ZeeHub Data Processing Agreement

Template version: November 5, 2026

This Data Processing Agreement ("DPA") forms part of the agreement between ZeeHub and Customer for the ZeeHub platform (the "Agreement"). It sets out how ZeeHub processes personal data on Customer's behalf.

Parties

Role	Party
Processor / Service Provider	ZeeHub Inc, a Delaware corporation, 809 Cuesta Drive Suite B PMB 1047, Mountain View, CA 94040 ("ZeeHub")
Controller / Business	[Customer legal entity name], [registered address] ("Customer")

This DPA takes effect on the date the Agreement takes effect, or the date both parties sign below, whichever is later. If Customer signs this DPA without separately signing the Agreement, this DPA applies to the order form or online terms under which Customer uses ZeeHub.

1. Definitions

Capitalized terms not defined here have the meaning given in the Agreement.

- **Applicable Data Protection Law**: all privacy and data protection laws that apply to the processing of Customer Personal Data under the Agreement. This includes the California Consumer Privacy Act as amended by the CPRA ("CCPA"), other US state privacy laws and, where applicable, the EU GDPR, the UK GDPR and the Swiss FADP.
- **Customer Data**: all data that Customer, its users or its suppliers submit to the ZeeHub platform. This includes product, packaging, bill of materials, specification and compliance documents.

- **Customer Personal Data**: any personal data within Customer Data that ZeeHub processes on Customer's behalf.
- **Supplier**: any third-party vendor of Customer that ZeeHub contacts, at Customer's instruction, to request compliance data.
- **Subprocessor**: any third party ZeeHub engages to process Customer Personal Data.
- **Security Incident**: a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Customer Personal Data.
- **AI Model Provider**: a Subprocessor that provides large language model or other machine-learning inference services to ZeeHub.
- "Controller", "Processor", "Data Subject", "Business", "Service Provider", "personal data" and "processing" have the meanings given in Applicable Data Protection Law.

2. Roles, scope and instructions

1. **Roles.** Customer is the Controller (or Business) of Customer Personal Data. ZeeHub is the Processor (or Service Provider). Where Customer is itself a processor for a third party, ZeeHub is Customer's subprocessor, and Customer confirms it has authority to engage ZeeHub.
2. **Scope.** ZeeHub processes Customer Personal Data only to provide the services in the Agreement. The subject matter, duration, nature and purpose of processing, and the categories of data and Data Subjects, are set out in Annex 1.
3. **Instructions.** ZeeHub processes Customer Personal Data only on Customer's documented instructions. The Agreement, this DPA, and Customer's configuration of the platform (including which Suppliers to contact and which regulations to cover) are Customer's complete instructions. ZeeHub will tell Customer promptly if it believes an instruction violates Applicable Data Protection Law.
4. **Supplier outreach.** When Customer instructs ZeeHub to contact Suppliers, ZeeHub sends requests, reminders and follow-ups in Customer's name or on Customer's behalf. Customer is responsible for having a lawful basis to share Supplier contact details with ZeeHub and to contact those Suppliers.

5. **Customer responsibilities.** Customer is responsible for the accuracy and lawfulness of the Customer Data it provides. Customer will not submit special categories of personal data, government identifiers or payment card data to the platform.
6. **No regulatory filing.** ZeeHub prepares and organizes compliance data. It does not file regulatory reports, act as Customer's compliance representative, or certify compliance, unless the Agreement expressly says otherwise.

3. AI processing

1. **No model training.** ZeeHub will not use Customer Data to train, fine-tune or improve any machine-learning model, whether ZeeHub's own or an AI Model Provider's.
2. **Enterprise APIs only.** ZeeHub uses AI Model Providers only through enterprise API terms that prohibit the provider from training on inputs or outputs. Where the provider offers zero or limited data retention, ZeeHub will request it.
3. **No cross-customer reuse without consent.** ZeeHub will not share Customer Data, including Customer's bills of materials, specifications and Supplier responses, with any other ZeeHub customer. The one exception is Supplier-authored documents (such as a Supplier's own specification sheet), which ZeeHub may reuse for another customer only with the written consent of both the Supplier and Customer.
4. **Human review.** AI-generated extractions and checks are presented to Customer for review. Customer remains responsible for final compliance decisions and any regulatory submissions.

4. Confidentiality, personnel and security

1. **Personnel.** ZeeHub limits access to Customer Personal Data to personnel who need it to provide the services. All such personnel are bound by written confidentiality obligations and receive security training.
2. **Named access.** Only the ZeeHub engineers assigned to Customer's deployment may access Customer Data in production. ZeeHub will give Customer the list of those individuals on request.

3. **Security measures.** ZeeHub will implement and maintain the technical and organizational measures in Annex 2. ZeeHub may update those measures, provided the overall level of protection does not decrease.
4. **Customer systems.** Where Customer grants ZeeHub access to its ERP, spec or other systems, ZeeHub will use read-only credentials issued by Customer wherever possible. Customer may revoke those credentials at any time, and access stops immediately.

5. Subprocessors

1. **Authorization.** Customer gives general authorization for ZeeHub to engage Subprocessors. The Subprocessors in use on the date of this DPA are listed in Annex 3.
2. **Flow-down.** ZeeHub will impose data protection terms on each Subprocessor that are at least as protective as this DPA. ZeeHub remains liable for its Subprocessors' performance.
3. **Notice of changes.** ZeeHub will notify Customer by email at least 30 days before adding or replacing a Subprocessor.
4. **Objection.** Customer may object on reasonable data protection grounds within 15 days of that notice. The parties will discuss the objection in good faith. If they cannot resolve it, Customer may terminate the affected services and receive a pro-rata refund of prepaid, unused fees.

6. Assistance and Security Incidents

1. **Data Subject requests.** ZeeHub will promptly forward to Customer any request it receives from a Data Subject about Customer Personal Data, and will not respond directly unless Customer instructs it to. ZeeHub will help Customer respond, taking into account the nature of the processing.
2. **Other assistance.** ZeeHub will provide reasonable help with Customer's data protection impact assessments and consultations with regulators, to the extent these relate to ZeeHub's processing.

3. **Incident notice.** ZeeHub will notify Customer without undue delay, and in any case within 72 hours, after becoming aware of a Security Incident.
4. **Incident details.** The notice will describe, as far as then known, the nature of the incident, the categories and approximate volume of data affected, the likely consequences, and the steps ZeeHub is taking. ZeeHub will update Customer as more information becomes available.
5. **No admission.** ZeeHub's notice of a Security Incident is not an admission of fault or liability.

7. Audits, return and deletion

1. **Information.** On written request, no more than once a year, ZeeHub will answer Customer's reasonable security questionnaire. Where available, it will also share its most recent third-party audit report (for example a SOC 2 report) under confidentiality.
2. **Audits.** If that information does not reasonably show compliance with this DPA, or a regulator requires it, Customer may audit ZeeHub's relevant processing. Customer must give 30 days' written notice, and the audit must be conducted during business hours, be no more than once a year, and use an independent auditor bound by confidentiality. Customer bears its own audit costs.
3. **Logging.** ZeeHub logs every action taken on Customer Data in the platform and will provide relevant logs on reasonable request.
4. **Return.** During the term and for 30 days after it ends, Customer may export its Customer Data from the platform, or ask ZeeHub to provide an export in a standard format (such as CSV or JSON).
5. **Deletion.** ZeeHub will delete Customer Data, including Customer Personal Data, within 30 days after the Agreement ends. Backups are overwritten in the normal backup cycle, within 35 days. On request, ZeeHub will confirm deletion in writing.
6. **Retention by law.** ZeeHub may keep data only where the law requires it. Any such data stays subject to this DPA and is used for no other purpose.

8. US privacy laws and international transfers

1. **CCPA and US state laws.** To the extent the CCPA or a similar US state law applies, ZeeHub will not:
    - sell or share Customer Personal Data;
    - retain, use or disclose it for any purpose other than providing the services, or outside the direct business relationship with Customer;
    - combine it with personal data from other sources, except as those laws permit.
2. **CCPA compliance.** ZeeHub will comply with the CCPA and provide the same level of protection it requires. ZeeHub will notify Customer if it can no longer meet its obligations. Customer may take reasonable steps to stop and remediate unauthorized use. ZeeHub certifies that it understands these restrictions.
3. **Location.** ZeeHub hosts and processes Customer Data in the United States.
4. **EU, UK and Swiss data.** Where Customer Personal Data subject to the GDPR, UK GDPR or Swiss FADP is transferred to ZeeHub in the US, the EU Standard Contractual Clauses (Commission Decision 2021/914, Module 2, or Module 3 where Customer is a processor) are incorporated by reference. The UK International Data Transfer Addendum and the Swiss amendments apply to UK and Swiss transfers. Annexes 1 to 3 of this DPA complete the SCC annexes. The SCCs prevail over this DPA if the two conflict.

9. General terms

1. **Liability.** Each party's liability under this DPA is subject to the limitations and exclusions of liability in the Agreement.
2. **Term.** This DPA stays in effect for as long as ZeeHub processes Customer Personal Data.
3. **Precedence.** If this DPA conflicts with the Agreement on the processing of Customer Personal Data, this DPA prevails. The SCCs, where they apply, prevail over both.
4. **Changes in law.** If Applicable Data Protection Law changes, the parties will negotiate in good faith any amendment needed to keep complying.

5. **Governing law.** This DPA is governed by the law that governs the Agreement, except where Applicable Data Protection Law or the SCCs require otherwise.

Signatures

	ZeeHub	Customer
Entity	ZeeHub Inc	[Customer legal entity name]
Signature		
Name	Shekhar Nirkhe	
Title	Founder and CEO	
Date		
Privacy contact	hello@zeehub.ai	

Annex 1: Details of processing

Item	Details
Subject matter	Providing the ZeeHub supplier compliance platform under the Agreement
Duration	The term of the Agreement plus the 30-day return and deletion period
Nature of processing	Collection, storage, extraction, organization, validation, retrieval, transmission and deletion
Purpose	Requesting, collecting, checking and maintaining Supplier compliance data (for example packaging EPR, PFAS, RoHS, REACH and food-contact); preparing data for Customer's reporting; providing platform access and support
Data Subjects	Customer's employees and authorized users; Supplier employees and contacts; Customer's consultants or filers who are given access
Categories of personal data	Business contact data (name, job title, company, business email, business phone); user account data (login identifiers, role, activity logs); names and contact details that appear in Supplier documents and email correspondence
Special categories	None. Customer will not submit special categories of personal data.
Frequency	Continuous for the duration of the Agreement
Retention	As set out in Section 7

Annex 2: Security measures

Area	Measure
Hosting	Microsoft Azure, United States regions. Physical security is inherited from Azure data centers.
Encryption	TLS 1.2 or higher in transit; AES-256 at rest (Azure storage and database encryption)
Tenant isolation	Customer Data is logically separated by tenant, with a separate database or schema per customer
Access control	Role-based access; least privilege; access limited to named engineers assigned to the deployment; MFA required for all ZeeHub administrative and cloud console access
Customer credentials	Read-only, customer-issued credentials for connected systems wherever possible; stored in a secrets manager (Azure Key Vault); revocable by Customer at any time
Logging and monitoring	Every action on Customer Data logged; logs retained for 12 months; alerting on anomalous access
AI model providers	Enterprise APIs with training disabled; no Customer Data used to train models
Backups and recovery	Automated encrypted backups; retention 35 days; restore tested twice a year
Vulnerability management	Dependency and container scanning in CI; timely patching of critical vulnerabilities; annual third-party penetration test
Secure development	Code review on all production changes; separate development, staging and production environments; no Customer Data in development
Personnel	Confidentiality agreements, background checks where lawful, security training at onboarding and every year

Area	Measure
Incident response	Documented incident response plan; Customer notice within 72 hours (Section 6)
Certifications	SOC 2 Type I in progress, target Q1 2027

Annex 3: Authorized subprocessors

Subprocessor	Purpose	Data processed	Location
Microsoft Corporation (Azure)	Cloud hosting, storage, databases	All Customer Data	United States
Microsoft Corporation (Azure Foundry)	AI inference for document reading, extraction and checks	Documents and text sent for processing	United States
Google LLC (Google Workspace)	Email used to send Supplier requests and receive Supplier replies	Supplier contact data, email content, attachments	United States