Data Processing Agreement

1. Entry provisions

1.1 Parties

This Data Processing Agreement ("DPA") according to Art 28 GDPR is concluded between:

CLIENT
in the following „CONTROLLER"
and the

Cortecs GmbH
Althanstraße 4
1090 Vienna
Austria
in the following „PROCESSOR".

1.2 Definitions

PROCESSOR refers to a processor within the meaning of Art. 4 No. 8 of the General Data Protection Regulation.

DATA refers to personal data within the meaning of Art. 4 No. 1 of the General Data Protection Regulation.

GDPR refers to the General Data Protection Regulation in its current version. CONTROLLER refers to a controller within the meaning of Art. 4 No. 7 of the General Data Protection Regulation.

CONTRACTING PARTIES include the contractor and the client.

SUB-PROCESSOR refers to another processor whose services the PROCESSOR uses to carry out certain processing activities.

1.3 Preamble

According to Art. 4 No. 8 GDPR, a natural or legal person, public authority, agency, or other body that processes personal data on behalf of the controller is to be qualified as a processor. In this case, the contracting parties are obliged to conclude a data processing agreement in accordance with Art. 28 GDPR. By signing this DPA, the

contracting parties comply with this obligation. The processor provides sufficient guarantees that appropriate technical and organizational measures will be implemented in such a manner that processing will meet the requirements of the GDPR and ensure the protection of the rights of the data subjects (Art. 28 para. 1 GDPR).

2. Main part

2.1 Object, duration, nature and purpose of the processing (Art. 28 para 3 GDPR)

This contract is concluded for an indefinite period. It ends as soon as the provision of the commissioned service ends. The subject and nature of this DPA can be described as follows:
— Receiving, routing, and forwarding input (which may include personal data)
— Returning the result to the CONTROLLER
— Ensuring secure and reliable operation of the routing system

2.2 Type of personal data and categories of data subjects (Art. 28 para 3 GDPR)

Types of DATA: Any personal data submitted via prompts, authentication data, usage metadata and user identifiers

Categories of data subjects: End users of controller, Employees, Customers, Individuals whose personal data is entered into the routing system

2.3 Processing only on documented instruction (Art. 28 para 3 lit a GDPR)

The PROCESSOR will process DATA only on documented instruction from the CONTROLLER within the framework of the agreement made, including with regard to the transfer of DATA to a third country or an international organization, unless the PROCESSOR is obliged to do so by the law of the European Union or the Member States to which the PROCESSOR is subject; in such a case, the PROCESSOR will inform the CONTROLLER of these legal requirements before processing, unless the relevant law prohibits such notification due to an important public interest.

2.4 Obligation of confidentiality (Art. 28 para 3 lit b GDPR)

The PROCESSOR ensures that persons authorized to process the DATA have committed themselves to confidentiality or are under an appropriate statutory obligation of secrecy. This obligation continues even after the contractual relationship has ended.

2.5 Obligation to implement the necessary measures (Art. 28 para 3 lit c GDPR)

The PROCESSOR ensures that all measures required under Article 32 GDPR are taken.

The PROCESSOR has provided the CONTROLLER with a list of the specific technical and organizational measures (hereinafter referred to as "TOMs") that have been taken or are being implemented on an ongoing basis before the conclusion of this data processing

agreement. This list of TOMs is attached to this contract as Annex I and is to be regularly re-evaluated and adjusted by the PROCESSOR.

2.6 Support obligations (Art. 28 para 3 lit e GDPR)

The PROCESSOR will assist the CONTROLLER, considering the nature of the processing, with appropriate technical and organizational measures to the extent possible, in fulfilling the CONTROLLER's obligation to respond to requests for exercising the rights of the data subject as set out in Chapter III of the GDPR. The PROCESSOR will only provide information to third parties or data subjects upon instruction from the CONTROLLER.

2.7 Information obligations (Art. 28 para 3 lit f GDPR)

The PROCESSOR will assist the CONTROLLER, considering the nature of the processing and the technical information available to them, in complying with the obligations set out in Articles 32 to 36 of the GDPR.

2.8 Return and deletion of data (Art. 28 para 3 lit g GDPR)

The PROCESSOR will, after the completion of the processing services, either delete or return all DATA at the choice of the CONTROLLER, unless there is an obligation to store the DATA under Union law or the law of the Member States.
Notwithstanding the general deletion obligations:
- Processor Retention: The parties acknowledge that Payload Content (prompts & completions) is processed by the PROCESSOR solely in volatile memory and is deleted immediately from the PROCESSOR's infrastructure upon the completion of the routing request. Consequently, the manual return or recovery of such specific data by the PROCESSOR is technically impossible.
- Sub-processor Retention: Data transmitted to an Inference Sub-processor is subject to the data retention policies of that specific provider. The CONTROLLER acknowledges that while the PROCESSOR provides technical filters to select providers with Zero Data Retention, it is the CONTROLLER'S responsibility to configure their routing logic to avoid Sub-processors whose retention policies do not meet their compliance requirements."

2.9 Options for verification (Art. 28 para 3 lit h GDPR)

The PROCESSOR will provide the CONTROLLER with all necessary information to demonstrate compliance with the obligations laid down in Art. 28 GDPR and will allow for and contribute to audits – including inspections – conducted by the CONTROLLER or another auditor mandated by the CONTROLLER.

2.10 Duty to inform in the event of a data breach (Art. 28 para 3 lit h GDPR)

The PROCESSOR will inform the CONTROLLER without delay if they believe that an instruction violates the GDPR or other data protection provisions of the Union or Member States.

cortecs®

2.11 Engagement of sub-contractors (Art. 28 para 4 GDPR)

If the PROCESSOR engages the services of another processor (hereinafter referred to as SUB-PROCESSOR) to carry out certain processing activities on behalf of the CONTROLLER, the same data protection obligations as set out in the contract or other legal instruments between the CONTROLLER and the PROCESSOR will be imposed on this SUB-PROCESSOR by means of a contract or other legal instrument under Union law or the law of the relevant Member States. In particular, sufficient guarantees must be provided that the appropriate technical and organizational measures will be implemented in such a manner that the processing will meet the requirements of the GDPR. If the SUB-PROCESSOR fails to fulfill its data protection obligations, the PROCESSOR will be liable to the CONTROLLER for the compliance with the obligations of that SUB-PROCESSOR.

The CONTROLLER acknowledges that the SERVICE allows for the dynamic selection of Upstream Inference Providers. The CONTROLLER authorizes specific Sub-processors by configuring the routing logic (e.g., via Dashboard or API parameters) to direct traffic to those providers. If the CONTROLLER configures the SERVICE to avoid specific providers, those entities shall not process the CONTROLLER'S data.

> **Upstream Inference Providers:** These sub-processors are engaged to provide generative AI model inference. When the CONTROLLER uses the Services, data put into the routing system is processed by these providers to generate a response. A complete list is provided at https://cortecs.ai/dpa.
> **Routing Service Sub-processors:** These sub-processors provide essential services to operate the CONTROLLER's platform. The sub-processors used for application and router hosting in this category will necessarily process data that flows through our Services for the purpose of operating and delivering the service. A complete list is provided at https://cortecs.ai/dpa.

The CONTROLLER agrees to the engagement of the mentioned SUB-PROCESSORS. The CONTROLLER grants a general authorization for the PROCESSOR to engage other SUB-PROCESSORS. However, the PROCESSOR must always inform the CONTROLLER of any intended changes regarding the engagement or replacement of other SUB-PROCESSORS. The CONTROLLER has the right to object to such changes within 30 days (Art. 28 para. 2 GDPR), otherwise, consent is assumed. The PROCESSOR undertakes to comply with the conditions set out in Art. 28 para. 2 and 4 GDPR for the engagement of another SUB-PROCESSOR (Art. 28 para. 3 lit d GDPR).

2.12 No Training on Customer Data

The PROCESSOR warrants that it shall not use Customer Data to train, fine-tune, or improve any Artificial Intelligence models.

— Standard Providers: Regarding Sub-processors, the PROCESSOR warrants that, unless otherwise indicated in the Service Interface, it engages with Inference

Providers that provide binding legal assurances prohibiting the use of Customer Data for model training.

— Experimental Providers: The PROCESSOR may offer access to specific Sub-processors marked as "Beta" or "Experimental" (or similar designations) within the Service Interface. The CONTROLLER acknowledges that these specific providers may not offer a legally-binding "No Training" guarantee. The Warranty for Standard Providers does not apply to these designated providers.

— The Service allows the CONTROLLER to configure routing rules to exclude or include such providers. By configuring the Service to route traffic to a designated "Beta" provider, the CONTROLLER explicitly instructs the PROCESSOR to transfer data to that provider according to that provider's specific terms of service.

3. Closing provisions

3.1 Partial invalidity / Severability clause

Invalid provisions of individual contractual components of this DPA do not affect the validity of the remaining provisions. Instead of the invalid provisions, appropriate replacement provisions shall apply, which, in light of the purpose of the contract, come closest to what the CONTRACTING PARTIES would have intended if they had known about the invalidity. The same applies to contractual gaps. In case of doubt, the rules of Art. 28 GDPR shall apply.

3.2 Applicable law and place of jurisdiction

This agreement (and all contractual components related to it) is governed by Austrian law and is deemed to be validly agreed upon. The application of the United Nations Convention on Contracts for the International Sale of Goods (CISG) is excluded. For the resolution of disputes regarding the validity of this agreement (and all contractual components related to it), arising from the contract and after the termination of this contract, the court with jurisdiction over the 9th district of Vienna is exclusively declared competent.

3.3 Costs of participation

The PROCESSOR is entitled to a separate reimbursement of costs for the cooperation required by law and contract (especially in the course of an audit or the exercise of data subject rights). However, there is no claim for reimbursement of costs if the effort in this context is very low (effort of less than four hours per month).

Annex - TOMs

Technical measures

1. Data transmission

All personal data is transmitted exclusively over secure communication channels using strong encryption (TLS 1.2 or higher). This applies to both external traffic between the Controller and the Service, as well as internal traffic between the Gateway and Upstream Inference Providers, ensuring end-to-end security of the payload. All APIs and web interfaces are accessible only via HTTPS, with HTTP Strict Transport Security (HSTS) enforced to prevent protocol downgrade attacks.

2. Access control

Access to systems is restricted to authorized users via robust authentication mechanisms including API Keys. Sensitive authentication data, specifically Upstream API Keys and Customer API credentials, are encrypted at rest using industry-standard algorithms (e.g., AES-256) and are never stored in plain text. Administrative access to the production routing infrastructure is limited to a minimal set of authorized personnel based on the principle of least privilege and requires Multi-Factor Authentication (MFA).

3. Data economy

The processing of Content Data (specifically Prompts and Completions) is performed strictly in volatile memory (RAM). Content Data is not written to persistent storage or disk at any point during the routing process. Once the API response is returned to the Controller, the payload data is immediately discarded from the Processor's infrastructure, enabling Zero Data Retention.

4. Backup and system recovery

Regular backups are performed to ensure the resilience of Account Data, including user configurations, billing records, and routing rules. Crucially, Payload Data (prompts & completions) is explicitly excluded from all backup routines to ensure compliance with the zero-retention policy. The routing infrastructure utilizes a multi-cloud strategy; if a primary Upstream Provider fails, the system is architected to automatically failover to configured backup providers (if enabled by the Customer) to ensure high availability without compromising data retention standards.

5. Privacy by design

Privacy principles are integrated into the architecture from the outset, specifically through the strict separation of logging data. System logs capture only operational metadata (such as timestamps, token counts, and error codes) required for metering and debugging, while technical filters ensure that the actual Payload is never written to system logs or debugging traces.

cortecs®

Organizational measures

1. Data protection policies and procedures

Creation of clear data protection policies and procedures to ensure compliance with the GDPR and clearly define the responsibilities of employees. Ensuring that data protection policies are regularly reviewed, updated, and understood and followed by all employees.

2. Awareness

Regular training sessions and training materials for employees to raise their awareness of data protection regulations and keep them up to date with best data protection practices.

3. Data confidentiality

Employees are obligated to maintain data confidentiality.

4. Data processing agreements

Conclusion of written contracts with processors that regulate the processing of personal data in accordance with the requirements of the GDPR and ensure that processors implement appropriate security measures.

5. Incident-response plan

Development of a clear plan for responding to data breaches, which includes procedures for reporting incidents, investigating data breaches, and notifying affected individuals.

6. Need-to-know principle

The need-to-know principle is strictly implemented and technically supported by appropriate authorization concepts.

cortecs®