Data Processing Agreement

Pursuant to Art. 28 GDPR · Vanadio (a product of Vanilla Steel GmbH)

Template / pro-forma. Complete the [Customer] fields and execute alongside the Main Contract.

Data Processing Agreement

This Data Processing Agreement ("DPA") is entered into by and between Vanilla Steel GmbH ("Vanilla Steel" or "Processor"), a corporation organized and existing under the laws of Germany with its principal office at Schönhauser Allee 36, 10435 Berlin, Germany, and [Customer legal name] (the "Customer" or "Controller"), with its registered office at [Customer registered office], each also a "Party" and jointly the "Parties".

Preamble

Vanilla Steel develops quoting software for companies in the metal industry under the brand name Vanadio, supporting the conversion of unstructured requests for quotation into structured quotes (the "Quoting Tool").

Vanilla Steel has granted Customer a right to use the Quoting Tool under a separate agreement concluded between the Parties (the "Main Contract").

In the context of the provision of the services under the Main Contract, Vanilla Steel will process personal data on behalf and under the instructions of the Customer for which the Customer acts as controller within the meaning of (Article 4 (7) GDPR). This DPA shall remain in force for as long as the Main Contract remains in effect.

1. Subject and Duration of the DPA

This DPA specifies the rights and obligations of the Parties under data protection law in connection with the Processor's handling of personal data related to the provision of the contractual services under the Main Contract. The Processor shall carry out the data processing activities listed in Annex 1. Annex 1 describes the subject matter, nature, purpose, and duration of the processing, as well as the categories of personal data processed and the data subjects concerned.

2. Instructions of the Controller

a) The Processor shall process personal data only for the purposes listed in Annex 1 or based on documented instructions from the Controller — including with regard to transfers of personal data to a third country or an international organization — unless the Processor is required to do so under EU or EU Member State law to which it is subject. In such a case, the Processor shall notify the Controller of those legal requirements prior to processing, unless the relevant law prohibits such notification on important grounds of public interest.

b) The Processor shall inform the Controller without undue delay if, in its opinion, an instruction violates applicable data protection law.

c) Processing of personal data for purposes other than those defined by the Controller — particularly for the Processor's own purposes — is not permitted, unless expressly authorized under the Main Contract.

3. Technical and Organizational Measures

a) The Processor shall implement technical and organizational measures as listed in Annex 3 to ensure the security of personal data. These measures shall ensure a level of protection appropriate to the risk, in accordance with Article 32 of the GDPR.

b) The technical and organizational measures listed in Annex 3 are subject to technical progress and further development. The Processor shall adapt these measures if the level of security agreed upon at the time of concluding the DPA can no longer be guaranteed. Any adaptations must provide at least the same level of protection as the previous measures. The Processor shall document such adaptations and notify the Controller of any significant changes without being prompted.

4. Duties of the Processor

a) The Processor shall only grant its personnel access to the personal data undergoing processing to the extent strictly necessary for the purposes listed in Annex 1. The Processor shall ensure that the persons authorized to process the personal data received are bound by confidentiality obligations or are subject to an appropriate legal duty of confidentiality.

b) Notwithstanding Section 7 of this DPA, the Processor shall provide the Controller with evidence of its compliance with its obligations under this Section 4 upon request.

5. Support Obligations of the Processor

a) Taking into account the nature of the processing and the information available to it, the Processor shall assist the Controller in ensuring compliance with its obligations under Articles 32 to 36 GDPR as well as Chapter III GDPR. This includes support in carrying out a data protection impact assessment, conducting any necessary consultations with supervisory authorities, and responding to data subjects' requests to exercise their rights. The Processor shall inform the Controller without undue delay of any such request or assertion of rights by data subjects.

b) The Processor shall provide reasonable assistance through appropriate technical and organizational measures to enable the Controller to fulfil its obligations under the GDPR.

6. Authorisation to Establish Subcontracting Relationships

a) The Controller authorizes the Processor to engage sub-processors for the direct provision of the services under the Main Contract involving the processing of personal data (Article 28 (2) GDPR). The current list of sub-processors is set out in Annex 2. The Processor shall notify the Controller of any intended changes concerning the addition or replacement of sub-processors. The notification shall include the name, address, a description of the processing activities, location of the data processing, and any relevant information regarding appropriate safeguards pursuant to Articles 44 et seq. GDPR. The Controller may object to such changes within two (2) weeks of receiving the notification at ian.madege@vanillasteel.com, provided that there are objective reasons for the objection. If the Controller raises an objective objection and it is not reasonably feasible for the Processor to replace the sub-processor, the Parties shall cooperate in good faith to find a mutually acceptable solution.

b) Sub-processors shall not be granted access to personal data until two (2) weeks after the notification pursuant to Section 6 a) of this DPA have elapsed without objection from the Controller, and until the Processor has entered into a contract with the sub-processor – concluded in writing or in electronic form – that imposes on the sub-processor the same data protection obligations as set out in this DPA, in accordance with Article 28 (4) GDPR. Upon request, the Processor shall provide the Controller with a copy of the sub-processing agreement and any subsequent amendments. Without limiting Section 7 of this DPA, if such documentation contains commercial or other confidential information, the Processor may redact those parts.

c) The Processor shall remain fully liable to the Controller for the sub-processor's compliance with its contractual obligations. The Processor shall also notify the Controller without undue delay of any breach of contractual obligations by a sub-processor.

d) In cases where sub-processing involves a transfer of personal data to a third country within the meaning of Chapter V of the GDPR, the Processor shall ensure compliance with Articles 44 et seqq. GDPR, including by implementing appropriate safeguards under Article 46 GDPR, where necessary. The sub-processor may only begin processing once an adequate level of data protection has been ensured.

7. Control Rights

a) The Processor shall provide the Controller with the information necessary to demonstrate compliance with the obligations set out in this DPA or directly resulting from the GDPR. Upon request by the Controller, the Processor shall allow for and contribute to audits of the processing activities covered by this DPA, either at reasonable intervals or where there are specific indications of non-compliance. In deciding whether to conduct an audit, the Controller may take into account relevant certifications of the Processor pursuant to Article 28 (5) GDPR.

b) Audits may be carried out by the Controller directly or by a qualified, independent third party auditor mandated by the Controller. Audits may include inspections of the Processor's premises or facilities, where appropriate, and shall be conducted with reasonable prior notice, during normal business hours, and in a manner that avoids disruption to operations and respects the Processor's business and trade secrets, unless required otherwise by a competent supervisory authority within the scope of its legal powers.

c) The Parties shall make the information referred to in this DPA, including audit results, available to the competent supervisory authorities upon request.

d) Where the facilitation of or cooperation with audits or other assistance required by law or covered by this DPA exceeds the Processor's contractual obligations under the Main Contract and the Annex 1, and this additional expense is not attributable to any fault or breach by the Processor, the Controller shall reimburse the Processor for any reasonable additional expenses incurred. This may be the case, for example, if an audit was carried out less than twelve (12) months prior and there is no reason to carry out another audit before the expiration of a reasonable interval. The Processor shall inform the Controller in advance of such additional costs by providing an estimate, and shall await the Controller's written approval before proceeding. If the Processor implements such measures without prior written approval, it waives the right to reimbursement under this section.

8. Notification of Breaches

The Processor shall inform the Controller without undue delay of any disruptions to operations that may pose a risk to the Controller's personal data, and of any personal data breach that the Processor becomes aware of in connection with the Controller's data.

The Processor acknowledges that the Controller may be subject to obligations to document, and in some cases report, such personal data breaches to supervisory authorities or affected data subjects under the GDPR.

Upon becoming aware of a personal data breach, the Processor shall notify the Controller without undue delay and shall provide, to the extent possible, the following information:

– A description of the nature of the breach, including, where feasible, the categories and approximate number of data subjects and data records concerned;
– The name and contact details of a contact person for further information;
– A description of the likely consequences of the breach; and
– A description of the measures taken or proposed to address the breach and mitigate its possible adverse effects.

9. Termination of the DPA

a) Upon termination of the commissioned processing, the Processor shall, at the choice of the Controller, either delete or return all personal data, unless EU or EU Member State law requires storage. This also applies to any backup copies in accordance with the technical and organizational measures taken. The Processor shall confirm deletion in text form upon request. "Text form" may include email or other electronic communication.

b) This DPA shall automatically terminate upon expiration or termination of the Main Contract. The right of either Party to terminate the DPA for cause remains unaffected. This includes the right of the Processor to terminate if the Controller insists on an instruction that violates applicable EU or EU Member State law or this DPA, despite having been informed accordingly.

10. Liability

a) The Controller and the Processor shall be jointly and severally liable for damage suffered by a data subject resulting from unlawful or otherwise non-compliant data processing within the scope of this DPA according to Art. 82 GDPR.

b) The Processor shall bear the burden of proof that the damage is not attributable to it, insofar as the data was processed under this DPA. Until such proof is provided, the Processor shall indemnify the Controller upon first request against all third-party claims arising in connection with the data processing.

c) Paragraph b shall not apply if the damage results from the proper execution of a processing activity or a lawful instruction issued by the Controller.

d) Unless otherwise provided herein, the limitation of liability under the Main Contract shall apply to the legally permissible extent.

11. Final Provisions

a) If the Controller's property or data in the possession of the Processor is endangered by measures of third parties (e.g. attachment or seizure), insolvency proceedings, or other events, the Processor shall notify the Controller without undue delay.

b) The Processor shall not have any right of retention with respect to the Controller's data carriers or data files.

c) In order to be valid, this DPA, any amendments to it, and any ancillary data protection agreements between the Parties must be made in writing; text, including electronic, form shall be sufficient.

d) Should individual provisions of this DPA be or become invalid, the validity of the remaining provisions shall remain unaffected.

e) To the extent that this DPA does not contain specific provisions, the provisions of the Main Contract shall apply. In the event of any conflict between this DPA and the Main Contract, the provisions of this DPA shall prevail.

12. Governing Law and Settlement of Dispute

a) This Agreement shall be governed by and interpreted in accordance with the laws of Germany, excluding the United Nations Convention on Contracts for the International Sale of Goods (CISG).

b) In the event of any dispute, controversy or claim arising out of or relating to this Agreement, or the breach, termination or invalidity hereof, the Parties shall, where reasonable, attempt in the first instance to resolve such dispute by amicable agreement.

c) All disputes arising out of or in connection with the present Agreement not resolved by amicable agreement shall be finally settled under the Rules of Arbitration of the International Chamber of Commerce in Berlin, Germany by one arbitrator appointed in accordance with the said Rules. Exclusive language of the arbitration proceedings shall be English. Documents originally existing in the German language may be submitted in the German language. The Parties shall be entitled to file for interim measures (vorläufigen Rechtsschutz) with the ordinary courts of law if the final settlement is made by the competent arbitral court.

Annexes

Annex 1 Overview of the commissioned services and contact details of DPO/Data Protection Contact

Annex 2 List of appointed sub-processors including processing locations

Annex 3 Technical and organizational measures for data security according to Art. 32 GDPR

Annex 1: Overview of the commissioned services and contact details of DPO/Data Protection Contact

Subject, nature and purpose of the data processing activities

Provision of the Quoting Tool as a Software-as-a-Service, including further development and testing of the Customer's instance of the Quoting Tool, as well as hosting, maintenance and support services under the Main Contract.

Types of personal data

Project-related data provided by the Controller for which a (at least indirect) identifiability of the data subject cannot be ruled out. This includes:

- Personal information: Name
- Business-related information: Company name, email address, phone number, job description

– Technical data: IP address, usage data, device data
– General company information, insofar as these are to be considered as personal data according to GDPR

Categories of persons concerned

– Business partners of the Controller, where these are themselves natural persons, and/or their employees and members of corporate bodies
– Employees and freelance consultants of the Controller

Duration for the data processing activities

The duration of the processing corresponds to the duration of the Main Contract.

Data Protection Officer / Data Protection Contact of the Processor

DPO: Not applicable.

Data Protection Contact of the Processor: ian.madege@vanillasteel.com

Data Protection Officer of the Controller

[Please add]

Annex 2: List of appointed sub-processors including processing locations

Sub-processor	Location	Purpose
Google Cloud EMEA Limited, Velasco, Clanwilliam Place, Dublin 2, Ireland	Europe West (Berlin, Frankfurt)	Use of Google Cloud Platform for hosting and operating the Quoting Tool: managed databases (Cloud SQL, Cloud Memorystore for Redis), compute and container infrastructure (Compute Engine, Cloud Run, Kubernetes Engine), analytics (BigQuery), networking and load balancing, and centralized logging (Cloud Logging).
OpenAI Ireland Ltd, 1st Floor, The Liffey Trust Centre, 117-126 Sheriff Street Upper, Dublin 1, D01 YC43, Ireland (EEA contracting entity of OpenAI, L.L.C., San Francisco, USA)	European Union (European data residency for the API is enabled on Vanilla Steel's account; transfer safeguards for any residual transfers: EU Standard Contractual Clauses as incorporated in OpenAI's Data Processing Addendum)	Use of the OpenAI API (large language models) to extract structured specifications from RFQs and related documents provided by the Controller and to support matching and quote generation. API inputs and outputs are processed solely to provide the service, are not used for model training, and are subject to zero data retention (requests and responses are not stored at rest) under OpenAI's Services Agreement and Data Processing Addendum.
Dropbox International Unlimited Company, One Park Place, Floor 5, Upper Hatch Street, Dublin 2, D02 FD79, Ireland	European Union (file data at rest in Frankfurt, Germany, with backup in France; certain metadata is processed in the United States; transfer safeguards: EU Standard Contractual Clauses as incorporated in Dropbox's Data Processing Agreement)	Use of Dropbox as a secure file exchange for the data provided by the Controller during the set-up and pilot phase (RFQs, quotes, price lists, inventory exports, product catalogues, customer master data), pending ingestion into the Quoting Tool.

Annex 3: Technical and organizational measures for data security according to Art. 32 GDPR

1. General

The Processor ensures the implementation and compliance with the required technical and organisational measures in accordance with Article 32 GDPR. These measures include those designed to ensure the ongoing confidentiality, availability, and resilience of processing systems and services.

The Processor uses procedures and documentation that provide for the regular testing, assessment, and evaluation of the effectiveness of the implemented technical and organisational measures, to ensure the security of processing.

The Processor leverages Google Cloud EMEA Limited, Velasco, Clanwilliam Place, Dublin 2, Ireland ("Google Cloud") for cloud infrastructure, which is certified with industry-leading standards such as ISO 27001, ISO 27017, and ISO 27018, ensuring robust security controls.

The following section outlines the technical and organisational measures, divided into those implemented by the Processor and by the key sub-processor Google Cloud EMEA Ltd ("Google"). This sub-processor has been selected based on its secure infrastructure and data protection guarantees. Data on the platform is processed in European data centres.

2. Processor

The following measures describe how the Processor ensures the confidentiality, integrity, availability, and resilience of its systems and services.

The Processor does not operate the platform infrastructure itself but relies on services and infrastructure provided by Google. Google has been carefully selected based on its data security measures and is subject to ongoing assessment and monitoring through the Processor's vendor management process.

The following measures and processes are implemented by the Processor:

a) Confidentiality. To ensure confidentiality, role-based access controls and multi-factor authentication (MFA) are implemented. Data is encrypted both at rest and in transit, and regular security assessments are conducted.

b) Integrity. To maintain integrity, hashing and cryptographic signatures are used to detect tampering. Sensitive data changes are tracked via versioning and audit logs, supported by regular security reviews and code audits. Regarding availability, the system is designed with redundant server and database architectures, including failover mechanisms. Automated backups are performed, accompanied by regular recovery tests, and protections are in place against DDoS attacks and system overload.

c) Resilience of processing systems and services. The resilience of processing systems and services is supported by business continuity management, automated system monitoring with anomaly alerts, and regular updates and patch management.

d) Ability to restore availability and access to personal data in a timely manner. The ability to restore availability and access to personal data in a timely manner is ensured through business continuity measures, structured backup procedures, and a disaster recovery plan.

e) Pseudonymisation and encryption of personal data. In terms of pseudonymisation and encryption of personal data, techniques such as hashing or tokenisation are applied, and plaintext data processing is minimised through anonymisation techniques.

f) Regular testing, assessment and evaluation of the effectiveness of TOM. Finally, the regular testing, assessment, and evaluation of the effectiveness of technical and organisational measures is ensured through vulnerability assessments, both internal and external audits of security policies, and annual employee training on data protection and security requirements.

3. Google Cloud

The platform infrastructure is operated on Google Cloud. Google Cloud's technical and organizational measures include, in particular: physically secured, geographically distributed data centers with redundant power and network infrastructure; encryption of data in transit (HTTPS/TLS); layered network security with intrusion detection and incident response; strict physical and logical access controls (unique user IDs, multi-factor authentication, need-to-know access, logged and audited access management); logical isolation of customer data and a verified erase policy for decommissioned storage media; personnel security (background checks, confidentiality agreements, security training); and security audits of its own subprocessors.

These measures are certified under ISO 27001, ISO 27017 and ISO 27018 and are documented in Google Cloud's current security documentation and Cloud Data Processing Addendum (cloud.google.com/security, cloud.google.com/terms/data-processing-addendum), which together form the reference for the measures implemented at the infrastructure level.