Paid Pilot Agreement

Public Legal Review Sample | Pilot Contract v1.2

$4,000 | Four Weeks (28 calendar days) | One Sandbox Workflow

---

This PDF is provided for prospective customer legal review only.

It is NOT a signed or executable agreement by itself.

All customer-specific variables must be completed before any signature:

workflow, objective tests, access boundaries, data categories, approved vendors,

hosting regions, sandbox security evidence and applicable schedules.

Customer Personal Data must not enter a Pilot sandbox before the necessary

DPA and verified security conditions have been satisfied.

Pilot use does not grant Production Go-Live or automatically convert to a PSA.

The signed Pilot Agreement must expressly incorporate the approved AUP v1.4.

The following pages reproduce the editable Pilot Integrated Template v1.2.

The signed customer-specific agreement, if any, controls over this sample.

OMEGANEON LLC | Legal inquiries: hastersun@zohomail.com

Source license: Common Paper Pilot Agreement Standard Terms v1.1, CC BY 4.0

01 / PILOT AGREEMENT

PAID PILOT AGREEMENT

Omeganeon LLC • $4,000 fixed fee • 4 weeks (28 calendar days) • one sandbox workflow • Based on Common Paper Pilot Agreement Standard Terms v1.1

TEMPLATE FOR CLIENT REVIEW — NOT AN EXECUTED AGREEMENT. Fill every bracketed item, approve the applicable exhibits, verify required safeguards, and remove template status only when preparing a completed customer signing copy.

A. Order Form / Parties & Commercial Terms

Field	Agreed value
Provider	Omeganeon LLC (Washington, USA) | Notice: hastersun@zohomail.com | Authorized representative: [NAME / TITLE]
Customer	[CUSTOMER LEGAL NAME / FORMATION STATE / NOTICE EMAIL / ADDRESS / SIGNATORY]
Effective Date	Last date of the parties' signatures on this Order Form.
Product / Services	One (1) customer-specific AI workflow prototype configured, tested and evaluated in a controlled sandbox, together with documented Pilot deliverables under Exhibit A. This is an implementation-and-evaluation service, not a production subscription.
Pilot Fee	$4,000 USD fixed, subject to applicable taxes; includes agreed pilot hosting and model/API usage within the Exhibit A scope. No automatic cloud/token/request overage charges.
Payment	100% ($4,000) invoiced on signing and received before written Kickoff. No duty to commence before cleared payment and prerequisites.
Kickoff / Pilot Period	[WRITTEN KICKOFF DATE] after payment, approved scope, needed data, access and approvals. Pilot Service Period = 28 consecutive calendar days beginning on that Kickoff Date.
Governing Law / Courts	State of Washington, USA / state and federal courts in King County, Washington.
General Cap Amount	$4,000 total aggregate (1× Pilot Fee), where enforceable; excludes non-waivable duties and applicable mandatory DPA / SCC / UK transfer liabilities to the extent not contractually limitable.
Included documents	Exhibit A Pilot SOW; Exhibit B DPA Cover Page only when activated; Exhibit C AI Addendum; Exhibit D Sandbox Security Schedule; Exhibit E Unified AUP v1.4 (issued Nov 19, 2026), expressly incorporated when attached; Common Paper Pilot Standard Terms v1.1.
Conversion	Pilot is separate from any Production PSA + SOW; no automatic subscription or fee credit. Any meeting-specific incentive must be confirmed in a signed written offer or Definitive Agreement.

B. Express Order Form Modifications to Standard Terms

1. Service scope / §1.1, §8.14. "Product" includes only the professional services and controlled sandbox prototype identified in Exhibit A. "Evaluation Purposes" include authorized internal tests of that prototype and review of the

specified outcomes. The parties have not authorized any live production operation, unrestricted external actions, or a general software subscription.

2. Evaluation term / §2.1. The Agreement takes effect on the Effective Date for contracting and preparation, but the 28-calendar-day Pilot Service Period begins solely on the documented Kickoff Date. Submission of the final Pilot report is due during the Pilot Service Period. The 5-Business-Day acceptance/review and any valid resubmission process survive its expiration without automatically extending full sandbox access, commencing production use, or creating recurring charges.

3. Payment / Fees. The Pilot Fee is prepaid and fixed for the agreed scope. No separate cloud infrastructure, AI token/request or automatic usage overage invoice applies. A materially changed scope, volume, vendor or hosting configuration requires both parties' advance written Change Order. Third-party extras require advance, itemized Customer written authorization. No retroactive usage charges.

4. Termination / §2.2. Section 2.2(c) (termination for any/no reason on 30 days' notice) is deleted for this fixed 28-day Pilot. For a curable material breach, the non-breaching party provides written notice and a cure period of five (5) Business Days; uncured material breach or an incurable material breach permits termination as provided in §2.2. Immediate risk restrictions under the executed Security Schedule do not themselves terminate the Agreement. If Kickoff cannot occur, the parties will agree in writing on a revised date or termination and fee reconciliation.

5. Earned fees / refunds / §2.2–§2.3. On permitted early termination, Provider retains only reasonably documented fees earned for Pilot services already performed and any specifically Customer-approved, non-cancellable costs incurred for the Pilot, without double recovery. Unearned prepaid amounts are returned according to the Agreement and applicable law. There is no unconditional forfeiture of the full $4,000 fee. Provide a written work-and-cost accounting on termination. No promise of a refund solely because an agreed acceptance test fails before the contractual cure process concludes.

6. Deliverables / §4.1. Notwithstanding the general "AS IS / AS AVAILABLE" Product disclaimer, Provider must perform the specific work and submit the objectively testable Pilot deliverables in Exhibit A and must follow the limited acceptance/remediation process there. This is not a guarantee of downstream revenue, full production readiness, zero defects, or specified business outcomes absent express agreement.

7. Acceptance. Provider submits the final deliverables and completed Acceptance Report per Exhibit A. Customer has five (5) Business Days after documented delivery to give a written, criterion-specific nonconformity notice. Without such notice, the deliverables are deemed accepted at the end of that period. Provider has five (5) Business Days after receipt of a valid rejection to correct and resubmit the affected deliverable; a fresh five (5) Business-Day review period then applies solely to the corrected deliverable. Disputes regarding acceptance do not authorize production deployment.

8. Intellectual property / §1.2, §1.7. Customer retains all rights in its Customer Content and owns the customer-specific Pilot findings, measurement and acceptance reports created specifically for Customer, subject to applicable law and Provider background materials. Provider retains ownership of the prototype implementation, workflow configuration, EDGEPORT, reusable templates, frameworks, code, methods and improvements not unique to Customer. Customer receives only a limited, revocable, non-transferable evaluation license to operate the sandbox prototype during authorized Pilot access; no production license or source-code transfer is granted. Customer may retain and internally use paid reports following expiration, subject to confidentiality and third-party rights.

9. Customer data / §1.4–1.5. The parties will use synthetic or properly anonymized test data by default. No Customer Personal Data, live CRM content or production credentials may be introduced without a prior written change approval, completed Exhibit B DPA if applicable, approved vendor/region schedule and evidence of appropriate sandbox security controls. Section 1.5 is narrowed: Customer Input/Output, non-public Feedback, Customer Content and Customer-derived Usage Data may be used only for contracted service delivery, security, troubleshooting and legal compliance; not for general model training, broad product improvement, sales promotion or cross-client reuse without separate express written authorization.

10. Exit / §2.3. Provider will return or securely delete Customer-provided sandbox content within thirty (30) calendar days after Pilot expiration or permitted termination, according to documented Customer instructions, subject to lawful backups and mandatory retention. This replaces the §2.3(b) 60-day customer-request-only timeline for pilot sandbox data. Provider will disable prototype access at the end of authorized evaluation, subject to limited read-only acceptance review if Exhibit A requires it. Minimal, content-redacted AI action audit metadata may remain for the agreed ninety (90) days only to the extent consistent with the DPA, deletion instructions and applicable law; no implied retention of raw Customer Personal Data.

11. Security / AUP. Exhibit D imposes minimum required sandbox entry controls, which must be implemented and verified before connecting any Customer systems or processing Customer-provided data. Production security certification/Go-Live obligations under a future Common Contract are not represented as satisfied by a Pilot. Exhibit E AUP applies only if its exact adopted version is attached or expressly identified in the executed Order Form.

12. Liability / §5.1–5.3. The aggregate General Cap Amount for claims arising from this Pilot is $4,000 to the maximum extent allowed by law, including claims for agreed deliverable-process obligations; the parties do not intend a $4,000 cap on liabilities which may not legally be capped or on mandatory data-transfer obligations to the extent prohibited. No standalone blanket AI-output indemnity or pilot-specific third-party IP indemnity is added. Section 6 confidentiality and any surviving rights remain subject to their express terms and applicable law.

13. Document precedence. Mandatory applicable transfer clauses take precedence to the extent required by law; if effective, Exhibit B controls personal-data processing, Exhibit C controls AI-specific restrictions, Exhibit D controls applicable sandbox security, Exhibit A controls implementation/acceptance/fees and workflow scope, and this Order Form controls other Pilot legal and commercial terms. The Common Paper Standard Terms v1.1 apply except for express amendments in this Order Form. Exhibit E AUP imposes customer conduct rules without creating new charges, IP warranties or unapproved data-processing rights.

One-signature attachment roster

Attachment	Application / version	Included at signature?
Exhibit A	Pilot SOW v1.0; required	YES
Exhibit B	Pilot DPA Cover v1.0; only if personal data	[YES / NOT APPLICABLE]
Exhibit C	Pilot AI Addendum v1.1; required if AI used	YES
Exhibit D	Pilot Sandbox Security Schedule v1.0; required	YES
Exhibit E	Unified AI AUP v1.4 (issued Nov 19, 2026), expressly incorporated as Exhibit E	[YES / VERSION / ATTACHED]
Standard Terms	Common Paper Pilot Agreement v1.1; incorporated by reference	YES

C. Signatures

The authorized signatories agree to this completed Order Form and every exhibit expressly identified as included above. A post-Pilot Acceptance Report is a later performance record, not a separate Day 0 contract.

Provider — Omeganeon LLC	Customer — [CUSTOMER LEGAL NAME]
Signature: _____	Signature: _____
Print name / title: [_____]	Print name / title: [_____]
Notice: hastersun@zohomail.com	Notice: [_____]
Date: [_____]	Date: [_____]

EXHIBIT A / PILOT STATEMENT OF WORK

PILOT STATEMENT OF WORK

Fixed-scope evaluation: one workflow • $4,000 • four weeks from documented Kickoff

CUSTOMER-SPECIFIC EXHIBIT. Must be completed and attached to the Pilot Agreement BEFORE signing. Pilot measurements and acceptance criteria cannot be supplied after the fact.

1. Parties, Pilot objective and prerequisites

Field	To complete before execution
Pilot Agreement ID	[PILOT ID] | Customer: [CUSTOMER LEGAL NAME]
Workflow name	[ONE HIGH-VALUE WORKFLOW ONLY]
Business bottleneck / baseline	[CURRENT MANUAL PROCESS, SYSTEMS, PERSONAS, MEASURED BASELINE OR "UNKNOWN—TO BE MEASURED IN WEEK 1"]
Pilot purpose	Test feasibility of [SCOPE] inside an isolated sandbox; evidence to evaluate an optional production contract.
Kickoff prerequisites	$4,000 received; workflow inputs, synthetic/anonymized dataset, sandbox access and authorized approver are ready; written Kickoff confirmation.
Kickoff date	[DATE, REVISED ONLY BY WRITTEN AGREEMENT]
Client project owner / approver	[NAME / ROLE / EMAIL]
Sandbox hosting	[OMEGANEON-HOSTED DEFAULT / BYOC IF AGREED]; region [REGION]; selected cloud [AWS/AZURE/GCP]; approved AI/model vendor [NAME/REGION]
Use of personal data	DEFAULT: no Customer Personal Data or sensitive data. Exception: [NO / WRITTEN APPROVAL + COMPLETED DPA + SECURITY GATE].

2. Work scope and exclusions

Included	Explicitly excluded unless amended
Discovery and workflow mapping; one sandbox implementation; test setup and deterministic checks; documented results; final acceptance report and production expansion outline.	Production Go-Live, live customer-facing execution, enterprise-wide rollouts, unmanaged third-party services, unapproved connectors, sustained managed operations, guarantees of headcount reduction/revenue, and rights to underlying prototype code.
Systems / connectors: [LIST]; data types: [LIST]; triggers/frequency: [DEFINE].	Out-of-scope external writes, financial or destructive operations, unapproved personal data, confidential access outside the sandbox.

3. Deliverables & objective acceptance criteria

Deliverable	Evidence / acceptance test	Target / threshold (complete now)
D1 Workflow map	Inputs, decision steps, human approvals and boundary diagram	[SIGNED-OFF SPECIFICATION / TEST]
D2 Sandbox prototype	Demonstration and repeatable test execution on agreed dataset	[TEST CASE SET / REQUIRED FUNCTIONS]
D3 Pilot testing results	Successful runs / failures / test artifacts / logs	[SAMPLE SIZE AND PASS RATE / ERROR THRESHOLD]
D4 Measurement and evaluation report	Before/after baseline, time/cost/quality	[METRICS / MINIMUM EVIDENCE]

Deliverable	Evidence / acceptance test	Target / threshold (complete now)
	evidence, caveats	
D5 Production expansion outline	Prerequisites, deployment risks, potential scope and next-step proposal	[REPORT SECTIONS]

Acceptance tests must be measurable against a frozen or documented test set, with objective input/output expectations and authorized approver. A test's commercial value is not assumed from the prototype alone. Customer is not obliged to enter a production contract.

4. Four-week delivery schedule

Week	Planned activity / checkpoint
Week 1	Discovery + Workflow Mapping; finalize baseline and synthetic evaluation set, confirm APB/HITL requirements.
Week 2	Sandbox Implementation; connectors and agent workflows under approved sandbox boundaries.
Week 3	Testing + Conversion Discussion; execute tests, capture evidence, discuss a possible production scope without binding conversion.
Week 4	Final Acceptance + Proposal; submit agreed deliverables and signed-off testing evidence by Day 28.

5. Acceptance mechanics

Submission. OMEGANEON delivers D1–D5 and a completed Acceptance Report by the end of the 28-calendar-day Pilot Service Period, subject to agreed schedule extensions for documented Customer dependencies and signed scope changes.

Review. Customer has five (5) Business Days from documented delivery to notify specific failures against the agreed criteria in writing. Silence after the deadline constitutes deemed acceptance under the Pilot Order Form.

Correction. Provider has five (5) Business Days from a valid rejection notice to correct and resubmit the affected deliverable; Customer has a new five (5) Business-Day review period limited to the corrections. The acceptance tail does not start ongoing managed fees or production access.

Customer actions. Customer supplies authorized approvers, approvals and synthetic datasets on time and does not introduce unapproved live or regulated data. Delays or scope expansion require documented schedule change / Change Order.

6. Fees, license, data lifecycle and next steps

Total fixed Pilot Fee $4,000 USD (100% received before Kickoff). The fee includes the agreed sandbox cloud and AI API consumption. No automatically billable cloud or token overages. If material additional usage or scope is requested, both parties must agree a written Change Order before implementation.

Customer retains its data and the customer-specific evaluation / acceptance reports. Prototype, reusable workflows/code, EDGEPORT and other Provider technology remain with OMEGANEON; Customer receives temporary evaluation rights only. No production use or perpetual deployment rights are conveyed by this SOW.

Sandbox Customer Content is returned/deleted within 30 calendar days after the Pilot ends, subject to lawful exceptions and the applicable DPA. The separate 90-day minimal audit log regime must avoid retaining raw personal content beyond authorized deletion limits. A Pilot-specific Security Schedule must be verified before connecting any Customer systems.

Any pricing concession on future production engagement is optional, case-specific and binding only when confirmed in a separate written offer or production PSA/SOW. No automatic $4,000 credit, renewal or conversion.

EXHIBIT B / CONDITIONAL PRIVACY TERMS

PILOT DATA PROCESSING AGREEMENT

Pilot-specific Cover Page adapting Common Paper DPA Standard Terms v1.1 • Activate only if Customer Personal Data will be processed

DEFAULT: synthetic or properly anonymized sandbox data only. Exhibit B is marked NOT APPLICABLE unless actual Pilot data flows include Customer Personal Data. If so, complete and approve this entire Cover Page and the security gate BEFORE transferring that data.

1. Activation and underlying agreement

Field	Agreed or customer-specific content
Underlying Agreement	OMEGANEON Paid Pilot Agreement Order Form between Omeganeon LLC and [CUSTOMER], effective [DATE], with Pilot SOW Exhibit A [ID].
Status	[ ] NOT APPLICABLE — synthetic/anonymized data only (confirm logs/account data) [ ] APPLICABLE — completed DPA activated before personal data handling
Provider security contact	support@omeganeonhq.com
Customer role	[CONTROLLER / PROCESSOR]; OMEGANEON role [PROCESSOR / SUBPROCESSOR] as applicable
Hosting / location	[CLOUD PROVIDER / TENANT / REGION / SUPPORT REGIONS]
Subprocessors	Only named, approved providers listed below may process Personal Data.
Source standard terms	Common Paper Data Processing Agreement Standard Terms v1.1: https://commonpaper.com/standards/data-processing-agreement/1.1/ (incorporated by reference when DPA activated).

2. Approved Subprocessors

Legal provider / subprocessors	Country / processing regions	Purpose / personal-data scope	Approved by Customer
[CLOUD / MODEL / LOGGING VENDOR]	[ ]	[ ]	[DATE / SIGNATURE]
[ ]	[ ]	[ ]	[ ]

A new or replacement subprocessor requires advance written notice of at least ten (10) Business Days and an opportunity to object within thirty (30) calendar days; that subprocessor may not receive Customer Personal Data until earlier express written approval or the objection window ends without objection, subject to applicable law. For a short Pilot, pre-approval at signature is preferred.

3. Annex I / Processing profile

Category	Completed information
Data subjects	[CUSTOMER TEAM MEMBERS / BUSINESS CONTACTS / END USERS—LIST]
Personal data	[NAME / CONTACT / SYSTEM IDENTIFIERS / LOGS; DO NOT INCLUDE SENSITIVE DATA WITHOUT SPECIAL APPROVAL]
Special-category data	DEFAULT NONE. Exception only after signed amendment describing explicit safeguards.
Nature / purpose	[LIMITED SANDBOX EVALUATION / AUTHORIZED

Category	Completed information
	WORKFLOW TESTING / SECURITY LOGS]
Frequency	[EVENT-TRIGGERED / SCHEDULED / CONTINUOUS]
Duration	Only for documented Pilot purpose, with content return/deletion within 30 calendar days following Pilot expiration/termination, except valid legal or agreed backup exceptions.
Exporting / importing parties	Customer: [LEGAL NAME / PHYSICAL ADDRESS / REPRESENTATIVE / ROLE]. OMEGANEON: [PHYSICAL ADDRESS IF REQUIRED / REPRESENTATIVE / ROLE].
Restricted transfers	[EEA / UK / SWISS? WHICH COUNTRIES / MODULE / SCC + UK ADDENDUM IF REQUIRED]. Do not assume US-only without review.

4. Security, retention and incident provisions

Annex II security. The agreed sandbox controls are those actually implemented, verified, and evidenced in Exhibit D before personal-data access. No SOC 2, ISO or independent audit certification is represented.

DPA §5.2 replacement. Provider does not represent that it is regularly audited by independent third-party security auditors or that it holds SOC 2 / ISO certifications. On reasonable confidential written request, Provider will share security information that actually exists and may lawfully be shared. In §5.3, “In addition to the Report” is replaced with “In lieu of an independent security Report when none exists”.

Records / §5.1. Provider will preserve DPA compliance evidence for three (3) years after the DPA terminates as in the Common Paper Standard Terms; this does not authorize retention of Customer raw personal data for three years. Implement before any covered Pilot access to Customer Personal Data.

Incident notification / §4. Notify Customer without undue delay and no later than 72 hours after awareness of a defined Security Incident, as required by applicable DPA terms. Customer incident contact: [CONTACT / EMAIL].

Data return / deletion / §7. Pilot sandbox Customer Content is returned/deleted as soon as reasonably practicable, not later than 30 calendar days after Pilot end under documented Customer instruction, subject to mandatory legal retention and proportionate backup exceptions. Minimal audit metadata may be retained for the distinct 90-day period only if it does not improperly preserve data subject content and complies with applicable law and Customer instructions.

Liability / §8. Pilot Order Form aggregate General Cap is $4,000 between the parties to the maximum extent permitted; it does not waive data-subject rights or liabilities that may not be capped under applicable restricted-transfer obligations or other law.

5. DPA approval / effect

When selected as APPLICABLE, this completed Exhibit B and the fixed Common Paper DPA Standard Terms v1.1 form the DPA under the Pilot Agreement. The Pilot Order Form expressly incorporates Exhibit B, and any legally required transfer annexes and approved subprocessor list must be completed before processing.

OMEGANEON	Customer
Authorized: [NAME/TITLE/DATE]	Authorized: [NAME/TITLE/DATE]

Source: Common Paper DPA Standard Terms v1.1, https://commonpaper.com/standards/data-processing-agreement/1.1/. Licensed CC BY 4.0. OMEGANEON adaptations are on this Cover Page and are not endorsed by Common Paper.

EXHIBIT C / PILOT AI SERVICES

PILOT AI ADDENDUM

Adaptation of Common Paper AI Addendum Standard Terms v1.0 to the independent Pilot Agreement

This Pilot attachment intentionally references the Pilot Agreement, NOT the Production PSA. AI use is limited to the one agreed sandbox workflow and evaluation activities in Exhibit A.

1. Agreement and AI service definition

Item	Pilot-specific cover page
Underlying Agreement	OMEGANEON Paid Pilot Agreement between Omeganeon LLC and [CUSTOMER], effective [DATE], and Pilot SOW Exhibit A [ID].
AI Services / Product	AI model-assisted configuration, execution and measurement of ONE authorized sandbox workflow only, including the defined evaluation report. No general software subscription or production license.
Hosted / BYOC	OMEGANEON-hosted sandbox default; any BYOC Pilot exception must be identified in Exhibit A. Actual model provider and data-processing region: [NAME / REGION].
AI API costs	Included in the $4,000 fixed Pilot Fee for the written scope; no automatic token, call or cloud overage invoices.
Model training	None permitted by default. No training on Input/Output/Customer Content without separate prior written authorization detailing model/vendor, dataset, purpose and safeguards.
Non-training improvements	No generalized product improvement or cross-customer reuse of Customer Input, Output, non-public Feedback, Customer Content or Confidential Information. Limited operational telemetry only for service, security or legal duties.
AUP	Unified AUP v1.4 (issued November 19, 2026) applies when expressly incorporated into or attached to this Pilot Agreement.
Source standard terms	Common Paper AI Addendum v1.0: https://commonpaper.com/standards/ai-addendum/1.0/ (incorporated by reference with express amendments herein).

2. Ownership and permitted activity

Input and standalone Output. Customer retains rights in its Input and, to the extent legally protectable and assignable, standalone AI Output arising from authorized Customer tasks. Neither party represents all output is copyrightable or exclusively owned.

Pilot prototype. Provider exclusively retains the prototype workflow, reusable code, EDGEPORT, components, systems, methods, templates and configuration know-how. Customer receives temporary evaluation-only access during authorized Pilot and acceptance review; no permanent license to operate the prototype in production or right to underlying source code.

Reports. Customer obtains its customer-specific final evaluation, measurement and Acceptance Reports, subject to Provider background tools and third-party rights. No permission to publish identifiable cases absent separate written approval.

Execution restrictions. Agent actions comply with the six APB primitives (System, Data, Action, Limit, Duration, Identity), least privilege and risk-tiered HITL as defined in Exhibit D and Exhibit A. No destructive, financial, external-facing or production write without separate explicit preapproval; production is outside scope.

3. AI output risk, liability and precedence

Common Paper AI Addendum Standard Terms §§3.1–3.2 acknowledge AI inaccuracies and potentially similar outputs. No blanket standalone AI Output non-infringement warranty or indemnity is provided. Provider remains obliged to submit the specified Pilot deliverables to measurable acceptance review. Pilot Agreement §5 and the $4,000 General Cap govern contractual liability to the extent lawful; DPA, SCC/UK transfer obligations and statutory rights prevail where mandatory.

The Pilot Order Form, this Exhibit C and Exhibit B (if effective) supersede conflicting defaults in Standard Terms only for their specific subject matters. AUP governs customer conduct but cannot introduce new fee, data training permission or warranty. No production PSA or SOW automatically results.

4. Incorporation

This Exhibit C is adopted only through the completed Pilot Order Form that expressly names the attachment and fixed Common Paper AI Addendum Standard Terms v1.0. The underlying Standard Terms were designed primarily for CSA/software license agreements; these Pilot-specific definitions and ownership provisions are deliberate adaptations.

Source: Common Paper AI Addendum v1.0, https://commonpaper.com/standards/ai-addendum/1.0/. CC BY 4.0; adapted for OMEGANEON Pilot; not endorsed by Common Paper.

EXHIBIT D / SANDBOX SECURITY CONTROLS

PILOT SANDBOX SECURITY SCHEDULE

Stage-specific: isolated evaluation sandbox • no production approval • verification required before Customer access

PLANNED CONTROLS ARE NOT CURRENT CERTIFICATIONS. The controls listed below are contract requirements / entry gates. OMEGANEON must implement and record actual evidence before connecting to any Customer-controlled system or handling Customer-provided data. Do not check “verified” until observed.

1. Controlled Sandbox boundaries

Only one workflow and approved test systems in Exhibit A; default synthetic/properly anonymized datasets. Pilot must not execute real production decisions, unrestricted writes, transfers, destructive changes or external communications. Any permission expansion requires written Customer authorization and updated APB/approval matrix.

A documented environment inventory shall identify [CLOUD PROVIDER / ACCOUNT / REGION / TENANT ID / SANDBOX NETWORK ISOLATION / MODEL PROVIDER / SUPPORT REGION]. A Pilot sandbox is not a certified Production environment.

2. Entry-gate security controls & verification log

Control	Minimum Pilot requirement / evidence	Status / evidence
APB (6 primitives)	Identity + System + Data + Action + Limit + Duration enforced in sandbox; rejected out-of-scope test recorded.	[NOT TESTED / VERIFIED / DATE / EVIDENCE]
Human approvals	Risk-ranked approvals; high-impact/external writes blocked by default and approved only by named customer contact.	[ ]
Access & MFA	Least privilege for operators, no shared privileged credentials; MFA on supported admin access, approved role roster.	[ ]
Sandbox isolation	Separate test boundaries; no live production writes or uncontrolled cross-tenant access; denied-access evidence.	[ ]
Encryption & secrets	Encrypt transit and stored customer content; secrets in managed secret storage, never in logs/docs.	[ ]
Action / approval audit	Minimal logs of approvals, identity, outcome, time and permission decision; default 90-day configurable retention with personal-content minimization.	[ ]
Backup / recovery	Backup and recovery only when data persistence and agreed SOW require it; evidence of restore or approved ephemeral strategy.	[ ]
Deletion / return	Record sandbox content inventory, deletion/return method, 30-day deadline, exception register.	[ ]
Incident response	Document contacts, alerting, escalation and if DPA applies no-undue-delay /	[ ]

Control	Minimum Pilot requirement / evidence	Status / evidence
	<=72h customer notification mechanism.	

3. Personal data, audit logs and data exit

Default NO Customer Personal Data. If actual Personal Data is proposed, execution must pause until: (i) the parties sign the specific use-case and permitted data categories, (ii) a completed Pilot DPA Exhibit B is activated, (iii) relevant processor/model vendors and restricted transfers are approved, and (iv) verified applicable security safeguards are recorded here.

Operational action logs: 90 days by default, customer-configurable as documented. Logs should contain minimal action metadata rather than raw prompts, tokens, credentials or confidential business records. Customer sandbox content: return/delete within 30 days after expiration/termination; any audit record containing personal data must comply with the DPA and deletion instructions, not simply be retained 90 days without a valid basis. DPA compliance evidence, if applicable, may have a separate 3-year duty.

4. Sandbox exit & production handoff

At Pilot end: revoke grants, disable prototype access, handle controlled acceptance access as provided in Exhibit A, export authorized results to Customer, and complete scheduled deletion; document any exceptions. Passing the Pilot does NOT constitute Production Go-Live approval or establish the full security baseline required under the separate Production PSA/SOW.

Security evidence reviewer: [NAME/ROLE]; Customer security contact: [NAME/EMAIL]; Last verified [DATE]; Material gaps [LIST]; Customer exceptions approved by [NAME/DATE]; No unapproved waivers of mandatory legal controls.

EXHIBIT E / UNIFIED CONDUCT POLICY

AI ACCEPTABLE USE POLICY

v1.4 Unified Public Policy • Paid Pilot and Production PSA/SOW

Version: 1.4 — Unified Public Policy

Issued: November 19, 2026

Contractual Effective Date: For each Customer, when this version is expressly incorporated into an executed Pilot Agreement or Professional Services Agreement, or separately accepted in writing.

Contact: support@omeganeonhq.com

1. Scope and application

This AI Acceptable Use Policy ("AUP") governs how a customer ("Customer") and its authorized users may use AI-enabled workflow services ("AI Services") provided by Omeganeon LLC ("OMEGANEON") under either (a) an executed Paid Pilot Agreement with its Pilot Statement of Work ("Pilot SOW"), or (b) an executed Professional Services Agreement ("PSA") with its production Statement of Work ("Production SOW"). The relevant signed contract, its applicable SOW and incorporated schedules are together the "Agreement". "SOW" in this policy means the applicable Pilot SOW or Production SOW.

This AUP primarily establishes Customer and authorized-user conduct requirements. OMEGANEON's delivery, sandbox or production security implementation, data protection, intellectual-property and commercial obligations are governed by the applicable Agreement, its Security Schedule, the Data Processing Agreement ("DPA") if applicable, and the AI Addendum. This AUP does not expand OMEGANEON's authorized system or data access.

2. Permitted use and Customer responsibilities

Customer and its authorized users may use AI Services for lawful business purposes within the agreed SOW, approved systems and Agent Permission Boundaries ("APB"). For a Pilot, authorized purposes are limited to the agreed controlled-sandbox evaluation; production use is not authorized by a Pilot Agreement. Customer is responsible for lawful instructions and supplied materials, data-use rights, required notices and consents, authorized users and approvers, and permissions for connected systems under its control.

Customer must designate authorized administrators and approvers, safeguard credentials and promptly revoke or adjust access when authorizations end or roles change.

Customer may request expanded systems, data, actions or limits through the agreed approval/change-control procedure. A lawful request for additional permissions is not itself a violation of this AUP. No requested permission takes effect before approval and technical implementation.

3. Prohibited use

Customer and authorized users must not:

- Access, extract, alter or disclose data or systems beyond approved scope, including information of another customer.
- Circumvent APB, identity controls, multi-factor authentication, required Human-in-the-Loop ("HITL") review, usage limits, monitoring or audit logging.
- Introduce malicious code, conduct unauthorized intrusion/security testing, disrupt services, engage in fraud or unlawful discrimination, or otherwise violate applicable law using AI Services.
- Submit data, credentials, prompts, media or materials without the rights and permissions necessary for intended use.
- Use AI Services for regulated or consequential decisions without required human review; conduct real-world production operations during a sandbox-only Pilot.

- Misrepresent AI-generated material as human-created where prohibited by law or the AI Addendum.

These restrictions do not prohibit lawful requests for additional permissions through an approved process.

4. Agent Permission Boundaries and human approval

Every agent action must remain within six APB dimensions: System (where), Data (what), Action (which operation), Limit (bounds), Duration (when) and Identity (whose authority). No user or agent may self-expand these permissions.

HITL is risk-tiered. Approved routine actions may run automatically within established APB. High-risk, destructive, irreversible, financial or externally consequential operations require human approval when designated in the SOW or Security Schedule; legally mandated human review always applies. Sandbox Pilot workflows must not bypass restrictions on production writes or live external actions.

Customer must identify authorized approvers and follow the agreed decision process. OMEGANEON's implementation duties are in the applicable Security Schedule.

5. Customer data, sensitive information and model training

Customer retains its Input rights and legally existing rights in AI Output. Prototype ownership and temporary Pilot evaluation rights, and production Deliverable assignment after payment where applicable, are defined in the relevant Agreement and AI Addendum. This AUP makes no IP assignment.

The standard service scope excludes special-category personal data, health records, banking credentials and comparable high-risk information unless categories, purposes and safeguards are expressly approved in the applicable SOW and DPA. A Pilot uses synthetic or properly anonymized sandbox data by default. Customer must not introduce Customer Personal Data into a Pilot until the parties have activated the necessary DPA and security controls.

Acceptance of this AUP does not authorize OMEGANEON or model vendors to train on Customer Input, Output or Customer Content. Training exceptions require prior express written authorization specifying vendor/model, data, purposes and safeguards. Customer Input, Output and non-public Customer Materials are not authorized for general product improvement or cross-client reuse.

Permitted limited service telemetry, deletion and lawful retention are governed by the applicable Agreement, DPA, AI Addendum and SOW, not this AUP.

6. Deployment and approved third parties

OMEGANEON-Hosted Cloud (default). OMEGANEON operates the hosting environment and service-side model connections within the agreed scope. A Pilot is a controlled sandbox, not production. Customer authorizes necessary connected-system actions and retains authority over its business instructions and approvals.

Bring Your Own Cloud (BYOC; optional add-on). BYOC applies only when expressly selected in the relevant SOW. Customer controls its cloud account and delegates only the access needed for contracted services; a sandbox-only Pilot remains limited to evaluation.

Actual vendors, regions, tenant isolation, credentials and approved subprocessors are specified in the SOW, DPA or related schedules. All pricing, cloud and AI API usage charges and Change Orders are governed by the applicable Pilot Agreement or PSA/SOW; this AUP imposes no separate fees or automatic usage overages.

7. Security requirements and audit records

Customer and authorized users must not bypass or interfere with required security controls and must cooperate with identity checks, approval procedures, access revocation and security investigations.

The applicable Pilot Sandbox Security Schedule or Production Security Schedule, together with the DPA and SOW when applicable, defines OMEGANEON's safeguards, verification gates, audit-log retention, customer access, backup, recovery and deletion duties. A Pilot's sandbox controls do not imply that production requirements have

been satisfied. Contractually required controls must be implemented and verified before the relevant system or data access, and before Production Go-Live where applicable. Merely listing a control is not a claim that it is operational today.

8. Reporting misuse and responding to security risks

Customer must promptly report suspected misuse, unauthorized agent actions, compromised credentials or security concerns to support@omeganeonhq.com and reasonably assist in containment.

Where an action or workflow creates an active security or misuse risk, OMEGANEON may temporarily restrict the affected action or permission only as authorized by the signed Agreement. Such restriction must be properly scoped, no broader than reasonably necessary, and subject to applicable notice and restoration procedures.

This AUP does not authorize seizure, withholding or deletion of Customer data, unrelated service shutdown or override of lawful customer access. Security incident response and notification duties are governed by the Agreement, DPA and Security Schedule.

9. Version control, changes and precedence

This AUP is version 1.4, issued November 19, 2026. For each Customer, only the version expressly incorporated into its executed Agreement or separately accepted in writing applies. OMEGANEON may publish future versions for new engagements; website posting alone does not amend an existing Pilot Agreement or PSA. Material changes require the respective Agreement's written amendment process. Previous accepted policy versions remain applicable unless validly amended and shall be retained for reference.

If provisions conflict, mandatory law and restricted-transfer clauses control to the extent required; the applicable DPA governs personal-data processing; the AI Addendum governs AI-specific rights; and the Pilot Agreement or PSA/SOW governs its own legal, delivery and commercial subjects, subject to express amendments. This AUP creates no new fees, model-training permissions, IP assignments, warranties or indemnities.

Version history: v1.4 is the policy version approved for new engagements beginning November 19, 2026. Previously accepted versions, including v1.3, remain effective for those Customers unless validly amended. Publication on the website is separate from contractual adoption.

REFERENCE APPENDIX / COMMON PAPER

PILOT AGREEMENT STANDARD TERMS v1.1

Original Common Paper source text reproduced for review. The Order Form above expressly amends identified provisions. The unmodified Standard Terms version is fixed at the source URL below.

1. Pilot Access

1.1 Access and Use. During the Pilot Period and subject to the terms of this Agreement, Customer may access and use the Product solely for Customer's Evaluation Purposes.

1.2 License. If the Product contains Software, then, during the Pilot Period and subject to the terms of this Agreement, Provider grants Customer a limited, non-exclusive, non-sublicensable, non-transferable license to install and use such Software on systems owned or controlled by Customer solely for Customer's Evaluation Purposes.

1.3 User Accounts. Customer is responsible for all actions on Users' accounts and for all Users' compliance with this Agreement. Customer and Users must protect the confidentiality of their passwords and login credentials. Customer will promptly notify Provider if it suspects or knows of any fraudulent activity with its accounts, passwords, or credentials, or if they become compromised.

1.4 Customer Content. Provider may copy, display, modify, and use Customer Content only as needed to provide and maintain the Product and related offerings. Customer is responsible for the accuracy and content of Customer Content.

1.5 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, enhance, and promote Provider's products and services without restriction or obligation. However, Provider may only disclose Usage Data to others if the Usage Data is aggregated and does not identify Customer or Users.

1.6 Restrictions. Except as expressly permitted by this Agreement, Customer will not (and will not allow anyone else to): (i) reverse engineer, decompile, or attempt to discover any source code or underlying ideas or algorithms of the Product (except to the extent Applicable Laws prohibit this restriction); (ii) provide, sell, transfer, sublicense, lend, distribute, rent, or otherwise allow others to access or use the Product; (iii) remove any proprietary notices or labels; (iv) copy, modify, or create derivative works of the Product; (v) conduct security or vulnerability tests on, interfere with the operation of, cause performance degradation of, or circumvent access restrictions of the Product; (vi) access accounts, information, data, or portions of the Product to which Customer does not have explicit authorization; (vii) use the Product to develop a competing service or product; (viii) use the Product with any High Risk Activities or with any activity prohibited by Applicable Laws; (ix) use the Product to obtain unauthorized access to anyone else's networks or equipment; or (x) upload, submit, or otherwise make available to the Product any Customer Content to which Customer and Users do not have the proper rights.

1.7 Reservation of Rights. Except for the limited license to install and use Software in Section 1.2 (License), Provider retains all right, title, and interest in and to the Product, whether developed before or after the Effective Date. Except for the limited rights in Section 1.4 (Customer Content), Customer retains all right, title, and interest in and to the Customer Content.

2. Term & Termination

2.1 Agreement. The Agreement will start on the Effective Date and, unless terminated earlier according to the terms of this Agreement, will continue through the Pilot Period.

2.2 Termination. Either party may terminate the Agreement immediately:

(a) if the other party fails to cure a material breach of the Agreement following 30 days notice;

(b) upon notice if the other party (i) materially breaches the Agreement in a manner that cannot be cured; (ii) dissolves or stops conducting business without a successor; (iii) makes an assignment for the benefit of creditors; or (iv) becomes the debtor in insolvency, receivership, or bankruptcy proceedings that continue for more than 60 days; or

(c) for any or no reason following 30 days notice to the other party.

2.3 Effect of Termination. If the parties do not have a Definitive Agreement, then upon the expiration or termination of this Agreement:

(a) Customer will no longer have any right to use the Product. If the Product contains Software, Customer will immediately and permanently uninstall or delete all such Software and will certify to Provider that Customer has complied with this obligation.

(b) Upon Customer's request, Provider will delete Customer Content within 60 days.

(c) Each Recipient will return or destroy Discloser's Confidential Information in its possession or control.

2.4 Survival.

(a) The following sections will survive expiration or termination of the Agreement: Section 1.5 (Feedback and Usage Data), Section 1.6 (Restrictions), Section 1.7 (Reservation of Rights), Section 2.3 (Effect of Termination), Section 2.4 (Survival), Section 3 (Representations), Section 4 (Disclaimer of Warranties), Section 5 (Limitation of Liability), Section 6 (Confidentiality), Section 7 (General Terms), Section 8 (Definitions), and the portions of an Order Form 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 6 (Confidentiality) will continue to apply to retained Confidential Information.

3. Representations

3.1 Each party represents to the other that: (a) it has the legal power and authority to enter into this Agreement; and (b) it is duly organized, validly existing, and in good standing under the Applicable Laws of the jurisdiction of its origin.

4. Disclaimer of Warranties

4.1 Provider makes no guarantees that the Product will always be safe, secure, or error-free, or that it will function without disruptions, delays, or imperfections. The Product is provided on an "AS IS" and "AS AVAILABLE" basis. Provider disclaims all warranties and conditions, whether express or implied, including the implied warranties and conditions of merchantability, fitness for a particular purpose, title, and non-infringement. These disclaimers apply to the maximum extent permitted by Applicable Laws.

5. Limitation of Liability

5.1 General Liability Cap. Each party's total cumulative liability for all claims arising out of or relating to this Agreement will not be more than the General Cap Amount.

5.2 Damages Waiver. Except for a breach of Section 6 (Confidentiality), under no circumstances will either party be liable to the other for lost profits or revenues (whether direct or indirect), 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.

5.3 Applicability. The limitations and waivers contained in Sections 5.1 (General Liability Cap) and 5.2 (Damages Waiver) apply to all liability, whether in tort (including negligence), contract, breach of statutory duty, or otherwise. However, nothing in this Agreement will limit, exclude, or restrict a party's liability to the extent prohibited by Applicable Laws.

6. Confidentiality

6.1 Non-Use and Non-Disclosure. Except as otherwise authorized in the Agreement or as needed to fulfill its obligations or exercise its rights under this Agreement, Recipient will not (a) use Discloser's Confidential Information; nor (b) 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.

6.2 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.

6.3 Required Disclosures. Recipient may disclose Discloser's Confidential Information to the extent required by Applicable Laws if, unless prohibited by Applicable Laws, Recipient provides Discloser reasonable advance notice of the required disclosure and reasonably cooperates, at Discloser's expense, with Discloser's efforts to obtain confidential treatment for the Confidential Information.

6.4 Permitted Disclosures. Recipient may disclose Discloser's Confidential Information to Users, 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 6 (Confidentiality) and Recipient remains responsible for everyone's compliance with the terms of this Section 6 (Confidentiality).

7. General Terms

7.1 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. No terms or conditions in any Customer documentation or online vendor portal will apply to Customer's use of the Product unless expressly agreed to in a legally binding written agreement signed by an authorized Provider representative, regardless of what such terms may say.

7.2 Modifications, Severability, and Waiver. Any waiver, modification, or change to the Agreement must be in writing and signed or electronically accepted by each party. 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.

7.3 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 in the Chosen Courts and each party irrevocably submits to the exclusive jurisdiction of the Chosen Courts.

7.4 Injunctive Relief. Despite Section 7.3 (Governing Law and Chosen Courts), a breach of Section 6 (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 6 (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.

7.5 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.

7.6 Assignment. Neither party may assign any rights or obligations under this Agreement without the prior written consent of the other party. However, Provider may assign this Agreement upon notice if Provider 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.

7.7 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.

7.8 Taxes. Customer is responsible for all duties, taxes, and levies that apply to any Fees paid under this Agreement, 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.

7.9 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.

7.10 No Third-Party Beneficiary. There are no third-party beneficiaries of this Agreement.

7.11 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.

7.12 Titles and Interpretation. Section titles are for convenience and reference only. All uses of "including" and similar phrases are non-exhaustive and without limitation. The United Nations Convention for the International Sale of Goods and the Uniform Computer Information Transaction Act do not apply to this Agreement.

7.13 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.

8. Definitions

8.1 Defining Variables. Variables have the meanings or descriptions given on the Order Form. However, if the Order Form omits or does not define a Variable, the default meaning will be "none" or "not applicable" and the correlating clause, sentence, or section does not apply to that Agreement.

8.2 "Agreement" means the Order Form, including between Provider and Customer.

8.3 "Applicable Laws" means the laws, rules, regulations, court orders, and other binding requirements of a relevant government authority that apply to or govern Provider or Customer.

8.4 "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 the Order Form. Customer's

Confidential Information includes non-public Customer Content and Provider's Confidential Information includes non-public information about the Product.

8.5 "Customer Content" means data, information, or materials submitted by or on behalf of Customer or Users to the Product but excludes Feedback.

8.6 "Definitive Agreement" means a separate, mutually agreed agreement between Provider and Customer for longer-term access to the Product.

8.7 "Discloser" means a party to this Agreement when the party is providing or disclosing Confidential Information to the other party.

8.8 "Evaluation Purposes" means the internal use of the Product solely to test and evaluate the Product to determine whether to enter into a Definitive Agreement with Provider.

8.9 "Feedback" means suggestions, feedback, or comments about the Product or related offerings.

8.10 "Fees" means the applicable amounts described in an Order Form.

8.11 "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 disasters like a major earthquake, war, pandemic, riot, act of terrorism, or public utility or internet failure.

8.12 "High Risk Activity" means any situation where the use or failure of the Product could be reasonably expected to lead to death, bodily injury, or environmental damage. Examples include full or partial autonomous vehicle technology, medical life-support technology, emergency response services, nuclear facilities operation, and air traffic control.

8.13 "Order Form" means a document that is signed or electronically accepted by the parties, incorporates these Standard Terms, and Provider and Customer, and includes the key business details and Variables for this Agreement. An Order Form includes and incorporates by reference the policies and documents referenced in or attached to the Order Form.

8.14 "Product" means the product described in the Order Form.

8.15 "Recipient" means a party to this Agreement when the party receives Confidential Information from the other party.

8.16 "Software" means the client-side software or applications made available by Provider for Customer to install, download (whether onto a machine or in a browser), or execute as part of the Product.

8.17 "Standard Terms" means these Common Paper Pilot Agreement Standard Terms Version 1.1, which are posted at https://commonpaper.com/standards/pilot-agreement/1.1.

8.18 "User" means any individual who uses the Product on Customer's behalf or through Customer's account.

Common Paper Pilot Standard Terms (v1.1) are licensed under CC BY 4.0, as indicated at https://commonpaper.com/standards/pilot-agreement/1.1/. Reproduced for convenience; controlling source is the fixed official version incorporated by the Order Form.