03 / DATA PROTECTION

Data Processing Agreement

OMEGANEON Public Sample v1.5 | Common Paper DPA Standard Terms v1.1 | Schedule B

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

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 the actual data-processing chain. OMEGANEON is Processor or Subprocessor as applicable. Hosted Cloud is the default service configuration; cloud account ownership does not decide legal processing roles.
Approved Subprocessors	Only Customer-approved cloud, AI/model and other vendors expressly listed in the completed Subprocessor Schedule may process Customer Personal Data. The selected cloud and AI provider(s), processing regions, data categories and functions are engagement-specific. No vendor is approved solely by publication of this sample. BYOC does not automatically determine Processor/Subprocessor status.
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.

Execution: When attached to an Integrated Engagement document, the signed Integrated Cover Page is intended to constitute acceptance of this completed DPA Cover Page. As a standalone DPA, parties must execute an appropriate DPA Cover Page separately. When using an integrated signature, every incorporated cover and applicable schedule must be expressly identified and included.

REFERENCE APPENDIX — Common Paper Standard Terms

Common Paper DPA Standard Terms v1.1 reproduced under CC BY 4.0. The express amendment in the DPA Cover Page supersedes Standard Terms §5.2 concerning independent security audits. The completed transaction-specific annexes form part of the customer agreement when executed.

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 13 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.