



Data Processing Agreement

AI Router Switzerland

Classification: Public

Vaikoon AG

Gotthardstrasse 47
CH-6045 Meggen

Register # CH-100.3.798.146-9
VAT # CHE 318.570.988

www.vaikoon.com
office@vaikoon.com

Table of Content

1	Scope, parties and definitions	3
2	Roles and processing.....	4
3	Security and Security Breaches	5
4	Information and audits	5
5	Hosting, Sub-processors and transfers	6
6	Retention and deletion.....	7
7	Cooperation	7
8	Liability and final provisions	8
	Annex 1 – Details of the processing	9
	Annex 2 – Technical and organisational measures	10

I Scope, parties and definitions

1.1 Scope

This DPA applies where and to the extent that Vaikoon processes Customer Personal Data as a processor on behalf of the Customer in the course of providing the Service, and the Customer is a controller whose processing is subject to the GDPR and/or the FADP – in particular where the Customer uses the Service for professional or commercial purposes.

1.2 Personal use

Where the Customer is a natural person who uses the Service exclusively for purely personal or household purposes, the GDPR (art. 2 (2) lit. c) and the FADP (art. 2 (2) lit. a) do not apply to the Customer's processing, and this DPA does not apply. Vaikoon's processing is then governed by its privacy policy (airouter.ch/privacy.html). The commitments on the handling of Customer Content in clauses 2.6, 3.1, 5.1 and 6.1 are applied by Vaikoon to all Customers in the same way.

1.3 Vaikoon as controller

This DPA does not apply to personal data which Vaikoon processes as controller in accordance with its privacy policy, in particular account, subscription and billing data of the Customer, and payment data processed by Vaikoon's payment service provider.

1.4 Customer and Account Owner

"Customer" means the natural person or legal entity that has registered for and holds a subscription to the Service. The Customer acts towards Vaikoon exclusively through the holder of the Customer's account (the "Account Owner"). Instructions, notices, requests and other communications under this DPA are given by and to the Account Owner at the e-mail address registered for the account, and Vaikoon may rely on them. No further representatives or contact persons are designated.

1.5 Definitions. In this DPA

"Applicable Data Protection Law" means the GDPR, the FADP, the Swiss Data Protection Ordinance ("DSV") and the national laws of the member states of the EU/EEA supplementing the GDPR, in each case as amended or replaced; "Customer Personal Data" means personal data which Vaikoon processes on behalf of the Customer in the course of providing the Service; "Customer Content" means the inputs submitted by or on behalf of the Customer to the Service (in particular prompts, messages, system instructions, documents, text and audio) and the outputs generated by the Service in response (in particular completions, embeddings, transcriptions and synthesised audio); "Technical Data" means the metadata generated when the Service is used, as described in Annex 1, which does not contain Customer Content; "Security Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Customer Personal Data; "Sub-processor" means any processor engaged by Vaikoon to process Customer Personal Data. The terms "controller", "processor", "processing" and "data subject" have the meanings given to them in Applicable Data Protection Law.

1.6 Conclusion and term

This DPA takes effect upon acceptance of the ToS and applies for as long as Vaikoon processes Customer Personal Data on behalf of the Customer. Acceptance in electronic form satisfies the form requirement of art. 28 (9) GDPR; art. 9 FADP does not impose a form requirement. Individually negotiated versions, separately signed copies or additional terms are not offered.

2 Roles and processing

2.1 Roles

The Customer is the controller and Vaikoon is the processor of Customer Personal Data. Where the Customer itself acts as processor on behalf of a third party, Vaikoon acts as its sub-processor; in that case the Customer is responsible for obtaining any authorisation required from its controller and for passing on to it the information provided under this DPA.

2.2 Instructions

Vaikoon processes Customer Personal Data only on documented instructions of the Customer. The ToS, this DPA and the Customer's use and configuration of the Service via the API (in particular the choice of models, endpoints and parameters) constitute the Customer's complete and final instructions. As the Service is a standardised service, Vaikoon is not obliged to implement instructions which go beyond or deviate from it; in that case the Customer may terminate its subscription in accordance with the ToS. Vaikoon informs the Customer without delay if, in its opinion, an instruction infringes Applicable Data Protection Law (art. 28 (3) last subparagraph GDPR).

2.3 Legally required processing

Where Vaikoon is required by Swiss law to process or disclose Customer Personal Data without an instruction of the Customer, it informs the Customer before doing so, unless the law prohibits such information on important grounds of public interest.

2.4 Customer responsibilities

The Customer is responsible for its lawful use of the Service and for the lawfulness of its processing of Customer Personal Data. In particular, the Customer ensures that it has a legal basis or justification for submitting Customer Personal Data to the Service, that it has informed data subjects as required and obtained any consents required, and that its instructions comply with Applicable Data Protection Law.

2.5 No assessment of Customer Content

Customer Content is processed automatically. Vaikoon does not monitor, inspect or assess Customer Content and has no obligation to identify personal data or information subject to specific legal or regulatory requirements in it. The Customer is responsible for determining whether its use of the Service meets its own requirements and legal obligations, in particular before submitting special categories of personal data (art. 9 and 10 GDPR; art. 5 lit. c FADP).

2.6 No use for Vaikoon's own purposes

Vaikoon does not process Customer Personal Data for its own purposes. In particular, Vaikoon does not use Customer Content to train, fine-tune or evaluate artificial intelligence models, does not log the content of inputs or outputs, and does not use Customer Content for product development, benchmarking or statistics. The Customer instructs Vaikoon to process Technical Data for the operation, security and stability of the Service, the prevention and detection of abuse, the enforcement of the fair-use limits of the ToS and capacity planning, and to anonymise or aggregate Technical Data for these purposes (the "Permitted Purposes"). Data so anonymised is no longer Customer Personal Data.

2.7 Confidentiality

Vaikoon treats Customer Personal Data as confidential and grants access only on a need-to-know basis to persons who are bound by an appropriate contractual or statutory obligation of confidentiality and who are instructed in the applicable data protection and security requirements.

3 Security and Security Breaches

3.1 Security measures

Vaikoon implements and maintains the technical and organisational measures described in Annex 2, taking into account the state of the art, the costs of implementation, the nature, scope, context and purposes of the processing and the risks for the data subjects (art. 32 GDPR; art. 8 FADP in conjunction with art. 1 to 5 DSV). Vaikoon may update the measures provided that the overall level of protection is not reduced.

3.2 Customer security responsibilities

The Customer is responsible for the security of its own systems and of its account. In particular, the Customer keeps its API keys and account credentials confidential, restricts their use to authorised persons and revokes or rotates them without delay if they may have been compromised. Vaikoon is not responsible for processing carried out using the Customer's valid API keys or credentials.

3.3 Notification of Security Breaches

Vaikoon notifies the Customer of a Security Breach without undue delay and in any event within forty-eight (48) hours after becoming aware of it. Vaikoon becomes aware once it has established with reasonable certainty that Customer Personal Data is or may be affected. The notification is sent to the Account Owner by e-mail.

3.4 Content of the notification

The notification contains, so far as known to Vaikoon at the time, a description of the nature of the Security Breach, the categories and approximate number of data subjects and records concerned, the likely consequences and the measures taken or proposed. Information not available at the time is provided as it becomes available. Vaikoon investigates the Security Breach, takes reasonable measures to mitigate its effects and cooperates with the Customer in its response. Notifications to supervisory authorities and communications to data subjects are the responsibility of the Customer (art. 33 and 34 GDPR; art. 24 FADP). A notification by Vaikoon is not an acknowledgement of fault or liability.

4 Information and audits

4.1 Information

Vaikoon makes available to the Customer the information necessary to demonstrate compliance with this DPA, in the first instance through this DPA and Annex 2, and by providing written responses, on a confidential basis, to reasonable requests for information, including information security questionnaires. The Customer may make such requests not more than once in any twelve (12) month period, unless a Security Breach has occurred or a competent supervisory authority requires the information.

4.2 Inspections

Where the information under clause 4.1 is not sufficient to demonstrate compliance, and an inspection is required under Applicable Data Protection Law or by a competent supervisory authority, the Customer may carry out an inspection itself or have it carried out by an independent auditor bound to confidentiality who is not a competitor of Vaikoon. The inspection requires at least thirty (30) days' prior notice, takes place during normal business hours on the basis of a scope agreed in advance and does not extend to data of other customers or to measures which would compromise the security of the Service. The Customer bears its own costs and reimburses Vaikoon's reasonable costs, unless the inspection reveals a material breach of this DPA by Vaikoon.

4.3 Supervisory authorities

The powers of the competent supervisory authorities remain unaffected.

5 Hosting, Sub-processors and transfers

5.1 Hosting location

Vaikoon processes Customer Personal Data exclusively in Switzerland, on infrastructure owned and operated by Vaikoon. Vaikoon does not use rented, leased or other third-party compute infrastructure (including GPU capacity) for the processing of Customer Content, including for temporary capacity scaling, and Customer Personal Data is not accessed from outside Switzerland. The Customer is responsible for the locations from which it accesses the Service and for any transfer of Customer Personal Data made by it.

5.2 Sub-processors

Vaikoon currently does not engage any Sub-processors. The Customer grants Vaikoon general written authorisation within the meaning of art. 28 (2) GDPR and art. 9 (3) FADP to engage Sub-processors in the future, subject to clauses 5.3 to 5.5.

5.3 Notice of changes

Vaikoon notifies the Account Owner by e-mail at least thirty (30) days before engaging a new Sub-processor or changing the hosting location described in clause 5.1, stating the name and location of the Sub-processor, the processing activities concerned and the place of processing. Vaikoon does not use a new Sub-processor or location for Customer Personal Data before the end of that period.

5.4 Objection

The Customer may object to a change under clause 5.3 on reasonable data protection grounds by e-mail within the notice period. The Customer's sole and exclusive remedy is to terminate its subscription in accordance with the ToS with effect no later than the date on which the change takes effect, without liability of either party. Fees already paid are not refunded. If the Customer neither objects nor terminates, the change is deemed approved.

5.5 Sub-processor obligations

Vaikoon imposes on each Sub-processor, by written agreement, data protection obligations which meet the requirements of art. 28 (3) and (4) GDPR and art. 9 FADP, and remains liable to the Customer for the performance of the Sub-processor's obligations as for its own.

5.6 Transfers

Customer Personal Data is not transferred outside Switzerland. Switzerland is recognised by the European Commission as providing an adequate level of data protection (art. 45 GDPR); no standard contractual clauses are therefore required for transfers from the EU/EEA to Vaikoon. Should a change under clause 5.3 involve a country without an adequate level of data protection, Vaikoon puts in place appropriate safeguards under art. 46 GDPR and art. 16 (2) FADP before the change takes effect.

6 Retention and deletion

6.1 Customer Content

Customer Content is processed transiently, solely to generate the requested output, and is not stored persistently. Pairs of requests and responses may be held in a response cache solely in order to answer identical requests; cache entries are deleted automatically no later than twenty-four (24) hours after their creation. Customer Content is not included in backups and cannot be retrieved or returned.

6.2 Technical Data and termination

Technical Data is retained for the period stated in Annex 1 and then deleted or anonymised. Upon termination of the subscription, Vaikoon deletes any remaining Customer Personal Data at the end of that period. If the Account Owner requests it before termination, Vaikoon instead provides the Technical Data relating to the account in a standard machine-readable format before deleting it.

6.3 Statutory retention

Vaikoon may retain Customer Personal Data to the extent required by mandatory Swiss law, including the retention of logs under art. 4 (5) DSV where that provision applies. Such data is processed only for that purpose and remains subject to this DPA.

7 Cooperation

7.1 Data subject requests

Taking into account the nature of the processing, Vaikoon assists the Customer with reasonable measures in responding to requests of data subjects. As Customer Content is not stored persistently, Vaikoon will generally not hold Customer Content to which a request could relate. If a data subject addresses a request to Vaikoon which Vaikoon can attribute to the Customer, Vaikoon refers the data subject to the Customer. The Customer is responsible for responding to such requests.

7.2 Requests of authorities

If Vaikoon receives a request from a court or authority to disclose Customer Personal Data, it attempts to refer the request to the Customer and otherwise notifies the Customer without delay, unless legally prohibited from doing so. Vaikoon discloses Customer Personal Data only to the extent required by law and challenges requests which appear manifestly unlawful.

7.3 Impact assessments and consultations

Taking into account the nature of the processing and the information available to it, Vaikoon provides the Customer with reasonably requested information to assist it with its obligations regarding security, Security Breaches, data protection impact assessments and prior consultations (art. 32 to 36 GDPR; art. 8, 22, 23 and 24 FADP).

7.4 Records

Vaikoon maintains a record of the categories of processing activities carried out on behalf of its customers (art. 30 (2) GDPR; art. 12 FADP).

8 Liability and final provisions

8.1 Liability

The liability of the parties under or in connection with this DPA is governed by the ToS, including its limitations of liability, subject to mandatory law. The liability of either party towards data subjects under Applicable Data Protection Law remains unaffected.

8.2 Amendments

Vaikoon may amend this DPA in accordance with the amendment provisions of the ToS. Material amendments are notified to the Account Owner by e-mail at least thirty (30) days before they take effect; if the Customer does not agree, it may terminate its subscription before that date. Amendments required by law or by a competent authority may take effect earlier.

8.3 Precedence

In the event of a conflict between this DPA and the ToS, this DPA prevails with regard to the processing of Customer Personal Data. In all other respects, the ToS remain unchanged.

8.4 Severability

Should a provision of this DPA be or become invalid, the validity of the remaining provisions is not affected.

8.5 Governing law and jurisdiction

This DPA is governed by the law applicable to the ToS. The place of jurisdiction is determined by the ToS. Mandatory provisions of Applicable Data Protection Law, mandatory consumer protection law of the country in which a Customer acting as consumer has its habitual residence, the competences of the supervisory authorities and the rights of data subjects remain unaffected.

8.6 Annexes

Annex 1 (Details of the processing) and Annex 2 (Technical and organisational measures) form an integral part of this DPA.

Annex I – Details of the processing

Item	Details
Subject matter	Provision of AI Router Switzerland: access via an OpenAI-compatible API to the artificial intelligence models offered by Vaikoon from time to time (in particular large language models, embedding models, speech-to-text and text-to-speech models), hosted by Vaikoon in Switzerland, as described in the ToS.
Nature and purpose of the processing	Customer Content: receipt, transient processing in memory for inference, transmission of the output to the Customer, temporary storage in the response cache to answer identical requests, automatic deletion. Technical Data: recording, storage and analysis for the Permitted Purposes (clause 2.6), anonymisation and deletion.
Categories of data subjects	Determined by the Customer in its sole discretion; may include in particular the Customer's employees, contractors and other users of the Service, users of the Customer's own applications which use the Service, and any other natural persons whose personal data the Customer includes in Customer Content.
Categories of personal data	(a) Customer Content: determined by the Customer in its sole discretion; may include any personal data contained in inputs (e.g. names, contact details, free text, documents, voice recordings) and outputs. (b) Technical Data: IP address, time stamps, API key or account identifier, endpoint and model used, status codes, token usage and other request metadata, without Customer Content.
Special categories of personal data	Not intended. Where the Customer submits special categories of personal data, clause 2.5 applies.
Frequency	Continuous, per API request, for the duration of the subscription.
Retention	Customer Content: for the duration of the request; response cache: no more than twenty-four (24) hours, deleted automatically. Technical Data: 12 months. Technical data included in backups will age out of the solution naturally. Backup Retention is 12 months. Statutory retention under clause 6.3 remains reserved.
Place of processing	Exclusively Switzerland, on infrastructure owned and operated by Vaikoon (data centre). No rented or third-party compute infrastructure (clause 5.1).
Sub-processors	None. The payment service provider (Stripe) processes subscription and billing data for which Vaikoon is controller (clause 1.3) and has no access to Customer Content or Technical Data.
Contact	Vaikoon AG, Gotthardstrasse 47, 6045 Meggen, Switzerland; data protection: privacy@vaikoon.ch ; support: support@airouter.ch .

Annex 2 – Technical and organisational measures

Vaikoon implements the following technical and organisational measures in accordance with clause 3.1.

Area	Measures
Pseudonymisation and encryption	Customer Content is transmitted exclusively over encrypted connections (TLS 1.2 or higher). Customer Content is processed in memory for the duration of the request and is not written to persistent storage, with the exception of the response cache (Annex 1) Cached Completions are stored as JSON under a hash/prefix key.. The input string gets hashed [SHA-256 (full 64-char hex digest)] to index the JSON Completions. Technical Data does not contain Customer Content. User passwords are stored as Argon2 hashes; Customer Content is not pseudonymised by Vaikoon, because its content is determined by the Customer and is not known to Vaikoon.
Confidentiality – physical access control	Vaikoon's infrastructure is owned by Vaikoon and located in, Switzerland. Physical access to the hardware is restricted to authorised personnel of Vaikoon. Third parties have no logical access to Vaikoon's systems.
Confidentiality – system access control	Personal administrative accounts; two-factor authentication for administrative and remote access; Administrative access only over VPN and SSH with key-based authentication; hardened hosts; perimeter firewall, reverse proxy and load balancer operated by Vaikoon; access to the API only with a valid API key; secure authentication for customer accounts.
Confidentiality – data access control	Role-based access on a need-to-know basis with periodic review of administrative accounts. Logging of prompts and outputs is disabled in the configuration of the API router (LiteLLM); the inference server for text-to-speech (Kokoro) has been modified so that inputs and outputs are not logged, including in debugging and error cases. Customer Content is therefore not available in logs and cannot be accessed by personnel through log files. Access to Technical Data is restricted to personnel who need it for the Permitted Purposes.
Confidentiality – separation control	Requests are processed in isolated compute environments (containerised workloads with network isolation). Customer Content of different customers is not combined. Cached Completions are stored as JSON under a hash/prefix key.. The input string gets hashed [SHA-256 (full 64-char hex digest)] to index the JSON Completions. Production, test and development environments are separated; test and development environments do not use Customer Content.
Integrity – transfer control	Encrypted transmission (TLS 1.2 or higher) between the Customer and the Service; no transmission of Customer Content to third parties; encrypted connections for administrative access.
Integrity – input control	Logging of Technical Data (IP address, time stamp, API key or account identifier, endpoint and model, status code, token usage) without Customer Content; logging of administrative actions; retention of logs for the period stated in Annex 1; protection of logs against modification and unauthorised deletion.
Integrity – change management	Documented change and release process, version control of configuration (including the logging configuration described above), review and testing before release, rollback concept. Changes which would re-enable logging of Customer Content are not permitted.
Availability – backup and recovery	Customer Content is not backed up. Configuration and account data are backed up daily encrypted; regular restore tests. Recovery objectives: RTO 12 hours, RPO 24 hours.



Area	Measures
Availability – resilience and continuity	Load balancing across inference nodes, monitoring with alerting, rate limiting and fair-use limits to protect availability, firewall and network segmentation, documented emergency procedures. Capacity is provided exclusively on infrastructure owned and operated by Vaikoon in Switzerland; rented or third-party compute capacity is not used (clause 5.1).
Procedures for regular testing, assessment and evaluation	[Vulnerability management and patching; periodic review of the logging configuration to verify that no Customer Content is logged.
Incident response management	Documented incident response process with classification, escalation, preservation of evidence, notification of the Customer in accordance with clause 3.3, root cause analysis and corrective measures.
Data protection by design and by default	No persistent storage of Customer Content; automatic deletion of the response cache after no more than twenty-four (24) hours; no use of Customer Content for training or evaluation of models; prompt and output logging disabled by default and by design, including in error and debugging paths; data-minimised Technical Data.
Processing control	Standardised instructions (clause 2.2); personnel bound to confidentiality and trained; no Sub-processors; any future Sub-processor and any change of the hosting location only in accordance with clause 5.
Personnel	Background checks within the limits permitted by law, confidentiality undertakings before access is granted, data protection and security training on entry and at regular intervals, defined procedures for entry, change of function and exit including timely revocation of authorisations.

The measures reflect the state as at the effective date of this DPA. Vaikoon may adapt them in accordance with clause 3.1.

Vaikoon AG

Gotthardstrasse 47
CH-6045 Meggen

Register # CH-100.3.798.146-9
VAT # CHE 318.570.988

www.vaikoon.com
office@vaikoon.com