

# **MASTER SERVICES AGREEMENT**

**This Master Services Agreement** (this **“Agreement”**) is entered into by and between **Wolfia, Inc.** (“**Wolfia**”), and the customer entity(“**Customer**”), and is effective as of the **Effective Date** (defined below). This Agreement governs Customer’s access to and use of Wolfia’s cloud-based artificial intelligence agent and related services (the **“Cloud Service”**). This Agreement is incorporated by reference into, and governs, each **Order Form** (defined below) executed by the parties.

**Effective Date.** The Effective Date is the latest date of signature on this Agreement or, if first referenced by an executed Order Form, the latest date of signature on that Order Form.

## 1. DEFINITIONS

1.1 **Affiliate** means any entity that directly or indirectly controls, is controlled by, or is under common control with a party, where “control” means ownership of more than 50% of the voting interests of such an entity.

1.2 **Authorized Users** means employees, contractors, and other individual users acting for Customer’s benefit who are provisioned by or on behalf of Customer to access the Cloud Service.

1.3 **Customer Content** means data, files, documents, questions, prompts, and other content that Customer (or its Authorized Users) submits to, stores on, or transmits through the Cloud Service, including content ingested via integrations (e.g., Confluence, OneDrive, Slack, Google Drive, Gong, websites, and email), but excluding Service Data and Output.

1.4 **Documentation** means Wolfia’s user guides, policies, technical documentation, and usage guidelines for the Cloud Service made available by Wolfia to Customer.

1.5 **Order Form** means an ordering document executed by the parties that references this Agreement and specifies the subscription start date and term, plan/tier and included features and limits, applicable fees and invoicing/payment terms, any referenced exhibits (e.g., SLA, DPA, SOW), renewal terms, and any expressly agreed special terms.

1.6 **Output** means content generated by or returned from the Cloud Service in response to Customer prompts or inputs.

1.7 **Service Data** means data about the configuration, environment, logs, telemetry, analytics, and other operational or technical data generated from use of the Cloud Service (e.g., usage volumes, feature adoption, performance metrics) that does not include Customer Content except in de-identified or aggregated form.

1.8 **SLA** means the service level agreement attached as \*\*Exhibit A\*\*, including any uptime commitments and support response targets.

1.9 **DPA** means the data processing addendum attached as \*\*Exhibit B\*\*, including any applicable standard contractual clauses and security exhibits.

1.10 **Third-Party Services** means products, services, platforms, data sources, or AI/LLM providers not provided by Wolfia that interoperate with, or are used in connection with, the Cloud Service (e.g., Slack, Salesforce, Google, Gong, etc).

1.11 **Beta Features** means pre-release, preview, alpha, or beta features or services identified as such by Wolfia.

## 2. ACCESS; LICENSE; RESTRICTIONS

2.1 **Access Grant.** Subject to this Agreement and an applicable Order Form, Wolfia grants Customer a non-exclusive, non-transferable, non-sublicensable right for its Authorized Users to access and use the Cloud Service during the Subscription Term solely for Customer’s internal business purposes.

2.2 **Use and Fair Use.** Customer’s access includes the features and limits enabled for Customer’s tenant as stated in the Order Form. “Unlimited” features (e.g., questions, questionnaires, knowledge base) are subject to reasonable/fair use aligned with normal enterprise usage and may not materially degrade the Cloud Service for other customers. If usage materially exceeds fair use, Wolfia may recommend plan adjustments or temporarily rate‑limit abusive processes after notifying Customer and working in good faith to remediate. Unless expressly stated in the Order Form, Customer may provision an unlimited number of Authorized Users, subject to reasonable/fair use.

2.3 **Customer Responsibilities.** Customer is responsible for: (a) the configuration of the Cloud Service and integrations; (b) the accuracy, content, and legality of Customer Content; (c) obtaining all rights and consents necessary to submit Customer Content and to enable interoperation with Third‑Party Services; and (d) all activities under its accounts. Customer will use commercially reasonable efforts to prevent unauthorized access and will promptly notify Wolfia of any unauthorized use.

2.4 **Restrictions.** Customer will not (and will not permit any third party to): (a) reverse engineer, decompile, or attempt to derive the source code or underlying models of the Cloud Service (except to the extent such restriction is prohibited by law); (b) use the Cloud Service to develop competing products; (c) remove or obscure proprietary notices; (d) access the Cloud Service for benchmarking or competitive analysis without Wolfia’s prior written consent, except for Customer’s internal benchmarking that does not disclose Wolfia Confidential Information or benchmarking results to any third party; (e) interfere with or disrupt the integrity or performance of the Cloud Service; (f) use the Cloud Service to transmit malicious code or to infringe, misappropriate, or violate third‑party rights; or (g) use the Cloud Service in violation of the Documentation or any applicable laws (including export, privacy, and anti‑corruption laws).

2.5 **Third‑Party Services.** Customer’s use of Third‑Party Services is subject to their terms; Wolfia is not responsible for such services or for any disclosure, modification, or deletion of Customer Content by Third‑Party Services. Wolfia may enable integrations and connectors for Customer’s convenience; Customer is solely responsible for enabling, configuring, and maintaining such integrations.

2.6 **Beta Features.** Beta Features are provided for evaluation “as is,” without warranties or SLA commitments, and may be changed or discontinued at any time. Wolfia has no liability arising from Beta Features.

## 3. OWNERSHIP; AI OUTPUT; FEEDBACK

3.1 **Ownership.** As between the parties, (a) Customer retains all right, title, and interest in and to Customer Content; (b) Wolfia retains all right, title, and interest in and to the Cloud Service, Service Data, Documentation, and Wolfia’s technology, models, software, know‑how, and IP; and (c) each party retains ownership of its trademarks and branding.

3.2 **Output.** As between the parties, to the extent permitted by applicable law, Customer owns the Output generated for Customer from the Cloud Service. Customer is responsible for (a) evaluating the Output, including for accuracy and appropriateness; and (b) using human review and judgment before relying on Output for any consequential purpose. Wolfia disclaims responsibility for Output that results from instructions or data provided by Customer or Third‑Party Services.

3.3 **Usage to Provide and Improve the Service.** Wolfia may access and use Customer Content and Output solely to provide, secure, support, troubleshoot, maintain, and improve the Cloud Service for Customer (including quality assurance, de‑identification, and aggregation). Unless expressly permitted by the DPA or by Customer’s written consent, Wolfia will not use Customer Content to train foundation models that are made available to other customers.

3.4 **Feedback.** If Customer provides suggestions, ideas, or feedback regarding the Cloud Service, Wolfia may use such feedback without restriction and without obligation to Customer.

## 4. SECURITY; PRIVACY; DATA TRANSFERS

4.1 **Security.** Wolfia will implement and maintain administrative, physical, and technical safeguards designed to protect the security, confidentiality, and integrity of Customer Content, including encryption in transit and at rest, access controls, vulnerability management, and employee security training. Wolfia’s Privacy Policy is available at https://wolfia.com/privacy.

4.2 **Incident Response.** Wolfia will notify Customer without undue delay after confirming a Security Incident involving Customer Content in Wolfia’s possession, and will provide information reasonably available to Wolfia for Customer to meet its incident reporting obligations.

4.3 **DPA.** To the extent Customer Content includes Personal Data (as defined in the DPA), the DPA is incorporated into and forms part of this Agreement and governs Wolfia’s processing of such Personal Data as a processor/service provider on Customer’s behalf, including any applicable cross‑border transfer mechanisms (e.g., EU/UK standard contractual clauses).

4.4 **Subprocessors.** Customer authorizes Wolfia to engage subprocessors to support delivery of the Cloud Service. Wolfia will be responsible for its subprocessors’ performance and will impose data protection obligations consistent with this Agreement. Wolfia maintains a current list of subprocessors at [**https://trust.wolfia.com/?tab=subprocessors**](https://trust.wolfia.com/?tab=subprocessors) and will provide **advance notice of material changes** via that page or email.

## 5. SUPPORT; SERVICE LEVELS; PROFESSIONAL SERVICES

5.1 **Support.** During the Subscription Term, Wolfia will provide standard support in accordance with the Service Level Agreement (Exhibit A). If the Order Form includes 24×7 Slack support, Wolfia will use commercially reasonable efforts to respond to support inquiries submitted via the designated Slack channel.

5.2 **Service Levels.** Any uptime commitments and service credits are described in the Service Level Agreement (Exhibit A). Service credits (if any) are Customer’s sole and exclusive remedy for failure to meet applicable service levels.

5.3 **Professional Services.** If professional services (e.g., implementation, training, or consulting) are purchased, they will be described in an Order Form or statement of work (each, an SOW), and are provided on a time‑and‑materials or fixed‑fee basis, as specified. Customer will provide reasonable cooperation and access needed to perform such services.

## 6. FEES; INVOICING; TAXES

6.1 **Fees.** Customers will pay the fees set forth in each Order Form. Except as expressly stated in this Agreement or an Order Form, all fees are non‑cancellable and non‑refundable.

6.2 **Invoicing and Payment.** Unless otherwise stated in an Order Form, fees are invoiced in advance and due net thirty (30) days from receipt of an undisputed invoice. Late amounts may accrue interest at the lesser of 1.5% per month or the maximum rate permitted by law. Customer is responsible for reasonable costs of collection of past due amounts.

6.3 **Taxes.** Fees are exclusive of taxes. Customers are responsible for all sales, use, VAT, GST, and similar taxes (excluding taxes based on Wolfia’s income). If a customer provides a valid exemption certificate, Wolfia will not charge applicable taxes.

6.4 **Purchase Orders.** If a customer issues a purchase order, it is for administrative reference only. Any additional or conflicting terms on a purchase order or similar instrument are rejected and have no force or effect.

## 7. TERM; RENEWAL; SUSPENSION; TERMINATION

7.1 **Term.** This Agreement begins on the Effective Date and continues until terminated as provided herein. Each Order Form has the subscription term stated therein (the Subscription Term).

7.2 **Renewal.** Subscriptions renew as stated in the Order Form. Unless otherwise stated, subscriptions automatically renew for successive twelve (12) month terms at renewal fees that may increase by up to ten percent (10%) over the original price, unless otherwise agreed in the Order Form.

7.3 **Suspension.** Wolfia may suspend access to the Cloud Service immediately upon notice if: (a) Customer’s account is delinquent by more than fifteen (15) days; (b) Customer’s use poses a security risk, may harm the Cloud Service or others, violates law, or breaches Section 2; or (c) as reasonably necessary to prevent material harm, subject to prompt restoration upon remediation.

7.4 **Termination for Cause.** Either party may terminate this Agreement or an Order Form for material breach that remains uncured thirty (30) days after written notice (ten (10) days for non‑payment). Upon termination for Wolfia’s uncured material breach, Wolfia will refund prepaid fees covering the remainder of the terminated Subscription Term after the effective date of termination. Upon termination for Customer’s breach, all unpaid fees for the remainder of the Subscription Term become immediately due.

7.5 **Effect of Termination; Data Return/Deletion.** Upon expiration or termination of an Order Form, Customer’s right to access the Cloud Service under that Order Form will cease. For thirty (30) days after expiration or termination (the Data Retrieval Period), and upon Customer’s request, Wolfia will make available to Customer an export of Customer Content in a commercially reasonable format. After the Data Retrieval Period, Wolfia will delete Customer Content from active systems, subject to archival backups retained in accordance with Wolfia’s standard retention schedules.

## 8. CONFIDENTIALITY

8.1 **Definition.** “**Confidential Information**” means non‑public information disclosed by one party (the Discloser) to the other (the Recipient) that is identified as confidential or that should reasonably be understood to be confidential given the nature of the information and circumstances of disclosure, including product plans, security documentation, pricing, customer lists, business and marketing plans, technology and technical information, and the terms of this Agreement and any Order Form. Customer Content is Customer’s Confidential Information; Service Data is Wolfia’s Confidential Information.

8.2 **Obligations.** Recipient will (a) use Discloser’s Confidential Information solely to perform under this Agreement; (b) not disclose it to any third party except to its and its Affiliates’ employees, advisors, and subprocessors who have a need to know and are bound by confidentiality obligations no less protective than this Section; and (c) protect it using at least the same degree of care Recipient uses to protect its own similar information (and no less than reasonable care).

8.3 **Exclusions.** Confidential Information does not include information that: (a) is or becomes generally available to the public through no breach by Recipient; (b) was known to Recipient without confidentiality obligation before receipt; (c) is independently developed by Recipient without use of or reference to the Confidential Information; or (d) is rightfully received from a third party without confidentiality obligation.

8.4 **Compelled Disclosure.** Recipient may disclose confidential information to the extent required by law or court order, provided Recipient gives Discloser prompt written notice and reasonable cooperation to seek confidential treatment.

8.5 **Term.** The obligations in this Section apply during the term of this Agreement and for five (5) years thereafter; trade secrets are protected for as long as they remain trade secrets under applicable law.

## 9. WARRANTIES; DISCLAIMERS

9.1 **Mutual Warranties.** Each party represents and warrants that it has the legal power and authority to enter into this Agreement and that its performance will comply with applicable laws.

9.2 **Wolfia Warranties.** Wolfia warrants that during the applicable Subscription Term: (a) the Cloud Service will perform materially in accordance with the Documentation; and (b) Wolfia will not materially reduce the overall security of the Cloud Service.

9.3 **Remedies.** Customer’s exclusive remedies for breach of the warranties in Section 9.2 are: (a) repair or replacement of the non‑conforming Cloud Service; or (b) if Wolfia cannot remedy the non‑conformity within a reasonable time, termination and a refund of prepaid fees for the affected portion of the Subscription Term.

9.4 **Disclaimers.** EXCEPT AS EXPRESSLY PROVIDED IN THIS AGREEMENT, THE CLOUD SERVICE, OUTPUT, BETA FEATURES, AND ALL RELATED MATERIALS ARE PROVIDED “AS IS.” WOLFIA AND ITS SUPPLIERS DISCLAIM ALL OTHER WARRANTIES, EXPRESS OR IMPLIED, INCLUDING ANY IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE, AND NON‑INFRINGEMENT. AI‑GENERATED OUTPUT MAY BE INACCURATE OR INCOMPLETE; CUSTOMER IS RESPONSIBLE FOR INDEPENDENTLY VERIFYING OUTPUT BEFORE RELIANCE.

9.5 Wolfia may modify the Cloud Service from time to time, provided such changes do not materially reduce the core functionality purchased under the applicable Order Form.

## 10. INDEMNIFICATION

10.1 **By Wolfia.** Wolfia will defend Customer against any third‑party claim alleging that the Cloud Service, as provided by Wolfia and used by Customer in accordance with this Agreement, infringes any U.S. patent, copyright, or trade secret, and will pay any damages and reasonable attorneys’ fees finally awarded against Customer (or settlement amounts approved by Wolfia) arising out of such claim. If the Cloud Service is or is likely to become the subject of an infringement claim, Wolfia may, at its option and expense: (a) procure the right for Customer to continue using the Cloud Service; (b) replace or modify the Cloud Service so that it becomes non‑infringing without materially reducing its functionality; or (c) terminate the affected Order Form and refund prepaid fees for the remainder of the Subscription Term.

10.2 **Exclusions.** Wolfia’s obligations in Section 10.1 do not apply to claims arising from: (a) use of the Cloud Service in combination with products or services not provided by Wolfia; (b) modifications to the Cloud Service not made by Wolfia; (c) Customer Content, Third‑Party Services, or Output; or (d) use in violation of the Documentation or this Agreement.

10.3 **By Customer.** Customer will defend Wolfia against any third‑party claim arising from Customer Content, Customer’s use of the Cloud Service in violation of law or this Agreement, or any Third‑Party Services enabled by or for Customer, and will pay any damages and reasonable attorneys’ fees finally awarded against Wolfia (or settlement amounts approved by Customer) arising out of such claim.

10.4 **Procedure.** The indemnified party will: (a) promptly notify the indemnifying party in writing of any claim; (b) give the indemnifying party sole control of the defense and settlement of the claim (except that the indemnifying party may not settle any claim without the indemnified party’s prior written consent if it imposes any admission of liability or obligation on the indemnified party); and (c) provide reasonable assistance at the indemnifying party’s expense.

## 11. LIMITATIONS OF LIABILITY

11.1 **Limitation.** TO THE MAXIMUM EXTENT PERMITTED BY LAW, IN NO EVENT WILL EITHER PARTY’S AGGREGATE LIABILITY ARISING OUT OF OR RELATED TO THIS AGREEMENT EXCEED THE TOTAL AMOUNT PAID OR PAYABLE BY CUSTOMER UNDER THE APPLICABLE ORDER FORM DURING THE TWELVE (12) MONTHS IMMEDIATELY PRECEDING THE FIRST EVENT GIVING RISE TO THE LIABILITY.

11.2 **Exclusion of Consequential Damages.** NEITHER PARTY WILL BE LIABLE FOR ANY INDIRECT, INCIDENTAL, SPECIAL, CONSEQUENTIAL, COVER, EXEMPLARY, OR PUNITIVE DAMAGES, OR FOR ANY LOSS OF PROFITS, REVENUE, GOODWILL, OR DATA, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

11.3 **Exclusions.** The limitations in this Section do not apply to: (a) a party’s payment obligations; (b) liability for death or bodily injury caused by a party’s negligence; or (c) a party’s willful misconduct or fraud.

11.4 **Allocation of Risk.** The parties agree that the fees reflect the allocation of risk set forth in this Agreement and that the limitations in this Section are an essential basis of the bargain between the parties.

## 12. PUBLICITY

With Customer’s prior written consent (email sufficient), Wolfia may identify Customer as a customer and use Customer’s name and logo in customer lists and marketing materials. Any deeper case study or press release requires mutual written approval.

## 13. COMPLIANCE; EXPORT; ANTI‑CORRUPTION

Each party will comply with applicable laws, including applicable export control and sanctions laws. Customer represents it is not named on any U.S. government denied‑party list and will not permit access to the Cloud Service in violation of such laws. Each party will comply with anti‑bribery and anti‑corruption laws, including the U.S. FCPA and UK Bribery Act.

## 14. MISCELLANEOUS

14.1 **Order of Precedence.** In the event of a conflict, the following order of precedence applies: (1) the Order Form; (2) this Agreement; (3) the DPA and SLA; and (4) any SOWs and the Documentation. Terms on a purchase order do not apply. Notwithstanding the foregoing, for privacy and data-protection matters, the DPA will prevail over conflicting terms in the Order Form or the MSA.

14.2 **Notices.** Notices must be in writing and will be deemed given when sent by email to the contacts listed on the Order Form (or as later designated in writing), with a copy to legal@wolfia.com (for notices to Wolfia). Notices of breach, indemnification claims, or termination must also be sent by internationally recognized overnight courier to the physical addresses designated by the parties on the Order Form or via e‑signature platform notification.

14.3 **Assignment.** Neither party may assign this Agreement without the other party’s prior written consent, except that either party may assign this Agreement in connection with a merger, reorganization, acquisition, or sale of substantially all assets or voting securities, provided the assignee is not a direct competitor of the non‑assigning party and assumes all obligations.

14.4 **Independent Contractors.** The parties are independent contractors. This Agreement does not create a partnership, franchise, joint venture, agency, fiduciary, or employment relationship.

14.5 **Force Majeure.** Neither party will be liable for delays or failures to perform due to causes beyond its reasonable control (e.g., acts of God, war, terrorism, pandemics, labor disputes, failure of communications or hosting providers), provided the affected party uses reasonable efforts to mitigate.

14.6 **Governing Law; Venue.** This Agreement is governed by the laws of the State of Delaware, without regard to its conflicts of law rules. The parties consent to the exclusive jurisdiction and venue of the state and federal courts located in New Castle County, Delaware, for any dispute arising out of or relating to this Agreement, and waive any objection to jurisdiction and venue in such courts.

14.7 **Severability; Waiver.** If any provision is held unenforceable, it will be modified to the minimum extent necessary to make it enforceable, and the remaining provisions will remain in effect. A waiver of any provision on one occasion is not a waiver of any other provision or of the same provision on another occasion.

14.8 **Entire Agreement; Amendments.** This Agreement, together with the Order Form(s) and any DPA, SLA, and SOWs, constitutes the entire agreement between the parties regarding the subject matter hereof, and supersedes prior or contemporaneous agreements, proposals, or representations, written or oral. Amendments must be in writing and signed by both parties.

14.9 **Counterparts; Electronic Signatures.** This Agreement may be executed in counterparts (including by electronic or digital signature), each of which will be deemed an original and together constitute one instrument.

14.10 **Survival.** The following survive expiration or termination: §§2.4, 3, 4, 6 (to the extent amounts are owed), 8–11, 13–14, and Exhibit B.

## EXHIBITS

### Exhibit A — Service Level Agreement (SLA)

**1. Uptime Commitment.** Wolfia will use commercially reasonable efforts to make the production Cloud Service available 99% of each calendar month (the “Uptime Commitment”).

**2. Measurement.** Monthly Uptime Percentage = (Total Minutes − Downtime) ÷ Total Minutes. Downtime excludes: (a) Scheduled Maintenance; (b) emergency maintenance; (c) issues caused by Customer, third-party services, networks, or infrastructure not controlled by Wolfia; (d) Beta Features or trials; (e) force majeure events.

**3. Maintenance.** Wolfia may conduct Scheduled Maintenance with at least 24 hours’notice via the status page or email/Slack; emergency maintenance may occur without notice when necessary to address security or stability. Service status is available at [**https://status.wolfia.com/**](https://status.wolfia.com/).

**4. Service Credits.** If Monthly Uptime Percentage falls below the Uptime Commitment, Customers may request a credit within 30 days of month-end. Credits apply to future invoices and are the sole remedy for uptime issues.

| **Monthly Uptime** | **Credit** |
| --- | --- |
| < 99% to ≥ 98.0% | 5% of monthly prorated subscription fees |
| < 98.0% to ≥ 95.0% | 10% of monthly prorated subscription fees |
| < 95.0% | 25% of monthly prorated subscription fees |

Credits exclude professional services and taxes and are capped at the monthly prorated subscription fees for the affected month.

**5. Support & Response Targets.** If the parties agree to Slack support, Wolfia will monitor the designated channel. Our enterprise plan targets are initial response times:

(a) Severity 1 (Critical): Production outage or data loss - 3 hours, 24×7;

(b) Severity 2 (High): Severe degradation or major feature unavailable - 12 business hours;

(c) Severity 3 (Normal): Material feature issue with workaround - 3 business days;

(d) Severity 4 (Low): Minor issue/requests - 10 business days.

**6. Exclusions & Remedies.** The SLA does not apply to: (i) misuse or use contrary to Documentation; (ii) Customer or third-party systems; (iii) sandbox/pre-production environments. Service credits are Customer’s sole and exclusive remedy for failure to meet this SLA.

**7. Status & Reporting.** Wolfia will maintain a service status page and incident communications via email or Slack where feasible.

### Exhibit B — Data Processing Addendum (DPA)

This DPA forms part of the Agreement and applies to the extent Wolfia processes Personal Data on behalf of Customer in providing the Cloud Service. Where this Exhibit B conflicts with the Agreement, this Exhibit B controls; where it conflicts with the SCCs, the SCCs control. Capitalized privacy terms not defined here (e.g., “Personal Data,” “Processing,” “Controller,” “Processor,” “Data Subject,” “Applicable Data Protection Laws”) have the meanings given in such laws (including GDPR/UK GDPR and CCPA/CPRA).

**Key Terms**

* **Approved Subprocessors:**<https://trust.wolfia.com/?tab=subprocessors> (See also Annex III below.)
* **Provider Security Contact:** security@wolfia.com
* **Provider Address:** 10500 Avery Club Dr Unit 6, Austin, Texas 78717, USA
* **Security Policy:**<https://trust.wolfia.com/> (Security Overview incl. data retention, encryption, access controls, incident response)
* **Governing Law & Chosen Courts (DPA):** Delaware.

**Service Provider / Processor Role (US State Laws).** To the extent the CCPA/CPRA and similar US state privacy laws apply, Wolfia acts as a service provider/processor and will not sell or share Personal Data, nor retain, use, or disclose Personal Data for any purpose other than to provide the Cloud Service, as permitted by law, or as otherwise instructed by Customer. Wolfia will notify Customer if it can no longer meet its obligations.

Restricted Transfers. For transfers of Personal Data from the EEA/UK/Switzerland to countries without adequate protection, the parties incorporate by reference the EU Standard Contractual Clauses (Controller-to-Processor, Module 2) (EU 2021/914) and, where applicable, the UK Addendum and Swiss Addendum. The governing Member State for EEA transfers is Netherlands; for UK transfers, England and Wales. Annexes I–II to this DPA serve as the SCC Annexes.

**Order of Precedence (DPA).** In case of conflict: SCCs → this DPA → Agreement.

#### Annex I — Description of Processing

* Service: Wolfia is a SaaS platform that automates completion of security questionnaires, RFPs, and vendor risk documentation using AI-driven retrieval-augmented generation (RAG). The service ingests customer-provided data, applies AI models to generate responses, and surfaces results via a web dashboard and API.
* Categories of Data Subjects: Customer’s employees and contractors; Customer’s end users or customers whose data appears within Customer Content.
* Categories of Personal Data: Name; contact information (email, phone, address); user activity/analytics (e.g., device information, IP address); and other Personal Data contained within Customer Content. Special categories are not intended to be processed.
* Special Category Data: No.
* Frequency of Transfer: Continuous.
* Nature & Purpose of Processing: Receiving/collecting; holding/storing; using/analyzing (including automated processing and profiling); updating/correcting; protecting/security testing; and erasing/deletion.
* Duration of Processing: For the Subscription Term and any data-return period, or as otherwise required by law.

#### Annex II — Technical and Organizational Measures

* Encryption: TLS 1.2+ in transit; AES-256-GCM at rest using AWS KMS keys. Sensitive direct identifiers are redacted or tokenized in logs/analytics for pseudonymization where full fidelity is unnecessary.
* Infrastructure & Monitoring: Production services in redundant AWS Availability Zones; least-privilege security groups; WAF; continuous monitoring via Grafana and AWS GuardDuty; SLA-backed metrics for uptime, integrity, and anomalous activity.
* Backups & DR: Encrypted snapshots hourly; cross-region storage; annual DR drills; RTO < 4 hours, RPO = 2 hours.
* Assurance & Testing: Annual SOC 2 Type II; annual external penetration tests; continuous SCA/SAST pipelines; findings triaged with remediation SLAs tied to severity.
* Access Management: All internal access via SSO with enforced MFA; least-privilege IAM roles; SCIM for provisioning & deprovisioning. Customer access authenticated via OpenID Connect; fine-grained authorization enforced by RBAC scopes.
* Transport Security: All external and inter-service traffic over HTTPS with HSTS; mutual TLS for micro-service calls; restricted cipher suites verified by automated SSL scans.
* Storage Security: Encrypted Amazon RDS and S3 with KMS keys rotated annually; object-lock versioning and server-side checksums for integrity.
* Physical Security: Data resides exclusively in AWS data centres with ISO 27001 and SOC 1/2/3 certifications, with 24×7 badge access, CCTV, and biometric controls.
* Logging: Security, application, and audit logs streamed to a centralized, tamper-evident Log Archive account with ~30-day hot retention; immutable logs feed real-time alerting and support forensic analysis under the incident-response plan.
* Governance: Security Committee meets quarterly to review risk, vulnerabilities, and policy compliance; all staff complete annual security awareness training and sign Acceptable Use and Confidentiality agreements.
* Data Minimization & Retention: Only required fields are ingested; transient processing data purged within 24 hours; customer workspace data deleted 30 days after contract termination or upon verified request; backups age out after 90 days.
* Data Quality: Input validations, schema constraints, and automated tests prevent malformed records; periodic reconciliations compare source data to generated outputs to detect drift or corruption.
* Portability & Erasure: Verified deletion requests trigger a documented erasure workflow across primary and secondary systems within 30 days.

#### Annex III — Subprocessors

Wolfia maintains a current list of subprocessors at <https://trust.wolfia.com/?tab=subprocessors> and will provide advance notice of material changes.

### Exhibit C — (Optional) Statement of Work (SOW)

If professional services are purchased, details (scope, deliverables, fees, timelines) will be set out in one or more SOWs executed by the parties and incorporated herein by reference.