DATA PROCESSING AGREEMENT

This Data Processing Agreement ("Agreement") forms part of the Contract for Services ("Principal Agreement") between:

_____ _____ _____ (the "Company" or "Controller")

and

Konrado.AI, Inc. 1111B S Governors Ave STE 29085 Dover, DE 19904 US (the "Data Processor" or "Processor")

(together as the "Parties")

WHEREAS

(A) The Company acts as a Data Controller. (B) The Company wishes to subcontract certain Services to the Data Processor, which imply the processing of personal data. (C) The Parties seek to implement a data processing agreement that complies with the requirements of the current legal framework in relation to data processing and with the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) (the "GDPR"). (D) The Parties wish to lay down their rights and obligations in relation to such processing.

IT IS AGREED AS FOLLOWS:

1. Definitions and Interpretation

1.1 Unless otherwise defined herein, capitalized terms and expressions used in this Agreement shall have the following meaning:

- "Agreement" means this Data Processing Agreement and all Schedules.
- "Company Personal Data" means any Personal Data Processed by the Processor on behalf of Company pursuant to or in connection with the Principal Agreement. This primarily includes data related to hosting support tickets, chat logs, server configurations, and customer account details as described in Section 2.2.

- "Data Protection Laws" means EU Data Protection Laws and, to the extent applicable, the data protection or privacy laws of any other country, including but not limited to the California Consumer Privacy Act (CCPA).
- "EEA" means the European Economic Area.
- "EU Data Protection Laws" means EU Directive 95/46/EC, as transposed into domestic legislation of each Member State and as amended, replaced or superseded from time to time, including by the GDPR and laws implementing or supplementing the GDPR.
- "GDPR" means EU General Data Protection Regulation 2016/679.
- "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data transmitted, stored or otherwise processed.
- "Services" means the AI-powered L1 (Level 1) and L2 (Level 2) hosting support automation services provided by Konrado.AI to the Company, as described in the Principal Agreement. This includes automating support responses, processing support tickets, providing technical assistance, and integrating with the Company's hosting and billing systems.
- "Subprocessor" means any person appointed by or on behalf of Processor to process Personal Data on behalf of the Company in connection with the Agreement.

1.2 The terms, "Commission", "Controller", "Data Subject", "Member State", "Personal Data", "Processing" and "Supervisory Authority" shall have the same meaning as in the GDPR, and their cognate terms shall be construed accordingly.

2. Scope of Processing Company Personal Data

2.1 The Processor shall:

- comply with all applicable Data Protection Laws in the Processing of Company Personal Data; and
- not Process Company Personal Data other than on the relevant Company’s documented instructions.

2.2 The Company instructs Processor to process Company Personal Data to provide the Services. This processing involves the collection and use of Personal Information (such as contact details, account information, communication data like support tickets and chat logs), and Technical Information (such as hosting data, integration data, usage data, and support

data). The Processor also processes Payment Information via third-party payment processors.

- Categories of Data Subjects: The processing primarily concerns the Company's customers, employees, and other individuals whose data is contained within the hosting support tickets, chat logs, and related system configurations.
- Nature and Purpose of Processing: The Processor processes Company Personal Data to automate L1 & L2 hosting support through AI, process support tickets, provide technical assistance, integrate with existing hosting/billing systems, and analyse support patterns to improve service quality. For AI processing, Konrado.AI uses third-party AI services, such as Azure OpenAI's models, to generate support responses and automate ticket handling, applying data minimisation by sending only relevant data to AI systems. Chat logs and tickets are processed to improve support quality.
- Duration of Processing: Data will be retained according to Konrado.AI's Privacy Policy: Support tickets for 2 years, chat logs for 1 year, account data until account closure + 30 days, and technical logs for 90 days unless needed for ongoing support.
- Payment Information processing is limited to transaction metadata necessary for service delivery and account management; the Processor does not store, process, or have access to full payment card details, which are handled directly by certified third-party payment processors in compliance with PCI DSS standards.

2.3 AI Processing Safeguards. When processing Company Personal Data through AI services, the Processor shall:

(a) implement data minimization by sending only relevant, non-sensitive data necessary for support automation;

(b) ensure AI service providers have appropriate data protection agreements prohibiting data retention, training, or any other use of Company Personal Data beyond the immediate processing request, with automatic deletion upon completion;

(c) maintain logs of all AI processing activities; and

(d) provide additional encryption for sensitive data processed through AI services.

(e) no company data is used to train third-party AI models

3. Processor Personnel

The Processor shall take reasonable steps to ensure the reliability of any employee, agent or contractor who may have access to the Company Personal Data. Access will be strictly limited to individuals who need it for the purposes of the Principal Agreement and to comply with applicable laws. All such individuals shall be subject to confidentiality undertakings or professional/statutory obligations of confidentiality.

4. Security

4.1 Taking into account the state of the art, the costs of implementation, and the nature, scope, context and purposes of Processing, as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the Processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to that risk, including, as appropriate, the measures referred to in Article 32(1) of the GDPR.

4.2 In assessing the appropriate level of security, the Processor shall take account in particular of the risks that are presented by Processing, especially from a Personal Data Breach.

4.3 Konrado.AI operates on a multi-tenant architecture, ensuring that each company can access only its own data. Data belonging to one client is never shared or visible to others, and strict isolation between tenants is maintained at all times.

4.4 Konrado.AI employs a defence-in-depth security approach, including:

- Network Security: TLS 1.3 encryption for all data in transit, private network connections, advanced DDoS protection, and a Web Application Firewall (WAF).
- Data Security: AES-256 encryption at rest across all data stores, application-level encryption for sensitive tokens, multi-factor authentication (MFA) enforcement, and role-based access control (RBAC).
- Application Security: Automated security scanning, regular penetration testing, comprehensive incident response procedures, and secure development lifecycle (SDLC) implementation.
- Logical Separation: Personal Data from different subscriber environments is logically segregated on the Processor’s systems.

5. Subprocessing

5.1 The Processor shall not appoint (or disclose any Company Personal Data to) any Subprocessor unless required or authorised by the Company.

5.2 The Company acknowledges, agrees, and consents that, for the sole purpose of providing the Service, Company Personal Data may be processed by the Processor and its Subprocessors, subject to the conditions herein.

5.3 The Processor is authorised to engage the Subprocessors listed below, which are essential for the provision of the Service. The Processor shall:

- enter into a written agreement with the Subprocessor containing obligations no less stringent than those set out in this Agreement;
- assess the Subprocessor and remain liable for the actions or omissions of the Subprocessor with regard to its obligations under this Agreement;
- make available a list of its current Subprocessors upon request, and will update the list to reflect any additions or replacements. The Processor will provide written notice to the Company of the engagement of any new Subprocessor.

5.4 The Company may reasonably object in writing to the use of a new Subprocessor within ten (10) calendar days of notice, provided such objection is based on reasonable grounds relating to data protection. In the event of an objection, the Parties will discuss such concerns in good faith. If no mutually acceptable solution can be found within thirty (30) days, either Party may terminate the Principal Agreement with sixty (60) days' written notice. The Company acknowledges that objecting to the use of a Subprocessor that is essential for core Service functionality may result in service limitations or termination. For Subprocessors listed in Section 5.3 as of the Effective Date, the Company's continued use of the Services constitutes consent to their use.

Current Subprocessors:

- Supabase: Database & Auth Tables (Ireland)
- OpenAI: AI Compute (USA)
- xAI (Grok): AI Compute (USA)
- Google (Gemini): AI Compute (USA)
- Hetzner: Server Infrastructure (Germany)
- Vercel: Application Hosting, Edge & Serverless (Frankfurt, Germany)
- LangSmith: AI Observability, LLM Tracing (Europe-West-4, Netherlands)

- Sentry: Application Monitoring, Telemetry (Frankfurt, Germany)
- Clerk: Authentication & Access Management (USA)
- Microsoft Clarity: User interaction analytics to improve usability and performance, with a commitment to transparency and compliance with applicable data protection laws

6. Data Subject Rights

6.1 Taking into account the nature of the Processing, the Processor shall assist the Company by implementing appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Company's obligations to respond to requests to exercise Data Subject rights under the Data Protection Laws.

6.2 The Processor shall promptly notify the Company if it receives a request from a Data Subject under any Data Protection Law in respect of Company Personal Data. The Processor shall ensure that it does not respond to that request except on the documented instructions of the Company or as required by Applicable Laws. In such a case, the Processor shall, to the extent permitted by Applicable Laws, inform the Company of that legal requirement before responding.

7. Personal Data Breach

7.1 The Processor shall notify the Company without undue delay and in any event within seventy-two (72) hours upon becoming aware of a Personal Data Breach affecting Company Personal Data, providing the Company with sufficient information to allow the Company to meet any obligations to report or inform Data Subjects of the Personal Data Breach under the Data Protection Laws.

7.2 The Processor shall co-operate with the Company and take reasonable commercial steps as are directed by the Company to assist in the investigation, mitigation and remediation of each such Personal Data Breach.

8. Data Protection Impact Assessment and Prior Consultation

The Processor shall provide reasonable assistance to the Company with any data protection impact assessments, and prior consultations with Supervisory Authorities or other competent data privacy authorities, which the Company reasonably considers to be required by Article 35 or 36 of the GDPR or equivalent provisions of any other Data Protection Law. This assistance will be solely in relation to Processing of Company Personal Data by, and taking into account the nature of the Processing and information available to, the Processor.

9. Deletion or Return of Company Personal Data

9.1 Subject to this Section 9, the Processor shall promptly and in any event within 10 business days of the Cessation Date, delete and procure the deletion of all copies of those Company Personal Data.

9.2 The Processor shall provide written certification to the Company that it has fully complied with this Section 9 within 10 business days of the Cessation Date.

10. Audit Rights

10.1 Subject to this Section 10, the Processor shall make available to the Company on request all information necessary to demonstrate compliance with this Agreement.

10.2 The Company may request an audit once per calendar year with thirty (30) days' notice. Audits will be conducted through documentation review only. The Company pays all audit costs.

11. Data Transfer

11.1 The Company acknowledges and consents that Company Personal Data may be transferred to and processed in countries outside the EU/EEA by the Subprocessors listed in Section 5.3, provided that such transfers are made in accordance with applicable Data Protection Laws and appropriate safeguards are in place as described in Section 11.2. For any new Subprocessors requiring data transfers outside the EU/EEA, the Processor will obtain the Company's prior written consent as part of the new Subprocessor notification process in Section 5.3.

11.2 If Personal Data processed under this Agreement is transferred from a country within the European Economic Area to a country outside the European Economic Area, the Parties shall ensure that the personal data are adequately protected. To achieve this, the Parties shall, unless agreed otherwise, rely on EU approved standard contractual clauses (SCC) for the transfer of personal data or applicable Adequacy Decisions, such as the EU-U.S. Data Privacy Framework (DPF) certification where applicable. Konrado.AI's core infrastructure is EU-resident (Vercel Frankfurt, Supabase Ireland, Azure Poland).

12. Controller's Responsibilities

12.1 The Company is responsible for assessing and ensuring that the Processing of Personal Data is legitimate and in compliance with Applicable Privacy Law.

12.2 The Company represents and warrants that it has an appropriate legal basis to process and disclose Personal Data to the Processor as part of the provision of the Service.

12.3 The Company represents and warrants that it fully complies with the Applicable Privacy Law, and shall indemnify and hold harmless the Processor from and against any claims, incidents, liabilities, procedures, damages, losses and expenses (including legal fees) arising out of or in any way connected with the Company’s breach of its obligations under this Agreement or the Applicable Privacy Law.

12.4 Processor Indemnification. The Processor represents and warrants that it will comply with all applicable Data Protection Laws in the performance of its obligations under this Agreement, and shall indemnify and hold harmless the Company from and against any claims, incidents, liabilities, procedures, damages, losses and expenses (including reasonable legal fees) arising out of or in any way connected with the Processor's material breach of its obligations under this Agreement or violation of applicable Data Protection Laws, provided that the Company promptly notifies the Processor of any such claim and cooperates reasonably in the defense thereof.

13. General Terms

13.1 Confidentiality. Each Party must keep this Agreement and information it receives about the other Party and its business in connection with this Agreement (“Confidential Information”) confidential and must not use or disclose that Confidential Information without the prior written consent of the other Party except to the extent that: (a) disclosure is required by law; or (b) the relevant information is already in the public domain.

13.2 Notices. All notices and communications given under this Agreement must be in writing and will be delivered personally, sent by post or sent by email to the address or email address set out in the heading of this Agreement or at such other address as notified from time to time by the Parties changing address.

13.3 In the event of a conflict between the terms of this Agreement and the Principal Agreement, this Data Processing Agreement will prevail regarding data processing matters.

13.4 Limitation of Liability.

(a) Each Party's total liability under this Agreement shall not exceed the total fees paid by the Company to the Processor under the Principal Agreement in the twelve (12) months preceding the event giving rise to the claim.

(b) Neither Party shall be liable for any indirect, incidental, special, consequential, or punitive damages, including but not limited to loss of profits, data, or business opportunities, regardless of the theory of liability.

(c) These limitations shall not apply to:

(i) a Party's breach of confidentiality obligations,

(ii) willful misconduct or gross negligence, or

(iii) claims arising from a Personal Data Breach caused by the Processor's failure to implement required security measures under Section 4.

13.5 Force Majeure. Neither Party shall be liable for any failure or delay in performance under this Agreement which is due to fire, flood, earthquake, pandemic, government action, war, terrorism, network infrastructure failures, cyber attacks, or other causes that are beyond the reasonable control of such Party, provided that such Party uses reasonable efforts to avoid and remove such causes of non-performance and continues performance with the utmost dispatch whenever such causes are removed.

13.6 Intellectual Property. Each Party retains all rights, title, and interest in its pre-existing intellectual property. The Processor retains all rights to its AI models, algorithms, software, methodologies, and any improvements or derivatives thereof developed in connection with the Services. The Company grants the Processor a limited license to use Company Personal Data solely for the purpose of providing the Services as described herein.

14. Governing Law and Jurisdiction

14.1 This Agreement is governed by the laws of the State of Delaware, United States.

14.2 Any dispute arising in connection with this Agreement, which the Parties will not be able to resolve amicably, will be submitted to the exclusive jurisdiction of the courts of Delaware, subject to possible appeal to the Delaware Supreme Court.

IN WITNESS WHEREOF, this Agreement is entered into with effect from the date first set out below.

Konrado.AI, Inc. (Processor)

Signature _____

Name: _____

Title: _____

Date Signed: _____

[Company Name] (Controller)

Signature _____

Name _____

Title _____

Date Signed _____