUDED / CUSTOMER-DIRECT] must be specified.
Deliverables	[ITEMIZE ACCEPTANCE-TESTABLE DELIVERABLES AND SPECIFICATIONS; in-progress drafts excluded unless expressly listed]
Scope and Usage Profile	[WORKFLOW(S), EXPECTED USAGE/VOLUME, TRIGGER FREQUENCY, NUMBER OF SYSTEM CONNECTIONS, MODEL/API FUNCTION(S), APPROVED BUSINESS ACTIONS AND MATERIAL EXCLUSIONS]. These agreed service parameters determine what is included in the flat Monthly Managed Fee. They are not per-token billing rates. Material expansion requires a pre-approved Change Order; no unapproved or retrospective overage invoices.
Complexity	Complexity is assessed individually for each proposed SOW; there are no fixed numerical system/connector thresholds. Before signature, parties identify either STANDARD or HIGH COMPLEXITY in writing based on scope, integrations, data, risk, customer dependencies and feasibility; any unresolved assessment is treated as HIGH for scheduling until written agreement. The classification alone does not replace SOW specifications.
Kickoff Trigger	The later of (i) signing; (ii) receipt of 35% Setup payment; (iii) Customer providing required information, access and written approvals; and (iv) mutually documented Kickoff confirmation.
Delivery Timeline	If this SOW expressly designates STANDARD Complexity, Provider will submit the agreed implementation Deliverables within seven (7) Business Days after the documented Kickoff Trigger and applicable security prerequisites are satisfied. For HIGH Complexity, enter customer-specific delivery milestones and dates: [DATES / MILESTONES]. Submission, Acceptance and Go-Live are separate events. If baseline security cannot be verified by proposed Go-Live, production personal-data processing must not commence; parties will document remediation and any schedule change under a Change Order.
Delay Adjustment	Reasonable extensions for documented Customer-caused delays, approved Change Orders or external dependencies beyond reasonable Provider control; promptly notify Customer in writing of cause and revised schedule. Scope/fee changes require written Change Order.
Acceptance	Rejection Period: 15 Business Days after each submitted Deliverable. Rejections must describe nonconformity in writing. Resubmission Period: 5 Business Days after a valid rejection notice. No qualifying rejection by the deadline means deemed acceptance under PSA §1.4.
Go-Live / Managed	Go-Live event: [TRIGGER / TARGET DATE]. Managed Operations begin: [TRIGGER / DATE]. Not automatically the same as delivery or acceptance.

Term / Renewal	SOW start [DATE/TRIGGER]; initial duration [TERM]; automatic renewal [YES/NO]; renewal term [TERM]; termination notice [PERIOD]; any convenience termination right [IF APPLICABLE].
Customer Obligations	Client contact [NAME/ROLE]; supply lawful access and necessary licenses, approvals, accurate data and system permissions. Special dependencies: [DESCRIBE].
Subcontractors	Pre-approved service subcontractors: [NAME / ROLE / NONE]. Data subprocessors are separately listed in DPA Schedule.
Third-Party Materials	Provider-procured [LIST/NONE]; Customer-procured [LIST/NONE]; customer written authorization [HOW/DATE].

05 Fees & Incentives

Fee component	List price	Discount	Agreed amount
Setup / Implementation	[$ AMOUNT]	[25% / 10% / 0%]	[$ AMOUNT]
Managed Operations — All-Inclusive Hosted	[$ / MONTH]	[15% if annual prepaid / 0%]	[$ / MONTH OR ANNUAL TOTAL]
BYOC Add-on / separately approved extras	[ONLY IF SPECIFICALLY INCLUDED]	[IF ANY]	[$ AGREED; OTHERWISE NONE]

Proposal Date	[DATE]; discount trigger measured from formal Proposal issuance. Execute within calendar days 1–7: Setup −25%; days 8–14: Setup −10%; thereafter 0%. Proposal expiry and calculation to be confirmed in final SOW.
Stacking	Setup discount may stack with 15% discount on annual prepaid Managed Fees, applied to different fee components, subject to pre-approved commercial terms and actual SOW amounts.
Setup Invoices	35% of final discounted Setup amount due and received before Kickoff; remaining 65% invoiced at Acceptance, Net 30 from receipt.
Managed Invoice	Hosted Cloud monthly charge covers agreed cloud hosting and AI model/API consumption plus workflow operations, maintenance and monitoring. No separate fee for cloud hosting or AI API usage; no token, request or automatic overage line items. Customer-approved extras outside this scope require a written Change Order. BYOC Add-on, if selected, has explicit Setup/Managed service charges, while Customer pays its own cloud vendor directly. Monthly Managed Fee remains prepaid; standard invoice payment terms are Net 30.
Early Termination	Initial 35% is an advance against startup services actually performed, not an unconditional forfeiture. Earned documented fees retained; unearned prepayments handled under PSA §5.3 and law. Setup work allocation: [LIST STARTUP ACTIVITIES OR RATE/MILESTONE BASIS].

SCHEDULE B — Data Processing Agreement (DPA) Cover Page

Once completed and executed or expressly incorporated by the parties, this DPA Cover Page supplements the PSA and incorporates Common Paper DPA Standard Terms v1.1 available at https://commonpaper.com/standards/data-processing-agreement/1.1/.

Underlying Agreement	OMEGANEON Professional Services Agreement and SOW between Omeganeon LLC and [CUSTOMER], effective [EFFECTIVE DATE].
Provider / Contact	Omeganeon LLC, Washington, USA. Security and privacy contact: support@omeganeonhq.com. Physical address for transfers: [COMPLETE IF REQUIRED].
Customer role	[CONTROLLER / PROCESSOR] based on actual processing chain. OMEGANEON acts as Processor or Subprocessor as applicable. Hosted Cloud is the default hosting configuration, but cloud account ownership by itself does not determine privacy-law roles.
Approved Subprocessors	Only expressly approved vendors in the completed customer-specific table process Customer Personal Data. For Hosted Cloud, include the selected infrastructure/cloud provider and model/API vendor(s), processing regions and tasks. BYOC vendors and processing purposes remain customer-specific. No vendor is approved by default.
Security Policy	For any production engagement, Provider shall implement, test and document all applicable security controls identified in the completed Security Schedule before Production Go-Live and before processing Customer Personal Data in production. Production processing must remain disabled until that verification is complete. Any remediation and related schedule changes shall be documented with Customer. This public sample does not represent that controls have already been deployed or independently audited; no SOC 2 or ISO 27001 certification is claimed.
Service Provider Relationship	CCPA service-provider terms apply only if parties and processing meet the statutory requirements; applicability to be confirmed against actual use. Provider will not sell or share Customer Personal Data contrary to applicable requirements.
DPA Liability	The agreed PSA General Cap of 1× the fees paid or payable under the applicable SOW in the twelve (12) months preceding the claim applies between the parties to the extent enforceable. PSA §8 and the express Cover Page clarification address the limited §6.3(b) warranty and §9 Covered Claims, including counted defense costs. The DPA does not create standalone AI Output IP indemnity, nor waive data-subject rights, mandatory SCC/UK Addendum liabilities, or other non-waivable obligations. No separate DPA supercap was elected.
Restricted Transfers	**[COMPLETE FOR APPLICABLE PROJECT: data subject regions, actual hosting/support locations, EEA/UK/Swiss transfers, SCC module and governing state, UK addendum and relevant assessments]. Do not assume US-only.**

Approved Subprocessor	Country / hosting regions	Anticipated processing
[VENDOR LEGAL NAME]	[COUNTRY / REGION]	[FUNCTION; TYPES OF PERSONAL DATA]
[VENDOR LEGAL NAME OR NONE]	[COUNTRY / REGION]	[FUNCTION]

Subprocessor change procedure (express clarification to Standard Terms §2.6(a)): Provide advance written notice no less than 10 Business Days before any intended addition/replacement; Customer retains 30 calendar days after notice to object. The new Subprocessor must not receive Customer Personal Data before the 30-day objection period ends without objection or Customer provides earlier written approval. Objections are addressed in good faith. Any mandatory stricter statutory rule prevails.

Annex I(A) Parties & Roles

Data Exporter	[CUSTOMER LEGAL NAME]; address [PHYSICAL ADDRESS]; representative [NAME/TITLE]; role [CONTROLLER / PROCESSOR].
Data Importer	Omeganeon LLC; [PHYSICAL ADDRESS IF RELEVANT]; privacy contact support@omeganeonhq.com; role Processor / Subprocessor depending on customer role.

Annex I(B) Processing Profile

Service	AI Workflow Implementation and Managed Operations under the SOW. DEFAULT: OMEGANEON-Hosted Cloud deployed into the Provider-managed cloud account on [AWS/AZURE/GCP] in [REGION(S)]. OPTIONAL: Customer-Owned Cloud (BYOC) Add-on only if elected in the SOW, with Customer-owned cloud account and OMEGANEON-managed limited operations. Actual hosting providers, regions, model/API services and authorized data-processing chain must be listed in the Approved Subprocessor Schedule and relevant transfer annexes.
Data Subjects	Customer employees and authorized business contacts; Customer customers / end users only to the extent their records are part of the approved SOW.
Personal Data	Business names, contact details, employee and business contact information, relevant CRM / onboarding / support and business transaction records. [CONFIRM CLIENT-SPECIFIC DATASET AND SENSITIVE FIELDS IN SOW].
Excluded by default	Special-category data, health records, bank account data, and comparable high-risk personal information are outside standard scope absent separately signed data-processing safeguards, a revised SOW and legal assessment.
Nature / Purpose	Authorized system integration and syncing, Customer-controlled internal analysis/classification, AI workflow processing, narrowly approved automated business actions, service and governance logs. No default human access by OMEGANEON engineers to raw customer business records, but automated processing/privileged system maintenance may still trigger processor obligations.
Frequency	[CONTINUOUS / EVENT-TRIGGERED / SCHEDULED] consistent with the SOW.
Duration / Deletion	Customer controls its retention instructions and any customer-facing deletion settings supported by the selected deployment. In the DEFAULT Hosted Cloud arrangement, OMEGANEON implements contractual deletion, return and backup retention procedures and provides agreed customer administration or technical assistance. In BYOC, Customer manages its cloud account and configurable retention while OMEGANEON provides contracted technical assistance. DPA §7 governs termination/deletion requests; legal retention and secure-backup exceptions apply only as provided in the DPA and law. This is separate from the three-year DPA compliance-evidence retention requirement.

Annex I(C) / Transfers

If EEA/UK restricted transfers apply, the parties must complete the relevant SCC/UK Addendum annex fields, governing member state and transfer assessment before such transfer. [DATA TRANSFER APPLICABILITY AND DETAILS REQUIRED IF TRIGGERED].

Annex II Technical & Organizational Measures

The required pre-production security baseline consists of APB (System, Data, Action, Limit, Duration, Identity), least privilege, HITL, encryption in transit/at rest, audit logging, MFA, backup/restore, and controlled deletion. Only measures evidenced as fully operational for this engagement become representations of implementation; written verification must be complete before production data processing.

Specific Overrides to DPA Standard Terms

§5.2 Security Reports	Replace §5.2 in its entirety: "Provider does not represent that it undergoes independent third-party security audits or possesses a SOC 2 or ISO certification. On reasonable confidential written request, Provider will make available only documentation and security information that actually exists and may lawfully be shared."
§5.3 Due Diligence	In §5.3, replace "In addition to the Report" with "In lieu of an independent third-party Report when none exists". The remainder of §5.3 is subject to the actual measures and the DPA.
§5.1 Records	**Provider shall maintain records demonstrating DPA compliance for three (3) years after termination of the DPA in accordance with Common Paper DPA §5.1. Restricted-access recordkeeping and retention procedures must be operational before Production Go-Live. This provision concerns compliance evidence; it does not require retention of Customer raw business data for three years.**
§4 Security Incident	Common Paper DPA Standard Terms §4 applies: Provider shall notify Customer without undue delay and no later than seventy-two (72) hours after becoming aware of a Security Incident. Incident monitoring, escalation and notification processes shall be implemented and verified before Production Go-Live.
§8–9 Liability & Priority	Retain mandatory statutory exceptions and SCC/UK Addendum primacy. Other DPA liabilities reference PSA caps where applicable.

SCHEDULE C — AI Addendum Cover Page

Adapts the Common Paper AI Addendum Standard Terms v1.0 (https://commonpaper.com/standards/ai-addendum/1.0/) from their CSA/software-license baseline to an OMEGANEON professional-services engagement. The express Cover Page adaptations are identified for review and apply if accepted in the executed agreement.

Underlying Agreement	OMEGANEON Professional Services Agreement + applicable SOW, effective [DATE], between Omeganeon LLC and [CUSTOMER].
AI Services / Product	For Common Paper AI Addendum §1.1 and §4.2, "Product" means only the AI-enabled Services, agreed workflows and managed operations in the SOW, whether default OMEGANEON-Hosted Cloud or optional BYOC; this does not create a general software-product license.
AI API Cost & Deployment	The default AI-enabled Services run in OMEGANEON-Hosted Cloud infrastructure and use OMEGANEON-provisioned commercial model/API services for the agreed SOW scope. Those model/API usage costs are included in the Monthly Managed Fee; no separate token or request charge or automatic pass-through applies. Model provider(s), processing regions, and applicable subprocessor approvals must be documented for each engagement. BYOC or Customer-provided API keys/credentials apply only if the SOW expressly selects and allocates them. Any material expansion of AI usage outside the SOW requires a prospective written Change Order, not retroactive usage billing.

Training Data	None by default. Neither OMEGANEON nor its authorized model vendors may train a model using Customer Input, Output or Customer Content except after a separate, advance written amendment that names model/vendor, data categories, purposes, retention and safeguards.
Training Purposes	None by default. An explicit written later authorization is required; silence, a general contract signature or routine service use is not consent to model training.
Improvement Restrictions	Notwithstanding Standard Terms §1.4, Customer Input, Output, Feedback, Confidential Information and Customer Materials may not be used for generalized non-training product improvement or cross-client reuse. Use only for the contracted Services, required security operations and legal compliance consistent with the DPA. PSA §2.5 is narrowed accordingly.
Output / Deliverables	Express modification of AI Addendum Standard Terms §2.1 solely to coordinate with PSA §2.1: As between the parties, Customer retains its Input rights and owns any legally protectable/assignable standalone operational AI Output produced by the authorized workflows upon generation, to the extent such rights exist. If AI-assisted content is incorporated into a specifically commissioned Custom Deliverable expressly identified in the SOW, the ownership/assignment of the Provider-created Deliverable portions transfers upon full payment of their associated Fees under PSA §2.1. No rights in EDGEPORT, Provider Pre-Existing Materials, third-party models or licensed Third-Party Materials are transferred; relevant licenses remain governed by the PSA/SOW. Ownership of Output does not constitute a promise that AI-generated content is copyrightable or exclusive.
Agent Permissions	AI actions must comply with the completed Security Schedule, including the six APB permission dimensions (System, Data, Action, Limit, Duration and Identity), risk-tiered HITL approvals, least privilege, MFA, encryption, audit logging, backup and deletion requirements. Provider shall implement and verify the applicable controls before Production Go-Live. This sample does not assert current deployment or certification.
Audit / Records	The production service shall retain relevant AI actions, permissions, approvals and execution records for ninety (90) days by default, subject to Customer-configured retention in the SOW or Security Schedule and applicable law. Customer visibility and OMEGANEON access are governed by the completed Security Schedule. The retention system must be verified before Production Go-Live.
AI Acceptable Use Policy	**OMEGANEON AI Acceptable Use Policy, Version 1.4 (issued November 19, 2026), is incorporated only when expressly attached to, or identified in, the executed agreement. Website reference, if used: [AUP PUBLIC URL]. The restrictions in Common Paper AI Addendum Standard Terms §1.2 also apply. Material amendments follow the PSA change process.**
Model Vendors	Only the cloud and AI model/API providers identified and approved for the engagement may process Customer Personal Data in accordance with the DPA Subprocessor Schedule. List each applicable provider legal name, processing region and function in the completed DPA. BYOC and customer-owned credentials, if elected, are identified in the SOW. The agreed AUP is OMEGANEON AI Acceptable Use Policy Version 1.4, attached to the final contract package or available at [AUP PUBLIC URL].

AI Covered Claims	**Common Paper AI Addendum §§3.1–3.2 (AI limitations and similarity of Output) continue to apply to standalone or automatically generated operational AI Output. They do not negate the expressly limited warranty for Provider-Authored Components of expressly commissioned Custom Deliverables under amended PSA §6.3(b), or Provider's third-party licensing duties under PSA §2.4(b). No general warranty or blanket indemnification is offered for standalone AI Output. The sole contractual third-party IP indemnities are the narrowly defined Provider and Customer Covered Claims in the PSA Cover Page, handled under PSA §9, subject to the aggregate 1× General Cap where enforceable, with the DPA, mandatory EEA/UK transfer obligations, data-subject rights and other non-waivable law preserved.**

A more specific data-protection requirement under the DPA or legally applicable SCCs overrides AI provisions. The AI Addendum controls AI subject matter otherwise; it does not override the SOW commercial scope by implication. Both parties are deemed to adopt this Cover Page only through the expressly identified integrated signature, if the integrated execution page expressly identifies and incorporates this completed Cover Page.

SCHEDULE D — Security Measures & Approval Register

For any production engagement, Provider shall implement, test and document all applicable security controls identified in the completed Security Schedule before Production Go-Live and before processing Customer Personal Data in production. Production processing must remain disabled until that verification is complete. Any remediation and related schedule changes shall be documented with Customer. This public sample does not represent that controls have already been deployed or independently audited; no SOC 2 or ISO 27001 certification is claimed.

Measure	Required control / verification criteria	Go-Live verification
APB — System/Data/Action/Limit/Duration/Identity	[Permission enforcement location, rules, audit evidence]	[EVIDENCE / DATE]
Human approval (HITL)	[Which high-risk actions need named approver]	[EVIDENCE / DATE]
Minimum privileges / MFA	[Identity provider, provider access, scopes, revocation]	[EVIDENCE / DATE]
Transport and at-rest encryption	[Cloud/KMS owner, TLS, encryption design]	[EVIDENCE / DATE]
Governance & activity logging	Audit events, retention configuration, Customer visibility and access controls; [VERIFICATION RECORD].	[EVIDENCE / DATE]
Backup, recovery and deletion	[Provider-managed hosted cloud or optional Customer-owned BYOC, according to SOW; test backups, restore, deletion, recovery objectives and account responsibilities]	[EVIDENCE / DATE]
Subprocessor/vendor access	[Named approved vendors and region constraints]	[EVIDENCE / DATE]

Measure	Required control / verification criteria	Go-Live verification
Incident handling	Incident response contact, escalation, time-of-awareness capture and notification workflow; [VERIFICATION RECORD].	[EVIDENCE / DATE]
PRODUCTION GO-LIVE GATE	Full baseline must be deployed and evidence recorded before any production Customer Personal Data is processed; otherwise hold processing and agree remediation	Production use requires sign-off

Security requirements are set by the completed Security Schedule and must be verified before Production Go-Live. The public sample makes no claim of existing independent security audits, certifications or completed controls.

Execution — one signature per party

By signing below, each party intends to accept: (i) the PSA Cover Page, selected SOW and the Common Paper PSA Standard Terms v1.1; (ii) the completed DPA Cover Page and Common Paper DPA Standard Terms v1.1 to the extent Personal Data processing is involved; (iii) the completed AI Addendum Cover Page and Common Paper AI Addendum Standard Terms v1.0 for AI Services; and (iv) the specifically identified completed Security Schedule D. The parties intend this integrated signature to constitute acceptance of each named Cover Page. Before execution, the parties must confirm that each identified Cover Page and required schedule is completed, included in the signing package, and unambiguously accepted through the signed Integrated Cover Page. The pre-sales Mutual NDA is separate.

PROVIDER — OMEGANEON LLC	CUSTOMER — [CUSTOMER LEGAL NAME]
Authorized signature: _____	Authorized signature: _____
Printed name: [NAME]	Printed name: [NAME]
Title: [TITLE]	Title: [TITLE]
Date: [DATE]	Date: [DATE]
Notice: hastersun@zohomail.com	Notice: [CUSTOMER NOTICE ADDRESS]

REFERENCE APPENDIX — Common Paper Standard Terms

PSA • https://commonpaper.com/standards/professional-services-agreement/1.1/ • Common Paper (CC BY 4.0; https://creativecommons.org/licenses/by/4.0/). Adapted by OMEGANEON; public sample updated 19 Nov 2026; not endorsed by Common Paper.

1. Services

1.1 Providing Services. Customer or its Affiliates may enter SOWs with Provider. Provider will perform the Services as detailed in an applicable SOW. Each SOW together with the Key Terms and Standard Terms will constitute a separate agreement. Provider will comply with Customer Policies, if any. If a Customer Affiliate enters an SOW with Provider, references to Customer in the SOW, Key Terms, or Standard Terms will mean that Affiliate for that agreement.
1.2 Cooperation. Customer will reasonably cooperate with Provider to allow the performance of Services. Provider is not responsible for an inability to perform the Services caused by Customer's failure to cooperate as reasonably requested. Provider will provide its own equipment and tools to perform the Services.
1.3 Change Orders. Provider or Customer may amend any SOW by entering a Change Order. If a party requests a Change Order, the other party will review and consider the proposed changes in good faith and respond to the Change Order request within a reasonable timeframe. However, a Change Order will not be binding until Provider and Customer agree in writing on the Change Order.
1.4 Acceptance. If according to the SOW Deliverables are subject to this section, Customer will be deemed to have approved a Deliverable if Customer does not reject the Deliverable within the Rejection Period. If Customer rejects a Deliverable, Customer must notify Provider in writing with reasonable detail about why the Deliverable did not meet the requirements in the SOW. Provider will correct the issue and resubmit the Deliverable within the Resubmission Period.
1.5 Subcontractors. Provider may use Subcontractors to perform the Services only with Customer's prior permission. However, Provider may use its Affiliates to perform Services without Customer's prior permission. If Provider uses Subcontractors to perform Services, Provider is responsible for (a) all acts and omissions of its Subcontractors, (b) ensuring its Subcontractors' compliance with this Agreement and the applicable SOW, and (c) making all payments owed to its Subcontractors for their portion of the Services.
1.6 Customer Obligations. Customer will comply with Customer Obligations, if any.

2. Intellectual Property

2.1 Deliverables. Except for Pre-Existing Materials and Third-Party Materials, Provider assigns all right, title, and interest in the Deliverables (if any) to Customer at the Time of Assignment. Upon the Time of Assignment, Provider will assert no rights over such Deliverables.
2.2 Customer Materials. Provider may copy, display, modify, and use Customer Materials only as needed to provide the Services. Customer is responsible for the accuracy and content of Customer Materials.
2.3 Pre-Existing Materials. To the extent Provider incorporates Pre-Existing Materials into Deliverables, Provider grants Customer a non-exclusive, non-transferrable, perpetual, irrevocable, worldwide license to use Pre-Existing Materials only as necessary to use the Deliverables according to this Agreement.
2.4 Third-Party Materials.
(a) Provider may incorporate Third-Party Materials into Deliverables only if allowed in the SOW and as authorized by Customer in writing (including by email).
(b) Provider is responsible for obtaining all rights, licenses, consents, approvals, and authorizations necessary to use and incorporate the Third-Party Materials procured by Provider and incorporated into the Deliverables. This includes securing the ability to grant Customer rights in the Deliverables under this Agreement and ensuring that Customer has all rights necessary in these Provider-procured Third-Party Materials so that Customer may use Deliverables according to this Agreement.
(c) Customer is responsible for obtaining all rights, licenses, consents, approvals, and authorizations necessary to use and incorporate the Third-Party Materials procured by Customer and incorporated into the Deliverables. This includes securing the ability to grant Provider rights in the Customer-procured Third-Party Materials so Provider can incorporate these Third-Party Materials into Deliverables. Provider will reasonably assist Customer in obtaining the necessary rights, licenses, consents, approvals, and authorizations for the Third-Party Materials that Provider recommends but that Customer procures.
2.5 Feedback and Usage Data. Customer may, but is not required to, give Provider Feedback, in which case Customer gives Feedback "AS IS". Provider may use all Feedback freely without any restriction or obligation. In addition, Provider may collect and analyze Usage Data, and Provider may freely use Usage Data to maintain, improve, and enhance Provider's products and services without restriction or obligation. However, Provider may only share Usage Data with others if the Usage Data is aggregated and does not identify Customer.
2.6 Reservation of Rights. Except for (a) Customer's ownership of Deliverables (if any) under Section 2.1 (Deliverables); (b) Provider's rights to use Customer Materials in Section 2.2 (Customer Materials); and (c) Customer's rights to Pre-Existing Materials in Section 2.3 (Pre-Existing Materials), neither party transfers any rights in any of their products, data, or any other intellectual property.

3. Privacy & Security

3.1 Personal Data. If the parties have a DPA, each party will comply with its obligations in the DPA, the terms of the DPA will control each party's rights and obligations as to Personal Data, and the terms of the DPA will control in the event of any conflict with this Agreement.
3.2 Security. Provider will comply with the Security Policy, if any.

4. Payment & Taxes

4.1 Fees and Invoices. Unless the currency is specified in the SOW, all Fees are in U.S. Dollars and are exclusive of taxes. Except for the prorated refund of prepaid Fees allowed with specific termination rights, Fees are non-refundable. Provider will send invoices for Fees as described in the SOW.
4.2 Payment. Customer will pay Provider the Fees and taxes in each invoice in U.S. Dollars, unless the SOW specifies a different currency, within the Payment Period.
4.3 Taxes. Customer is responsible for all duties, taxes, and levies that apply to Fees, including sales, use, VAT, GST, or withholding, that Provider itemizes and includes in an invoice. However, Customer is not responsible for Provider's income taxes.
4.4 Payment Dispute. If Customer has a good-faith disagreement about the amounts charged on an invoice, Customer must notify Provider about the dispute during the Payment Period for the invoice and must pay all undisputed amounts on time. The parties will work together to resolve the dispute within 15 days after the end of the Payment Period. If no resolution is agreed, each party may pursue any remedies available under the Agreement, the applicable SOW, or Applicable Laws.

5. Term & Termination

5.1 Term. This Agreement will start on the Effective Date and continue until 12 months have elapsed since the end of the latest SOW Term end date.
5.2 Termination.
(a) Either party may terminate this Agreement or an SOW immediately if the other party (i) fails to cure a material breach of the Agreement or SOW within 30 days after receiving notice of the breach; (ii) materially breaches the Agreement or SOW in a manner that cannot be cured; (iii) dissolves or stops conducting business without a successor; (iv) makes an assignment for the benefit of creditors; or (v) becomes the debtor in insolvency, receivership, or bankruptcy proceedings that continue for more than 60 days.
(b) Either party may terminate an affected SOW immediately if a Force Majeure Event prevents Provider from providing the Services for 30 or more consecutive days.
(c) Either party may terminate this Agreement for any or no reason if there are no active SOWs.
(d) A party must notify the other of its reason for termination.
5.3 Effect of Termination. Upon any expiration or termination:
(a) Termination of the Agreement pursuant to Section 5.2(a) or the Key Terms will automatically terminate all SOWs.
(b) Provider will no longer have to provide the Services.
(c) Each Recipient will return or destroy Discloser's Confidential Information in its possession or control.
(d) Except where Customer terminates pursuant to Section 5.2(a), Provider will submit a final invoice for all outstanding Fees accrued before termination and Customer will pay the invoice according to Section 4 (Payment & Taxes).
(e) Except where Provider terminates pursuant to Section 5.2(a), Provider will issue a refund for any unearned, prepaid Fees.
5.4 Survival.
(a) The following sections will survive expiration or termination of the Agreement: Section 2.1 (Deliverables), Section 2.3 (Pre-Existing Materials), Section 2.5 (Feedback and Usage Data), Section 2.6 (Reservation of Rights), Section 4 (Payment & Taxes) for fees accrued or payable before expiration or termination, Section 5.3 (Effect of Termination), Section 5.4 (Survival), Section 6 (Representations & Warranties), Section 7 (Disclaimer of Warranties), Section 8 (Limitation of Liability), Section 9 (Indemnification), Section 10 (Insurance) for the time period specified, Section 11 (Confidentiality), Section 12 (General Terms), Section 13 (Definitions), and the portions of a Cover Page referenced by these sections.
(b) Each Recipient may retain Discloser's Confidential Information in accordance with its standard backup or record retention policies maintained in the ordinary course of business or as required by Applicable Laws, in which case Section 3 (Privacy & Security) and Section 11 (Confidentiality) will continue to apply to retained Confidential Information.

6. Representations & Warranties

6.1 Mutual. Each party represents and warrants to the other that: (a) it has the legal power and authority to enter into this Agreement; (b) it is duly organized, validly existing, and in good standing under the Applicable Laws of the jurisdiction of its origin; (c) it will comply with all Applicable Laws in performing its obligations or exercising its rights in this Agreement; and (d) it will comply with the Additional Warranties.
6.2 From Customer. Customer represents and warrants to Provider that (a) Provider's use of Customer Materials and Customer-procured Third-Party Materials under this Agreement does not and will not infringe or misappropriate anyone else's copyright, trademark, trade secret, or right of publicity; and (b) it has all rights necessary to provide Customer Materials and Customer-procured Third-Party Materials under Section 2.
6.3 From Provider. Provider represents and warrants to Customer that: (a) it will perform the Services in a timely, competent, and professional manner; (b) the Deliverables (if any, however excluding Customer Materials and Customer-procured Third-Party

Materials) do not and will not infringe or misappropriate anyone else's copyright, trademark, trade secret, or right of publicity; (c) the Deliverables (if any) will conform to the requirements in the SOW; and (d) it has all rights necessary to perform the Services and convey the Deliverables (if any, however excluding Customer Materials and Customer-procured Third-Party Materials) under Section 2 (Intellectual Property).

6.4 Warranty Remedy. If Provider breaches the warranty in Section 6.3(c), Customer must give Provider notice (with enough detail for Provider to understand or replicate the issue) within 45 days of discovering the issue. Within 45 days of receiving sufficient details of the warranty issue, Provider will reperform the Services. If Provider cannot resolve the issue, Customer may terminate the affected SOW and Provider will pay to Customer a prorated refund of prepaid Fees for the remainder of the SOW Term. Provider's reperformance obligations and Customer's termination right are Customer's only remedies if Provider does not meet the warranty in Section 6.3(c).

7. Disclaimer of Warranties

7.1 Except for the warranties in Section 6 (Representations & Warranties), Provider and Customer each disclaim all other warranties, whether express or implied, including the implied warranties of merchantability, fitness for a particular purpose, title, and non-infringement. These disclaimers apply to the maximum extent permitted by Applicable Laws.

8. Limitation of Liability

8.1 Liability Caps. If there are Increased Claims, each party's total cumulative liability for the Increased Claims arising out of or relating to this Agreement will not be more than the Increased Cap Amount. Each party's total cumulative liability for all other claims arising out of or relating to this Agreement will not be more than the General Cap Amount.

8.2 Damages Waiver. Each party's liability for any claim or liability arising out of or relating to this Agreement will be limited to the fullest extent permitted by Applicable Laws. Under no circumstances will either party be liable to the other for lost profits or revenues, or for consequential, special, indirect, exemplary, punitive, or incidental damages relating to this Agreement, even if the party is informed of the possibility of this type of damage in advance.

8.3 Exceptions. The liability caps in Section 8.1 do not apply to any Unlimited Claims. The damages waiver in Section 8.2 does not apply to any Increased Claims or a breach of Section 11 (Confidentiality).

9. Indemnification

9.1 Protection by Provider. Provider will indemnify, defend, and hold harmless Customer from and against all Provider Covered Claims made by someone other than Customer or its Affiliates, and all out-of-pocket damages, awards, settlements, costs, and expenses, including reasonable attorneys' fees and other legal expenses, that arise from the Provider Covered Claim.

9.2 Protection by Customer. Customer will indemnify, defend, and hold harmless Provider from and against all Customer Covered Claims made by someone other than Provider or its Affiliates, and all out-of-pocket damages, awards, settlements, costs, and expenses, including reasonable attorneys' fees and other legal expenses, that arise from the Customer Covered Claim.

9.3 Procedure. The Indemnifying Party's obligations in this section are contingent upon the Protected Party: (a) promptly notifying the Indemnifying Party of each Covered Claim for which it seeks protection; (b) providing reasonable assistance to the Indemnifying Party at the Indemnifying Party's expense; and (c) giving the Indemnifying Party sole control over the defense and settlement of each Covered Claim. A Protected Party may participate in a Covered Claim for which it seeks protection with its own attorneys only at its own expense. The Indemnifying Party may not agree to any settlement of a Covered Claim that contains an admission of fault or otherwise materially and adversely impacts the Protected Party without the prior written consent of the Protected Party.

9.4 Exclusive Remedy. This Section 9 (Indemnification) describes each Protected Party's exclusive remedy and each Indemnifying Party's entire liability for a Covered Claim.

10. Insurance

10.1 During the term of the Agreement and for six months after, each party will carry commercial insurance policies with coverage limits that meet the relevant Insurance Minimums required in the SOW, if any. Upon request, each party will give the other a certificate of insurance evidencing its insurance policies that meet the required Insurance Minimums. A party's insurance policies will not be considered as evidence of its liability. Insurance coverage will be on a date of occurrence form and waive rights of subrogation or crossclaim.

11. Confidentiality

11.1 Non-Use and Non-Disclosure. Unless otherwise authorized in the Agreement, Recipient will (a) only use Discloser's Confidential Information to fulfill its obligations or exercise its rights under this Agreement; and (b) not disclose Discloser's Confidential Information to anyone else. In addition, Recipient will protect Discloser's Confidential Information using at least the same protections Recipient uses for its own similar information but no less than a reasonable standard of care.

11.2 Exclusions. Confidential Information does not include information that (a) Recipient knew without any obligation of confidentiality before disclosure by Discloser; (b) is or becomes publicly known and generally available through no fault of Recipient; (c) Recipient receives under no obligation of confidentiality from someone else who is authorized to make the disclosure; or (d) Recipient independently developed without use of or reference to Discloser's Confidential Information.

11.3 Required Disclosures. Recipient may disclose Discloser's Confidential Information to the extent required by Applicable Laws if, unless prohibited by Applicable Laws, Recipient provides the Discloser reasonable advance notice of the required disclosure and reasonably cooperates, at the Discloser's expense, with the Discloser's efforts to obtain confidential treatment for the Confidential Information.
11.4 Permitted Disclosures. Recipient may disclose Discloser's Confidential Information to employees, advisors, contractors, and representatives who each have a need to know the Confidential Information, but only if the person or entity is bound by confidentiality obligations at least as protective as those in this Section 11 and Recipient remains responsible for everyone's compliance with the terms of this Section 11.

12. General Terms

12.1 Entire Agreement. This Agreement is the only agreement between the parties about its subject and this Agreement supersedes all prior or contemporaneous statements (whether in writing or not) about its subject. Provider expressly rejects any terms included in Customer's purchase order or similar document, which may only be used for accounting or administrative purposes.
12.2 Modifications, Severability, and Waiver. Any waiver, modification, or change to the Agreement must be in writing and signed or electronically accepted by each party. However, this does not limit Provider's or Customer's ability to update an SOW by following the Change Order procedures. If any term of this Agreement is determined to be invalid or unenforceable by a relevant court or governing body, the remaining terms of this Agreement will remain in full force and effect. The failure of a party to enforce a term or to exercise an option or right in this Agreement will not constitute a waiver by that party of the term, option, or right.
12.3 Governing Law and Chosen Courts. The Governing Law will govern all interpretations and disputes about this Agreement, without regard to its conflict of laws provisions. The parties will bring any legal suit, action, or proceeding about this Agreement or an SOW in the Chosen Courts and each party irrevocably submits to the exclusive jurisdiction of the Chosen Courts.
12.4 Injunctive Relief. Despite Section 12.3 (Governing Law and Chosen Courts), a breach of Section 11 (Confidentiality) or the violation of a party's intellectual property rights may cause irreparable harm for which monetary damages cannot adequately compensate. As a result, upon the actual or threatened breach of Section 11 (Confidentiality) or violation of a party's intellectual property rights, the non-breaching or non-violating party may seek appropriate equitable relief, including an injunction, in any court of competent jurisdiction without the need to post a bond and without limiting its other rights or remedies.
12.5 Non-Exhaustive Remedies. Except where the Agreement provides for an exclusive remedy, seeking or exercising a remedy does not limit the other rights or remedies available to a party.
12.6 Assignment. Neither party may assign any rights or obligations under this Agreement or any SOW without the prior written consent of the other party. However, Customer may assign this Agreement upon notice if Customer undergoes a merger, change of control, reorganization, or sale of all or substantially all its equity, business, or assets to which this Agreement relates. Any attempted but non-permitted assignment is void. This Agreement will be binding upon and inure to the benefit of the parties and their permitted successors and assigns.
12.7 No Publicity. Neither party may publicly announce the existence of this Agreement or any SOW without the prior written approval of the other party.
12.8 Notices. Any notice, request, or approval about the Agreement must be in writing and sent to the Notice Address. Notices will be deemed given (a) upon confirmed delivery if by email, registered or certified mail, or personal delivery; or (b) two days after mailing if by overnight commercial delivery.
12.9 Independent Contractors. The parties are independent contractors, not agents, partners, or joint venturers. Neither party is authorized to bind the other to any liability or obligation.
12.10 No Third-Party Beneficiary. There are no third-party beneficiaries of this Agreement.
12.11 Force Majeure. Neither party will be liable for a delay or failure to perform its obligations of this Agreement if caused by a Force Majeure Event. However, this section does not excuse Customer's obligations to pay Fees.
12.12 Export Controls. Customer may not remove or export from the United States or allow the export or re-export of the Service, Deliverables, or any related technology or materials in violation of any restrictions, laws, or regulations of the United States Department of Commerce, the United States Department of Treasury Office of Foreign Assets Control, or any other United States or foreign agency or authority.
12.13 Anti-Bribery. Neither party will take any action that would be a violation of any Applicable Laws that prohibit the offering, giving, promising to offer or give, or receiving, directly or indirectly, money or anything of value to any third party to assist Provider or Customer in retaining or obtaining business. Examples of these kinds of laws include the U.S. Foreign Corrupt Practices Act and the UK Bribery Act 2010.
12.14 Titles and Interpretation. Section titles are for convenience and reference only. All uses of "including" and similar phrases are non-exhaustive and without limitation.
12.15 Signature. This Agreement may be signed in counterparts, including by electronic copies or acceptance mechanism. Each copy will be deemed an original and all copies, when taken together, will be the same agreement.

13. Definitions

13.1 "Affiliate" means an entity that, directly or indirectly, controls, is under the control of, or is under common control with a party, where control means having more than fifty percent (50%) of the voting stock or other ownership interest.
13.2 "Agreement" means these Standard Terms, the Key Terms between Provider and Customer, and the policies and documents referenced in or attached to the Key Terms.

13.3 “Applicable Laws” means the laws, rules, regulations, court orders, and other binding requirements of a relevant government authority.
13.4 "Change Order" means a document that identifies the SOW being changed, describes what the parties are changing, and is approved by an authorized representative of each party.
13.5 “Confidential Information” means information in any form disclosed by or on behalf of a Discloser, including before the Effective Date, to a Recipient in connection with this Agreement that (a) the Discloser identifies as “confidential”, “proprietary”, or the like; or (b) should be reasonably understood as confidential or proprietary due to its nature and the circumstances of its disclosure. Confidential Information includes the existence of this Agreement and the information on each Cover Page.
13.6 “Cover Page” means a document that is signed or electronically accepted by the parties that incorporates these Standard Terms, identifies Provider and Customer, and may include a SOW, Key Terms, or both.
13.7 “Covered Claim” means either a Provider Covered Claim or Customer Covered Claim.
13.8 "Customer Materials" means data, information, or materials owned or provided by or on behalf of Customer for use with the Services, but excludes Feedback and Customer-procured Third-Party Materials.
13.9 “Discloser” means a party to this Agreement when the party is providing or disclosing Confidential Information to the other party.
13.10 “Feedback” means suggestions, feedback, or comments about the Services or related offerings.
13.11 “Force Majeure Event” means an unforeseen event outside a party’s reasonable control where the affected party took reasonable measures to avoid or mitigate the impacts of the event. Examples of these kinds of events include unpredicted natural disaster like a major earthquake, war, pandemic, riot, act of terrorism, or public utility or internet failure.
13.12 “Indemnifying Party” means a party to this Agreement when the party is providing protection for a particular Covered Claim.
13.13 "Key Terms” means a Cover Page that includes the key legal details and definitions for this Agreement that are not defined in the SOW or Standard Terms. The Key Terms may include details about Covered Claims, set the Governing Law, or contain other legal details about this Agreement.
13.14 "Pre-Existing Materials" means any information, tools, materials, or intellectual property that Provider developed or owned before the Effective Date or developed after the Effective Date that are independent from or outside the scope of the Agreement, and any derivatives of these items that are not unique to Customer or that have generally applicable use and do not incorporate or disclose any Customer Confidential Information.
13.15 “Protected Party” means a party to this Agreement when the party is receiving the benefit of protection for a particular Covered Claim.
13.16 “Recipient” means a party to this Agreement when the party receives Confidential Information from the other party.
13.17 “Services” means the services described in a SOW, including the creation of Deliverables (if any).
13.18 "SOW" means a Cover Page that includes the key business details and definitions for this Agreement that are not defined in the Key Terms or Standard Terms. A SOW may include details about the Deliverables, Fees, or other details about the Services.
13.19 “Subcontractors” means other people or companies engaged by Provider to perform some of the Services, including Provider's Affiliates.
13.20 "Third-Party Materials" means any information, tools, materials, or intellectual property owned by anyone other than Provider, its Affiliates, or Customer.
13.21 “Usage Data” means data and information about the provision, use, and performance of the Services based on Customer’s use of the Services.

REFERENCE APPENDIX — Common Paper Standard Terms

The Common Paper PSA v1.1, DPA v1.1 and AI Addendum v1.0 Standard Terms are reproduced under CC BY 4.0. The OMEGANEON Cover Page includes express amendments; notably, DPA §5.2 in the reference text is replaced by the Cover Page amendment. The executed customer agreement determines the operative terms.

DPA • https://commonpaper.com/standards/data-processing-agreement/1.1/ • Common Paper (CC BY 4.0; https://creativecommons.org/licenses/by/4.0/). Adapted by OMEGANEON; public sample updated 19 Nov 2026; not endorsed by Common Paper.

1. Processor and Subprocessor Relationships

1.1 Provider as Processor. In situations where Customer is a Controller of the Customer Personal Data, Provider will be deemed a Processor that is Processing Personal Data on behalf of Customer.
1.2 Provider as Subprocessor. In situations where Customer is a Processor of the Customer Personal Data, Provider will be deemed a Subprocessor of the Customer Personal Data.

2. Processing

2.1 Processing Details. Annex I(B) on the Cover Page describes the subject matter, nature, purpose, and duration of this Processing, as well as the Categories of Personal Data collected and Categories of Data Subjects.

2.2 Processing Instructions. Customer instructs Provider to Process Customer Personal Data: (a) to provide and maintain the Service; (b) as may be further specified through Customer's use of the Service; (c) as documented in the Agreement; and (d) as documented in any other written instructions given by Customer and acknowledged by Provider about Processing Customer Personal Data under this DPA. Provider will abide by these instructions unless prohibited from doing so by Applicable Laws. Provider will immediately inform Customer if it is unable to follow the Processing instructions. Customer has given and will only give instructions that comply with Applicable Laws.
2.3 Processing by Provider. Provider will only Process Customer Personal Data in accordance with this DPA, including the details in the Cover Page. If Provider updates the Service to update existing or include new products, features, or functionality, Provider may change the Categories of Data Subjects, Categories of Personal Data, Special Category Data, Special Category Data Restrictions or Safeguards, Frequency of Transfer, Nature and Purpose of Processing, and Duration of Processing as needed to reflect the updates by notifying Customer of the updates and changes.
2.4 Customer Processing. Where Customer is a Processor and Provider is a Subprocessor, Customer will comply with all Applicable Laws that apply to Customer's Processing of Customer Personal Data. Customer's agreement with its Controller will similarly require Customer to comply with all Applicable Laws that apply to Customer as a Processor. In addition, Customer will comply with the Subprocessor requirements in Customer's agreement with its Controller.
2.5 Consent to Processing. Customer has complied with and will continue to comply with all Applicable Data Protection Laws concerning its provision of Customer Personal Data to Provider and/or the Service, including making all disclosures, obtaining all consents, providing adequate choice, and implementing relevant safeguards required under Applicable Data Protection Laws.
2.6 Subprocessors.
(a) Provider will not provide, transfer, or hand over any Customer Personal Data to a Subprocessor unless Customer has approved the Subprocessor. The current list of Approved Subprocessors includes the identities of the Subprocessors, their country of location, and their anticipated Processing tasks. Provider will inform Customer at least 10 business days in advance and in writing of any intended changes to the Approved Subprocessors whether by addition or replacement of a Subprocessor, which allows Customer to have enough time to object to the changes before the Provider begins using the new Subprocessor(s). Provider will give Customer the information necessary to allow Customer to exercise its right to object to the change to Approved Subprocessors. Customer has 30 days after notice of a change to the Approved Subprocessors to object, otherwise Customer will be deemed to accept the changes. If Customer objects to the change within 30 days of notice, Customer and Provider will cooperate in good faith to resolve Customer's objection or concern.
(b) When engaging a Subprocessor, Provider will have a written agreement with the Subprocessor that ensures the Subprocessor only accesses and uses Customer Personal Data (i) to the extent required to perform the obligations subcontracted to it, and (ii) consistent with the terms of Agreement.
(c) If the GDPR applies to the Processing of Customer Personal Data, (i) the data protection obligations described in this DPA (as referred to in Article 28(3) of the GDPR, if applicable) are also imposed on the Subprocessor, and (ii) Provider's agreement with the Subprocessor will incorporate these obligations, including details about how Provider and its Subprocessor will coordinate to respond to inquiries or requests about the Processing of Customer Personal Data. In addition, Provider will share, at Customer's request, a copy of its agreements (including any amendments) with its Subprocessors. To the extent necessary to protect business secrets or other confidential information, including personal data, Provider may redact the text of its agreement with its Subprocessor prior to sharing a copy.
(d) Provider remains fully liable for all obligations subcontracted to its Subprocessors, including the acts and omissions of its Subprocessors in Processing Customer Personal Data. Provider will notify Customer of any failure by its Subprocessors to fulfill a material obligation about Customer Personal Data under the agreement between Provider and the Subprocessor.

3. Restricted Transfers

3.1 Authorization. Customer agrees that Provider may transfer Customer Personal Data outside the EEA, the United Kingdom, or other relevant geographic territory as necessary to provide the Service. If Provider transfers Customer Personal Data to a territory for which the European Commission or other relevant supervisory authority has not issued an adequacy decision, Provider will implement appropriate safeguards for the transfer of Customer Personal Data to that territory consistent with Applicable Data Protection Laws.
3.2 Ex-EEA Transfers. Customer and Provider agree that if the GDPR protects the transfer of Customer Personal Data, the transfer is from Customer from within the EEA to Provider outside of the EEA, and the transfer is not governed by an adequacy decision made by the European Commission, then by entering into this DPA, Customer and Provider are deemed to have signed the EEA SCCs and their Annexes, which are incorporated by reference. Any such transfer is made pursuant to the EEA SCCs, which are completed as follows:
(a) Module Two (Controller to Processor) of the EEA SCCs apply when Customer is a Controller and Provider is Processing Customer Personal Data for Customer as a Processor.
(b) Module Three (Processor to Sub-Processor) of the EEA SCCs apply when Customer is a Processor and Provider is Processing Customer Personal Data on behalf of Customer as a Subprocessor.
(c) For each module, the following applies (when applicable):
(i) The optional docking clause in Clause 7 does not apply;
(ii) In Clause 9, Option 2 (general written authorization) applies, and the minimum time period for prior notice of Subprocessor changes is 10 business days;
(iii) In Clause 11, the optional language does not apply;

(iv) All square brackets in Clause 13 are removed;
(v) In Clause 17 (Option 1), the EEA SCCs will be governed by the laws of Governing Member State;
(vi) In Clause 18(b), disputes will be resolved in the courts of the Governing Member State; and
(vii) The Cover Page to this DPA contains the information required in Annex I, Annex II, and Annex III of the EEA SCCs.
3.3 Ex-UK Transfers. Customer and Provider agree that if the UK GDPR protects the transfer of Customer Personal Data, the transfer is from Customer from within the United Kingdom to Provider outside of the United Kingdom, and the transfer is not governed by an adequacy decision made by the United Kingdom Secretary of State, then by entering into this DPA, Customer and Provider are deemed to have signed the UK Addendum and their Annexes, which are incorporated by reference. Any such transfer is made pursuant to the UK Addendum, which is completed as follows:
(a) Section 3.2 of this DPA contains the information required in Table 2 of the UK Addendum.
(b) Table 4 of the UK Addendum is modified as follows: Neither party may end the UK Addendum as set out in Section 19 of the UK Addendum; to the extent ICO issues a revised Approved Addendum under Section 18 of the UK Addendum, the parties will work in good faith to revise this DPA accordingly.
(c) The Cover Page contains the information required by Annex 1A, Annex 1B, Annex II, and Annex III of the UK Addendum.
3.4 Other International Transfers. For Personal Data transfers where Swiss law (and not the law in any EEA member state or the United Kingdom) applies to the international nature of the transfer, references to the GDPR in Clause 4 of the EEA SCCs are, to the extent legally required, amended to refer to the Swiss Federal Data Protection Act or its successor instead, and the concept of supervisory authority will include the Swiss Federal Data Protection and Information Commissioner.

4. Security Incident Response

4.1 Upon becoming aware of any Security Incident, Provider will: (a) notify Customer without undue delay when feasible, but no later than 72 hours after becoming aware of the Security Incident; (b) provide timely information about the Security Incident as it becomes known or as is reasonably requested by Customer; and (c) promptly take reasonable steps to contain and investigate the Security Incident. Provider's notification of or response to a Security Incident as required by this DPA will not be construed as an acknowledgment by Provider of any fault or liability for the Security Incident.

5. Audit & Reports

5.1 Audit Rights. Provider will give Customer all information reasonably necessary to demonstrate its compliance with this DPA and Provider will allow for and contribute to audits, including inspections by Customer, to assess Provider's compliance with this DPA. However, Provider may restrict access to data or information if Customer's access to the information would negatively impact Provider's intellectual property rights, confidentiality obligations, or other obligations under Applicable Laws. Customer acknowledges and agrees that it will only exercise its audit rights under this DPA and any audit rights granted by Applicable Data Protection Laws by instructing Provider to comply with the reporting and due diligence requirements below. Provider will maintain records of its compliance with this DPA for 3 years after the DPA ends.
5.2 Security Reports. Customer acknowledges that Provider is regularly audited against the standards defined in the Security Policy by independent third-party auditors. Upon written request, Provider will give Customer, on a confidential basis, a summary copy of its then-current Report so that Customer can verify Provider's compliance with the standards defined in the Security Policy.
5.3 Security Due Diligence. In addition to the Report, Provider will respond to reasonable requests for information made by Customer to confirm Provider's compliance with this DPA, including responses to information security, due diligence, and audit questionnaires, or by giving additional information about its information security program. All such requests must be in writing and made to the Provider Security Contact and may only be made once a year.

6. Coordination & Cooperation

6.1 Response to Inquiries. If Provider receives any inquiry or request from anyone else about the Processing of Customer Personal Data, Provider will notify Customer about the request and Provider will not respond to the request without Customer's prior consent. Examples of these kinds of inquiries and requests include a judicial or administrative or regulatory agency order about Customer Personal Data where notifying Customer is not prohibited by Applicable Law, or a request from a data subject. If allowed by Applicable Law, Provider will follow Customer's reasonable instructions about these requests, including providing status updates and other information reasonably requested by Customer. If a data subject makes a valid request under Applicable Data Protection Laws to delete or opt out of Customer's giving of Customer Personal Data to Provider, Provider will assist Customer in fulfilling the request according to the Applicable Data Protection Law. Provider will cooperate with and provide reasonable assistance to Customer, at Customer's expense, in any legal response or other procedural action taken by Customer in response to a third-party request about Provider's Processing of Customer Personal Data under this DPA.
6.2 DPIAs and DTIAs. If required by Applicable Data Protection Laws, Provider will reasonably assist Customer in conducting any mandated data protection impact assessments or data transfer impact assessments and consultations with relevant data protection authorities, taking into consideration the nature of the Processing and Customer Personal Data.

7. Deletion of Customer Personal Data

7.1 Deletion by Customer. Provider will enable Customer to delete Customer Personal Data in a manner consistent with the functionality of the Services. Provider will comply with this instruction as soon as reasonably practicable except where further storage of Customer Personal Data is required by Applicable Law.

7.2 Deletion at DPA Expiration.
(a) After the DPA expires, Provider will return or delete Customer Personal Data at Customer's instruction unless further storage of Customer Personal Data is required or authorized by Applicable Law. If return or destruction is impracticable or prohibited by Applicable Laws, Provider will make reasonable efforts to prevent additional Processing of Customer Personal Data and will continue to protect the Customer Personal Data remaining in its possession, custody, or control. For example, Applicable Laws may require Provider to continue hosting or Processing Customer Personal Data.
(b) If Customer and Provider have entered the EEA SCCs or the UK Addendum as part of this DPA, Provider will only give Customer the certification of deletion of Personal Data described in Clause 8.1(d) and Clause 8.5 of the EEA SCCs if Customer asks for one.

8. Limitation of Liability

8.1 Liability Caps and Damages Waiver. To the maximum extent permitted under Applicable Data Protection Laws, each party's total cumulative liability to the other party arising out of or related to this DPA will be subject to the waivers, exclusions, and limitations of liability stated in the Agreement.
8.2 Related-Party Claims. Any claims made against Provider or its Affiliates arising out of or related to this DPA may only be brought by the Customer entity that is a party to the Agreement.
8.3 Exceptions. This DPA does not limit any liability to an individual about the individual's data protection rights under Applicable Data Protection Laws. In addition, this DPA does not limit any liability between the parties for violations of the EEA SCCs or UK Addendum.

9. Conflicts Between Documents

9.1 This DPA forms part of and supplements the Agreement. If there is any inconsistency between this DPA, the Agreement, or any of their parts, the part listed earlier will control over the part listed later for that inconsistency: (1) the EEA SCCs or the UK Addendum, (2) this DPA, and then (3) the Agreement.

10. Term of Agreement

10.1 This DPA will start when Provider and Customer agree to a Cover Page for the DPA and sign or electronically accept the Agreement and will continue until the Agreement expires or is terminated. However, Provider and Customer will each remain subject to the obligations in this DPA and Applicable Data Protection Laws until Customer stops transferring Customer Personal Data to Provider and Provider stops Processing Customer Personal Data.

11. Definitions.

11.1 "Applicable Laws" means the laws, rules, regulations, court orders, and other binding requirements of a relevant government authority that apply to or govern a party.
11.2 "Applicable Data Protection Laws" means the Applicable Laws that govern how the Service may process or use an individual's personal information, personal data, personally identifiable information, or other similar term.
11.3 "Controller" will have the meaning(s) given in the Applicable Data Protection Laws for the company that determines the purpose and extent of Processing Personal Data.
11.4 "Cover Page" means a document that is signed or electronically accepted by the parties that incorporates these DPA Standard Terms and identifies Provider, Customer, and the subject matter and details of the data processing.
11.5 "Customer Personal Data" means Personal Data that Customer uploads or provides to Provider as part of the Service and that is governed by this DPA.
11.6 "DPA" means these DPA Standard Terms, the Cover Page between Provider and Customer, and the policies and documents referenced in or attached to the Cover Page.
11.7 "EEA SCCs" means the standard contractual clauses annexed to the European Commission's Implementing Decision 2021/914 of 4 June 2021 on standard contractual clauses for the transfer of personal data to third countries pursuant to Regulation (EU) 2016/679 of the European Parliament and of the European Council.
11.8 "European Economic Area" or "EEA" means the member states of the European Union, Norway, Iceland, and Liechtenstein.
11.9 "GDPR" means European Union Regulation 2016/679 as implemented by local law in the relevant EEA member nation.
11.10 "Personal Data" will have the meaning(s) given in the Applicable Data Protection Laws for personal information, personal data, or other similar term.
11.11 "Processing" or "Process" will have the meaning(s) given in the Applicable Data Protection Laws for any use of, or performance of a computer operation on, Personal Data, including by automatic methods.
11.12 "Processor" will have the meaning(s) given in the Applicable Data Protection Laws for the company that Processes Personal Data on behalf of the Controller.
11.13 "Report" means audit reports prepared by another company according to the standards defined in the Security Policy on behalf of Provider.
11.14 "Restricted Transfer" means (a) where the GDPR applies, a transfer of personal data from the EEA to a country outside of the EEA which is not subject to an adequacy determination by the European Commission; and (b) where the UK GDPR applies, a transfer of personal data from the United Kingdom to any other country which is not subject to adequacy regulations adopted pursuant to Section 17A of the United Kingdom Data Protection Act 2018.

11.15 “Security Incident” means a Personal Data Breach as defined in Article 4 of the GDPR.
11.16 “Service” means the product and/or services described in the Agreement.
11.17 "Special Category Data” will have the meaning given in Article 9 of the GDPR.
11.18 “Subprocessor” will have the meaning(s) given in the Applicable Data Protection Laws for a company that, with the approval and acceptance of Controller, assists the Processor in Processing Personal Data on behalf of the Controller.
11.19 “UK GDPR” means European Union Regulation 2016/679 as implemented by section 3 of the United Kingdom’s European Union (Withdrawal) Act of 2018 in the United Kingdom.
11.20 “UK Addendum” means the international data transfer addendum to the EEA SCCs issued by the Information Commissioner for Parties making Restricted Transfers under S119A(1) Data Protection Act 2018.

REFERENCE APPENDIX — Common Paper Standard Terms

The Common Paper PSA v1.1, DPA v1.1 and AI Addendum v1.0 Standard Terms are reproduced under CC BY 4.0. The OMEGANEON Cover Page includes express amendments; notably, DPA §5.2 in the reference text is replaced by the Cover Page amendment. The executed customer agreement determines the operative terms.

AI Addendum • https://commonpaper.com/standards/ai-addendum/1.0/ • Common Paper (CC BY 4.0; https://creativecommons.org/licenses/by/4.0/). Adapted by OMEGANEON; public sample updated 19 Nov 2026; not endorsed by Common Paper.

1. AI Services

1.1 Using AI Services. The AI Services are part of the Product and subject to the Agreement as supplemented by this AI Addendum. Customer may use AI Services by providing Input. The AI Services may generate Output in response to Input. Provider may copy, display, modify, distribute, and use Input to the extent necessary to provide the AI Services as contemplated by this AI Addendum. Customer authorizes Provider to process Input for all such purposes.
1.2 Restrictions. Without limiting the restrictions contained in the Agreement, Customer will not (and will not allow anyone else to): (a) use the AI Services for decision-making in a regulated industry or capacity without proper human oversight and review in compliance with Applicable Laws and applicable professional ethics, guidelines, and rules; (b) use the AI Services to violate, misappropriate, or otherwise infringe the intellectual property or other proprietary rights of others; or (c) falsely state Output was created by a human.
1.3 Model Training. Unless the Cover Page identifies Training Data and Training Purposes, Provider may not use Customer's Inputs or Outputs to Train any Model. If the Cover Page permits Training, then subject to the Training Restrictions, Provider may copy, modify, distribute, and use Training Data for the Training Purposes.
1.4 Non-Training Improvement. Subject to the Improvement Restrictions, Provider may use Input, Output, and Training Data to provide, maintain, develop, and improve the AI System, provided that such usage does not constitute Training except to the extent authorized for Training Purposes.

2. Intellectual Property and Privacy

2.1 Ownership. As between the parties, Customer (a) retains all right, title, and interest in and to all Input, and (b) owns all Output. To the extent permitted by Applicable Laws, Provider hereby assigns to Customer all right, title, and interest—if any—in and to Output.
2.2 Personal Data. Nothing in this AI Addendum will reduce or limit Provider's obligations under Applicable Data Protection Laws regarding Personal Data that may be contained in Input.
2.3 Rights to Input. Customer represents and warrants that it, all Users, and anyone submitting Input each have and will continue to have all rights necessary to submit Input to the AI Services.

3. Disclaimers

3.1 Nature of AI. Due to the nature of artificial intelligence and machine learning, information generated by the AI Services may be incorrect or inaccurate. The AI Services are not human and are not a substitute for human oversight. Output generated by the AI Services may not be protectable as intellectual property.
3.2 Similarity of Output. Output may resemble or be duplicative of data, information, and materials created by the AI Services for others. Provider does not provide any representation or warranty that Output (a) does not and will not incorporate or reflect the data, information, prompts, or materials of others, (b) will not violate, misappropriate, or otherwise infringe upon the intellectual property or other proprietary rights of another person or entity, or (c) will not be reproduced in the same or similar way to another user of the AI Services.

4. Definitions

4.1 "AI Addendum Standard Terms" means these Common Paper AI Addendum Standard Terms Version 1.0, which are posted at https://commonpaper.com/standards/ai-addendum/1.0/.
4.2 "AI Services" means the artificial intelligence or machine learning components of the Product, including the AI System and underlying Model(s).
4.3 "AI System" means the artificial intelligence or machine learning application, program, and services layers of the AI Services, excluding the underlying Models.
4.4 "Input" means the data, information, prompts, or materials submitted by or on behalf of Customer or Users to the AI Services but excludes Feedback.
4.5 "Model" means a large language, machine learning, or artificial intelligence model.
4.6 "Output" means the data, information, or materials created by the AI Services in response to Input.
4.7 "Train" or "Training" means the use of data, information, or materials to create or improve a Model.