DATA PROCESSING AGREEMENT (DPA)

Version 1.3 | As of: June 2026

Between:

The entity that has accepted this Agreement electronically during the registration process on https://vennie.tech, hereinafter referred to as the "data controller"

Vennie Tech UG
Bluntschlistr. 31
69115 Heidelberg
HRB 265814

hereinafter referred to as the "Processor"

1. Subject and Duration of Processing

1.1. The Processor processes personal data on behalf of the Controller within the scope of its AI-based customer support automation. This processing is exclusively to automate customer service, including identifying customer inquiries, retrieving relevant data from Shopify, and generating response suggestions via the customer support ticket system.

1.2. This Agreement takes effect upon electronic acceptance and remains valid as long as the Controller uses the AI chatbot. Upon termination of the use of the AI chatbot by the Controller, this Agreement shall automatically terminate unless otherwise agreed in writing.

1.3. The Controller shall provide the Processor with written notice of termination at least one month in advance, effective at the end of the following month, regarding the discontinuation of the AI chatbot.

2. Nature and Purpose of Processing

2.1. The Processor collects, stores, and processes the personal data of the Controller's end customers to respond to customer inquiries. This includes:

– Identifying the intent of the inquiry;
– Retrieving relevant order data from Shopify;
– Generating internal notes, answers, and suggestions for support responses;
– Transmitting the final response via the customer support ticket system.

2.2. Chat transcripts are automatically collected from the start date of the trial phase.

2.3. The Processor reserves the right to suspend processing if there are reasonable doubts regarding the lawfulness of the consent obtained by the Controller. The Processor shall notify the Controller immediately in such cases.

3. Types of Processed Data

3.1. The following personal data may be processed:

– Name and email address of the end customer

– Chat content of support inquiries

– May include health data, such as information regarding pregnancies, allergies, skin conditions etc.

– Order information (e.g., order number, product details)

– Any other data submitted within the inquiry that is necessary for the processing of the customer request.

3.2. Categories of Data Subjects: The personal data processed relates to the Controller's end customers and individuals who submit inquiries or requests via the customer support ticket system.

4. Rights and Obligations of the Controller

4.1. The Controller remains responsible for compliance with data protection regulations, particularly the GDPR. The Controller ensures that affected individuals are informed about data processing and that any necessary consents are obtained.

4.2. Upon request, the Controller shall provide the Processor with evidence of the lawfulness of the consents obtained from data subjects.

4.3. The Controller shall indemnify the Processor against any claims arising from the Controller's failure to comply with data protection laws or obtain lawful consent.

4.4. The Processor shall process personal data only based on documented instructions from the Controller, which shall be provided in writing (including via email) and logged by both parties for audit purposes. The Controller has the right to issue instructions at any time regarding:

– Deletion, correction, or restriction of personal data

– Modification of the scope of processing

– Security measures and access rights

4.5. The Controller is responsible for ensuring that all necessary consents, including explicit opt-in for the processing of sensitive data such as health data, are obtained from the data subjects by applicable data protection laws (including the GDPR). The Controller shall provide the Processor with proof of such consents upon request.

4.6. The Controller shall ensure that the processing of sensitive data, such as health-related information (e.g., information regarding pregnancies, allergies, skin conditions etc.), is only carried out if the appropriate legal basis, including valid and explicit consent, has been obtained from the data subjects prior to such processing.

The Processor shall implement these instructions without undue delay. If the Processor believes an instruction violates applicable data protection law, it must inform the Controller without delay via written notice, specifying the legal concern.

5. Obligations of the Processor

5.1. The Processor commits to:

– Processing data solely for contract fulfillment;

– Implementing appropriate technical and organizational measures (TOMs; see Annex 1) to protect the data;

– Transferring data only to third parties when necessary for the agreed processing (e.g., hosting providers, LLM providers);

– Enabling data subject rights (e.g., access, deletion) in cooperation with the Controller;

– Ensuring that all data is deleted from the Processor's servers no later than 180 days after processing unless legal retention obligations apply. The Processor shall notify the Controller of any applicable retention obligations.

5.2. The Processor shall conduct regular security audits and update its TOMs (Annex 1) to address new threats.

5.3. The Processor ensures that all persons authorized to process personal data have committed to confidentiality or are under an appropriate statutory obligation of confidentiality.

5.4. The Processor shall assist the Controller in meeting obligations under Articles 35 and 36 GDPR, where applicable, by providing necessary information and documentation to facilitate data protection impact assessments and prior consultations with supervisory authorities, as required for the processing activities.

5.5. The Controller shall have the right to verify the Processor's compliance with data protection requirements. To this end, the Processor shall:

– Allow the Controller to conduct audits and inspections at reasonable intervals;

– Provide relevant documentation on compliance;

– Cooperate with the Controller's requests for compliance verification.

The Controller must give at least 30 days' notice before an audit, and both parties must agree on the scope and duration to keep disruptions minimal.

6. Subprocessors

6.1 The Controller approves the participation of the listed subprocessors (as detailed in Annex 2).

6.2. Any further subcontracting requires prior approval from the Controller. The Processor shall notify the Controller of any proposed new subprocessor, and the Controller shall have 14 days to object based on documented legal non-compliance risks. If no objection is received within this period, the new subprocessor is deemed approved.

6.3. The Processor shall ensure that subprocessors comply with applicable data protection laws, including the use of the latest Standard Contractual Clauses (SCCs) approved by the European Commission for data transfers to third countries, where required. For transfers to countries without an adequacy decision (e.g., USA), the Processor relies on SCCs and existing technical measures to safeguard personal data. Copies of executed SCCs shall be provided to the Controller upon request. The Processor shall not be liable for any failure caused by the subprocessor unless directly resulting from the Processor's gross negligence or willful misconduct.

7. Security of Processing

7.1. The Processor commits to implementing appropriate security measures under Article 32 GDPR to ensure the confidentiality, integrity, and availability of personal data.

7.2. The Processor shall conduct regular security audits and update its security measures to address new threats.

8. Data Subject Rights and Requests

8.1. The Processor ensures that all requests for access, correction, deletion, or restriction of processing from data subjects are handled in compliance with GDPR. The process includes:

1. Receiving the request;
2. Verifying authenticity and eligibility, in cooperation with the Controller;
3. Forwarding the request to relevant subprocessors;
4. Providing a status update to the data subject;
5. Executing the necessary actions (e.g., retrieval, deletion);
6. Confirming the completion of the request.

8.2. All requests will be processed within the legally required timeframes. The Controller shall remain primarily responsible for verifying the authenticity of data subject requests.

9. Incident Management & Data Breaches

9.1. In the event of a personal data breach, the Processor will:

– Assess and mitigate risks;

– Notify the Controller within 24 hours of becoming aware of the breach, via written communication (e.g., email);

– Provide relevant details (e.g., nature of the breach, affected data, potential consequences, and mitigation steps) for compliance with GDPR reporting obligations under Article 33;

– Take corrective actions to prevent future incidents and document these actions for review by the Controller.

9.2. The Controller shall remain solely responsible for regulatory notifications or communications with affected data subjects. The Processor will provide reasonable assistance to the Controller in fulfilling its legal obligations.

9.3. The Processor shall not be liable for breaches caused by subprocessors unless directly resulting from the Processor's gross negligence or willful misconduct.

10. Data Deletion and Return

10.1. After the termination of the processing, the Processor shall, at the choice of the Controller, either return all personal data in a structured, commonly used format or delete it without undue delay. If the Controller does not specify, the data will be deleted no later than 180 days after contract termination, unless legal retention obligations apply. The Processor shall confirm the deletion or return of data in writing upon request.

10.2. The Processor may retain anonymized data for the purpose of improving its AI models, provided that such data is irreversibly anonymized in compliance with GDPR (e.g., through aggregation, pseudonymization, and removal of direct and indirect identifiers), ensuring no risk of re-identification. The Processor shall document the anonymization process and make it available to the Controller upon request.

11. Liability

11.1. The Processor is only liable for damages resulting from non-GDPR-compliant processing if caused by gross negligence or willful misconduct. The Processor is not liable for:

– Data protection breaches resulting from the Controller's failure to comply with applicable data protection laws;

– The Controller's failure to obtain necessary consent from data subjects;

– Inaccuracies or errors in the data provided by the Controller;

– Any security breach caused by vulnerabilities in the Controller's systems;

– Processing carried out in accordance with the Controller's documented instructions;

– Breaches caused by subprocessors, unless directly resulting from the Processor's gross negligence or willful misconduct.

11.2. Unless otherwise required by mandatory law, the Processor's total liability under this Agreement shall not exceed the total amount paid by the Controller for processing services in the last six months. This limitation shall be subject to applicable mandatory law.

12. Indemnification

12.1. The Controller shall indemnify, defend, and hold harmless the Processor from any claims, damages, penalties, or legal actions arising from:

– The Controller's non-compliance with applicable data protection laws;

– Failure to obtain lawful consent from data subjects;

– Inaccuracies in the data provided;

– Any legal claims resulting from the Controller's instructions to the Processor.

12.2. The Controller shall provide evidence of compliance with data protection laws upon request by the Processor.

13. Final Provisions

13.1. Changes and amendments to this Agreement must be made in writing.

13.2. If any provision is deemed invalid, the validity of the remaining provisions remains unaffected.

13.3. This Agreement shall be governed by German law. The exclusive place of jurisdiction for all disputes arising from or in connection with this Agreement shall be Heidelberg, Germany.

This Agreement is concluded through electronic consent during the registration process on https://vennie.tech.

The Agreement is deemed concluded as soon as the Controller has actively checked the corresponding checkbox during registration.

The date, time, and version of the agreed DPA will be stored and can be provided upon request.

Heidelberg, April 2026 Vennie Tech UG — Leon Jungfleisch

Annex 1: Technical and Organizational Measures (TOMs)

The Processor undertakes to implement technical and organizational measures that are appropriate to the risk of processing:

Technical Measures:

– Data Security: Transport Layer Security (TLS) / HTTPS is enforced.
– Access Control: Role-based access control (RBAC) is implemented.
– Server & API Security: No open ports, regular updates are performed.
– Automatic Deletion: Data is automatically deleted after 180 days.

Security Enforcement in Layers:

– NGINX Reverse Proxy: Blocks unauthorized external access.
– JWT Protection: Endpoints are secured via JWT for user authentication and logging.
– Database Access: Only the server can access the database through an IP whitelist and password protection.

Organizational Measures:

– Incident Response Plan: A structured approach to detecting, responding to, and mitigating security incidents.
– Safety Concept: Ensuring secure handling of data throughout its lifecycle.
– Incident Management: Notify the Controller about significant data protection breaches within a reasonable timeframe.
– Data Backup: Appropriate backup measures at the Processor's discretion.

The Processor does not apply pseudonymization, as the processing of support inquiries requires matching end customer identities to order data in real time, rendering pseudonymization technically incompatible with the purpose of processing (Art. 25(1) GDPR).

The Processor reserves the right to adjust these measures, provided that an equivalent level of protection is maintained. The Controller shall be notified of any material changes to TOMs within 14 days of implementation. The implementation of measures considers the state of the art, implementation costs, as well as the nature, scope, and purposes of the processing.

Annex 2: Subprocessor list

Subprocessor	Legal Form	Headquarters	Purpose
Pinecone Systems Inc.	Incorporated under US law (Delaware corporation)	1375 Broadway, 11th Fl, New York, NY 10018	Vector database for similarity search and retrieval.
OpenAI, L.L.C.	Incorporated under US law (Delaware LLC)	3180 18th Street, San Francisco, CA 94110, USA	Processing of inquiries via LLMs.
Amazon Web Services, Inc. (AWS)	Incorporated under US law (Delaware corporation)	410 Terry Avenue North, Seattle, WA 98109, USA	Processing and storage of personal data on AWS servers located within the European Economic Area.
Google LLC (as the provider of Google Cloud & Gemini, a subsidiary of Alphabet Inc., USA)	Limited Liability Company, under US law, is a subsidiary of Alphabet Inc.	1600 Amphitheatre Parkway, Mountain View, CA 94043, USA	Processing and storage of personal data on Google Cloud servers and processing of inquiries via LLMs. LLM inference performed via Vertex AI within the EEA.
Microsoft Azure (by Microsoft Corporation)	Incorporated under US law (Washington state corporation)	One Microsoft Way, Redmond, WA 98052, USA	Cloud computing services, infrastructure, and processing of inquiries via LLMs. LLM inference performed via Azure OpenAI Service in Europe (Sweden Central).
MongoDB	Incorporated under US law (Delaware corporation)	1633 Broadway, 38th Floor, New York, NY 10019, United States.	Atlas database hosted in Frankfurt, Germany.
Dysprosium Consulting, LLC	Incorporated under US law	2 Marchant Rd., Winchester, MA, 01890, USA	Research and development services.
Requesty Ltd	Private limited company under English & Welsh law (No. 15165717)	71–75 Shelton Street, Covent Garden, London WC2H 9JQ, UK	LLM routing platform; forwarding of prompts to third-party LLM providers and return of model outputs. Data stored in Frankfurt, Germany (EEA).