Data Processing Agreement

This Data Processing Agreement ("DPA") forms part of the Master Services Agreement (the "MSA") between KEIGHT LLC, an Iowa limited liability company ("Company" or "Processor") and Customer ("Customer" or "Controller"). Capitalized terms not defined here have the meanings in the MSA.

Which parts apply. Part A applies to every Customer. Part B (US Privacy Addendum) applies to Customers established in the United States. Part C (International Transfers) applies to Customers established in, or whose Customer Data includes personal data of individuals in, the European Economic Area, the United Kingdom, or Switzerland. The DPA attaches automatically for those Customers on signature of the MSA (MSA Section 11.2).

Part A: General Terms

1. Definitions

"**Applicable Data Protection Law**" means all laws that apply to the processing of Personal Data under this DPA, including, where applicable, the EU General Data Protection Regulation 2016/679 ("GDPR"), the UK GDPR and Data Protection Act 2018, the Swiss Federal Act on Data Protection, and United States state privacy laws such as the California Consumer Privacy Act as amended ("CCPA") .

"**Customer Personal Data**" means Personal Data contained in Customer Data that Company processes on Customer's behalf.

"**Data Subject**" means the individual to whom Personal Data relates.

"**Personal Data**," "**processing**," "**controller**," "**processor**," "**personal data breach**," and "**supervisory authority**" have the meanings in the GDPR, or the closest equivalent in other Applicable Data Protection Law.

"**SCCs**" means the standard contractual clauses for the transfer of personal data to third countries adopted by the European Commission by Implementing Decision (EU) 2021/914, as amended or replaced .

"**Sub-processor**" means a third party engaged by Company to process Customer Personal Data.

"**UK Addendum**" means the International Data Transfer Addendum to the EU SCCs issued by the UK Information Commissioner's Office under section 119A of the Data Protection Act 2018, as amended or replaced .

2. Roles and Scope

2.1 Customer is the controller (or, where Customer acts for its own customers, a processor) of Customer Personal Data, and Company is Customer's processor (or sub-processor). Annex I describes the processing.

2.2 Customer instructs Company to process Customer Personal Data only (a) to provide the Services under the MSA and Order Documents, (b) as further documented in Tickets and written instructions from Customer's authorized contacts, and (c) as required by law applicable to Company, in which case Company will inform Customer before processing unless the law prohibits it.

2.3 Company will inform Customer if, in Company's opinion, an instruction infringes Applicable Data Protection Law. Company may suspend the instruction until Customer confirms or changes it.

2.4 Customer is responsible for the lawfulness of the Customer Personal Data it stores in Odoo, including having a legal basis and giving notices to Data Subjects. Customer will not instruct Company to process special-category data beyond what is incidental to operating an Odoo instance unless the parties agree additional measures in writing.

3. Confidentiality and Personnel

3.1 Company will ensure that persons authorized to process Customer Personal Data (Company personnel) are bound by written confidentiality obligations and receive data protection training appropriate to their role.

3.2 Company will limit access to Customer Personal Data to personnel who need it to perform the Services.

4. Security

4.1 Company will implement and maintain the technical and organizational measures in Annex II, and will not materially reduce them during the term.

4.2 Customer is responsible for security of the parts of the Customer Environment it controls, for its users' credentials, and for deciding which recommended safeguards to enable (MSA Section 6.4).

5. Sub-processors

5.1 **Authorization.** Customer gives general written authorization for Company to engage the Sub-processors listed in Annex III.

5.2 **Changes.** Company will give Customer at least 30 days' notice before adding or replacing a Sub-processor, by notice in the Support Portal and email to Customer's authorized contact. Customer may object in writing within the 30 days on reasonable data protection grounds. If the parties cannot resolve the objection within 30 days after it is raised, either party may terminate the affected Services on written notice, with exit assistance under MSA Section 8.5 and a pro-rata refund of prepaid fees for the terminated Services.

5.3 **Flow-down.** Company will impose on each Sub-processor data protection obligations that provide at least the level of protection in this DPA, by written contract, and remains liable to Customer for the Sub-processor's performance.

5.4 **AI Sub-processor.** Customer specifically acknowledges Anthropic PBC as a Sub-processor for Ticket triage and diagnostics (MSA Section 5). Company will send Anthropic only the Ticket content and the excerpts of Customer Data needed to handle the Ticket, and will not send full database dumps.

6. Data Subject Rights

6.1 Company will, taking into account the nature of the processing, assist Customer with appropriate technical and organizational measures to respond to Data Subject requests (access, rectification, erasure, restriction, portability, objection). In practice, Customer can fulfill most requests directly in Odoo; Company will help with requests that require database-level action within 5 Business Days of a Ticket.

6.2 If Company receives a request directly from a Data Subject, it will not respond except to direct the Data Subject to Customer, and will notify Customer promptly.

7. Personal Data Breach

7.1 Company will notify Customer without undue delay, and in any case within 48 hours, after becoming aware of a personal data breach affecting Customer Personal Data, so that Customer can meet its own 72-hour notification obligation to supervisory authorities where applicable.

7.2 The notification will describe, to the extent known, the nature of the breach, the categories and approximate number of Data Subjects and records affected, the likely consequences, the measures taken or proposed, and a contact point. Company may provide information in phases as it becomes available.

7.3 Company will assist Customer with investigation, mitigation, and Customer's notifications to authorities and Data Subjects. Assistance beyond 8 hours per breach is billable at Company's hourly rate unless the breach was caused by Company's breach of this DPA.

7.4 Company will not notify authorities or Data Subjects on Customer's behalf unless Customer asks in writing or the law requires it.

8. Assistance with Impact Assessments and Consultations

Company will provide reasonable assistance, on request, with data protection impact assessments and prior consultations with supervisory authorities, to the extent they relate to Company's processing and the information is reasonably available to Company. Assistance beyond 4 hours per year is billable at Company's hourly rate.

9. Audits

9.1 Company will make available the information reasonably necessary to demonstrate compliance with this DPA, including the current Annex II, Sub-processor list, action logs, and summaries of any third-party security assessments Company has obtained.

9.2 If that information is not sufficient to satisfy a legal requirement, Customer (or an independent auditor bound by confidentiality) may audit Company's compliance once per 12 months, or after a personal data breach, on at least 30 days' notice, during Business Hours, in a manner that does not

disrupt Company's operations or expose other customers' data. Customer bears its own audit costs and reimburses Company's time for audit assistance beyond 4 hours per year at Company's hourly rate.

10. Return and Deletion

10.1 On termination of the Services, Company will return Customer Personal Data by delivering the final backup under MSA Section 8.5 and, after Customer confirms receipt or 30 days after handover, whichever is earlier, delete Customer Personal Data from Company's systems, including monitoring systems and Support Portal attachments, and will revoke Company's key to Customer's Backblaze bucket (the bucket itself and its backups remain Customer's), except where law requires retention.

10.2 Customer Personal Data in Customer's own Hetzner project remains Customer's; Company's obligation is to remove its own access.

10.3 Ticket history in the Support Portal that contains Customer Personal Data is deleted 12 months after termination unless Customer requests earlier deletion or an export.

10.4 Company will confirm deletion in writing on request.

11. Liability, Term, and Precedence

11.1 Each party's liability under this DPA is subject to the limitation of liability in the MSA, to the extent permitted by Applicable Data Protection Law.

11.2 This DPA lasts as long as Company processes Customer Personal Data.

11.3 If this DPA conflicts with the MSA, this DPA controls as to processing of Personal Data. If the SCCs conflict with this DPA, the SCCs control.

Part B: US Privacy Addendum

Applies to Customers established in the United States. For these Customers, Part C does not apply unless Customer Data includes Personal Data of individuals in the EEA, UK, or Switzerland.

B.1 **Service provider role.** Company acts as a "service provider" or "processor" as those terms are defined under the CCPA and comparable US state privacy laws.

B.2 **Restrictions.** Company will not (a) sell or share Customer Personal Data; (b) retain, use, or disclose it for any purpose other than the business purpose of providing the Services under the MSA, or outside the direct business relationship with Customer; or (c) combine it with Personal Data from other sources, except as permitted for service providers under Applicable Data Protection Law.

B.3 **Compliance.** Company will comply with the obligations of a service provider under Applicable Data Protection Law, provide the same level of privacy protection required of businesses, notify Customer if it can no longer meet its obligations, and allow Customer to take reasonable steps to stop and remediate unauthorized use.

B.4 **Sub-processors, security, breach, deletion.** Sections 3 through 10 of Part A apply.

B.5 **Consumer requests.** Company will assist Customer with verifiable consumer requests under Section 6 of Part A.

Part C: International Transfers (EEA, UK, Switzerland)

C.1 **Transfer mechanism.** Customer Personal Data hosted in the Customer Environment stays in the Hetzner region Customer selects. Company's access from the United States and the Anthropic Sub-processor constitute transfers of Personal Data to the United States. The parties rely on the SCCs and UK Addendum as follows, unless Company later certifies to the EU-US Data Privacy Framework and notifies Customer.

C.2 **EU SCCs incorporated.** The SCCs, Module Two (controller to processor), are incorporated by reference into this DPA with these selections:

- Clause 7 (docking clause): included.
- Clause 9(a): Option 2, general written authorization, with the notice period in Section 5.2 of Part A.
- Clause 11(a): the optional independent dispute resolution language is not included.
- Clause 13 and Annex I.C: the supervisory authority of the EU member state where Customer is established, or where Customer's EU representative is established.
- Clause 17: the laws of Ireland.
- Clause 18(b): the courts of Ireland.
- Annex I of the SCCs is completed by Annex I below; Annex II of the SCCs is completed by Annex II below; Annex III of the SCCs is completed by Annex III below.

Where Customer itself acts as a processor for its own customers, Module Three (processor to processor) applies with the same selections.

C.3 **UK Addendum incorporated.** For transfers subject to UK GDPR, the UK Addendum is incorporated by reference, with Table 1 completed by the parties' details in the MSA, Table 2 selecting the SCCs as incorporated in C.2, Table 3 completed by the Annexes below, and Table 4 allowing either party to end the UK Addendum as set out in its Section 19.

C.4 **Switzerland.** For transfers subject to Swiss law, the SCCs apply with the adaptations the Swiss Federal Data Protection and Information Commissioner requires, including references to the Swiss supervisory authority and Swiss law where the transfer is governed solely by Swiss law.

C.5 **Transfer impact.** Company will, on request, provide information reasonably available to it to help Customer assess the transfer, including whether Company has received government access requests for Customer Personal Data (Company has received none as of the date of this DPA), and will notify Customer of any such request unless legally prohibited.

C.6 **EU hosting option.** On request and subject to the Order Document, Company will operate the Managed Instance in a Hetzner EU data center and store backups in a Backblaze EU region, which reduces (but does not eliminate) transfers, because Company's personnel and the AI Sub-processor remain in the United States.

Annex I: Description of Processing

A. List of parties

	Data exporter (Customer)	Data importer (Company)
Name	[CUSTOMER LEGAL NAME]	KEIGHT LLC, an Iowa limited liability company
Address	[ ]	109 SE 4th Street, Des Moines, IA 50309, USA
Contact	[name, role, email]	Mark Kladivo, privacy@allodi.us
Role	Controller (or processor)	Processor (or sub-processor)
Signature and date		

B. Description of transfer and processing

Item	Description
Categories of Data Subjects	Customer's employees and users of its Odoo instance; Customer's customers, prospects, suppliers, and their contact persons; portal users; job applicants (if Customer uses Odoo recruitment); any other individuals whose data Customer stores in Odoo
Categories of Personal Data	Names, business and personal contact details, job titles, user account data, IP addresses and login logs, order and invoice history, payment references (not full card numbers), communications stored in Odoo chatter and email, delivery addresses, and any other fields Customer configures in Odoo
Special-category data	Not intended. Incidental processing may occur if Customer stores such data in Odoo (for example, HR records with health or union information). Customer is responsible for restricting such data and for applying additional measures if needed. Company applies Annex II measures uniformly
Frequency	Continuous for hosting operations and backups; on request for support Tickets and projects
Nature of processing	Hosting operations; backup and restore; monitoring; diagnostics; support; code development and deployment; migration and upgrade; storage
Purpose	Providing the Services described in the MSA and Order Documents
Retention	For the term of the Services; backups retained per the Service Description; deleted under Part A Section 10 after termination
Sub-processor transfers	To the Sub-processors in Annex III for the purposes and durations stated there

C. Competent supervisory authority

The supervisory authority of the EU member state in which Customer is established, or as determined under Clause 13 of the SCCs.

Annex II: Technical and Organizational Security Measures

These measures reflect Company's delivery model: a small team, AI-assisted operations under human oversight, and customer-owned infrastructure.

Area	Measure
Access control to Customer Environments	SSH key-only access; no password login; per-person keys; MFA required on Company's Hetzner, Backblaze, repository, and Support Portal accounts; database access only through the VM, never exposed to the internet; MFA on any interactive database access path; access removed within one Business Day when a person's role changes
AI Agent boundaries	AI Agent runs with credentials limited to read-only diagnostics and the published Pre-Approved Actions; no deployment, migration, financial, or outbound-messaging capability without a human approval step; every AI Agent action logged with identity, timestamp, target, and command; Ticket and record content treated as data, not instructions
Human oversight	A named Company person reviews and approves any action outside Pre-Approved Actions before it is executed; production restores and financial changes require written approval from Customer's authorized contact
Logging and monitoring	Central action log visible to Customer; system logs retained at least 90 days on the VM and 12 months in Company's systems; monitoring for availability, disk, backup success, TLS expiry, cron health, and mail failures
Data minimization to AI Sub-processor	Only Ticket content and the excerpts needed for the Ticket are sent to Anthropic; no full database dumps; Company's commercial API terms with Anthropic govern retention
Encryption	TLS for all traffic to the Odoo instance, the Support Portal, Hetzner, Backblaze, and Anthropic; backups encrypted at rest in Backblaze B2 with server-side encryption and, where enabled on the Order Form, client-side encryption with a Customer-held key; Hetzner volume encryption where offered
Backups and recovery	Daily backups and continuous archiving of database transaction logs for point-in-time recovery; retention per Service Description; periodic test restores recorded in the monthly report; backups in a bucket in each Customer's own Backblaze account; Company holds only a key limited to that bucket
Isolation	Each Customer's Odoo runs on VMs in Customer's own Hetzner project; no shared databases between customers; a separate Backblaze account and bucket per Customer, owned by Customer; separate Support Portal tenant per Customer
Vulnerability and patch management	Unattended OS security updates; Odoo and dependency updates applied after testing; firewall restricting inbound ports to HTTPS and SSH; SSH restricted to Company IP ranges where practical

Secure development	Custom Modules kept in Customer's repository; changes reviewed before deployment; secrets never committed to repositories; a neutralized staging copy on Customer's server used for changes under Managed Odoo (Service Description Section 4.7) or where the Order Document provides one
Personnel	Confidentiality obligations for all Company personnel; data protection awareness training; background of Company personnel verified before granting production access
Incident response	Documented process for detection, containment, notification (Part A Section 7), and post-incident review; contact point security@allodi.us
Physical security	Company does not operate data centers. Hetzner and Backblaze are responsible for physical security of their facilities under their own certifications. Company's own devices are encrypted with screen lock and remote wipe
Data deletion	Deletion per Part A Section 10; Company's Backblaze key revoked at exit (the bucket and backups remain Customer's); confirmation on request
Sub-processor management	Written contracts with each Sub-processor; review of their security documentation at onboarding and annually; 30-day notice of changes

Annex III: Sub-processors

Sub-processor	Location	Purpose	Data involved	Notes
Hetzner Online GmbH	Germany (data centers in Germany, Finland, and the United States; Customer selects region)	Cloud infrastructure on which the Managed Instance runs	All Customer Data in the Managed Instance	Customer contracts with Hetzner directly for the VM; Hetzner is listed because Company operates on that infrastructure and may use Hetzner snapshot or console features.
Backblaze, Inc.	United States (regions in the US and EU; Customer may request EU)	Backup storage (B2)	Full database and filestore backups	Bucket in Customer's own Backblaze account; Company uses a bucket-limited key.
Anthropic, PBC	United States	Large language model API for Ticket triage, diagnostics, and drafting	Ticket content, log excerpts, and data excerpts needed for the Ticket; no full dumps	Commercial API under Anthropic's commercial terms; no training on API inputs or outputs per those terms
Hetzner Online GmbH	Germany (Company's own server, in Hetzner's Ashburn, Virginia,	Hosting of the Support Portal	Ticket content, attachments, action logs	Company's own Hetzner account; Company operates the Support Portal

	USA data center)			on it
Microsoft Corporation	United States	Company email (Microsoft 365), including notification emails from the Support Portal	Email addresses, Ticket subject lines	Company's Microsoft 365 account
Telnyx LLC	United States	Telephone and text-message services: on-call alerts (text messages and calls) to Company's on-call person, and Company's support phone lines, including Customers' Direct Emergency Lines	In alerts, Customer's company name and site address and the subject line and number of Priority 1 Tickets; on the phone lines, callers' phone numbers, call records, and voicemail messages	Company's own Telnyx account; no credentials and no Customer Data from the Managed Instance
Hetzner Online GmbH	Germany (Company's own server, in Hetzner's Falkenstein, Germany data center)	Watcher server that checks from outside Customer's network that the Managed Instance answers and its TLS certificate is valid	Customer's company name and site address, its support tier, and the subject line and number of Priority 1 Tickets; no credentials and no Customer Data from the Managed Instance	Company's own Hetzner account

Company will maintain the current list in the Support Portal and notify Customer of changes under Part A Section 5.2.

Signatures

Where the SCCs or UK Addendum require separate signature, the parties' signatures below serve as signature of this DPA and of the SCCs and UK Addendum as incorporated.

	KEIGHT LLC, an Iowa limited liability company	**[CUSTOMER LEGAL NAME]**
Signature		
Name	Mark Kladivo	
Title		
Date		