TRUST CENTER

Standard Data Processing Agreement

Between VW-CODING, SASU (Processor), operating the platform magif.ai, and the Customer identified in the signature block (Controller).

Last updated: Version 1.0 - 21 September 2026

This Data Processing Agreement (the "Agreement" or "DPA") governs the processing of personal data carried out by VW-CODING, SASU on behalf of the Customer in connection with the Customer's use of the Magif AI-agent platform. It forms part of, and is subject to, the terms of service or subscription agreement between the parties (the "Principal Agreement").

VW-CODING, SASU is a French simplified joint-stock company (SASU) with a share capital of EUR 4,000, registered with the Registre du commerce et des societes (RCS) of Paris under number 914 650 387, having its registered office at 121 quai de Valmy, 75010 Paris, France, with VAT number FR41914650387, and operating the platform magif.ai (referred to in this Agreement as "Magif" or "the Processor"). The Customer is the coach, creator, or organisation that deploys AI agents on the platform and is identified in the signature block (referred to as "the Controller" or "the Customer").

This Agreement is entered into to comply with Article 28 of Regulation (EU) 2016/679 (the General Data Protection Regulation, "GDPR") and applicable data protection law. Where this Agreement conflicts with the Principal Agreement on matters of personal data processing, this Agreement prevails.

1. Definitions

Terms used in this Agreement have the meanings given in the GDPR unless defined otherwise below.

- "Personal Data" means any information relating to an identified or identifiable natural person that is processed by the Processor on behalf of the Controller under this Agreement.

- "Processing" means any operation performed on Personal Data, whether or not by automated means, as defined in Article 4(2) GDPR.
- "Data Subject" means the identified or identifiable natural person to whom Personal Data relates.
- "Controller", "Processor", and "Subprocessor" have the meanings given in the GDPR.
- "End User" means a client or user of the Controller who interacts with an agent deployed by the Controller on the platform.
- "Personal Data Breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Personal Data.
- "Applicable Data Protection Law" means the GDPR and all other data protection and privacy laws applicable to the processing under this Agreement.
- "Trust Center" means the set of public pages published by Magif that document its subprocessors, data residency, security measures, and retention practices, referenced throughout this Agreement.

2. Roles of the parties

The parties acknowledge that, with respect to the processing of Personal Data under this Agreement, the Customer acts as the Controller and Magif acts as the Processor. Magif processes Personal Data only on behalf of and under the documented instructions of the Controller.

The Controller is responsible for determining the purposes and means of the processing, for the lawfulness of the instructions it gives, and for ensuring that it has a valid legal basis for the processing carried out on its behalf.

For the processing of payment and billing information, the payment provider Stripe acts as an independent controller in its own right. Such processing is governed by Stripe's own terms and privacy notice and is outside the scope of the processing that Magif carries out as Processor under this Agreement.

3. Subject matter and duration

The subject matter of the processing is the provision of the Magif AI-agent platform, which enables creators to build specialised AI agents from their own content and to make those agents available to their clients and end users.

The processing continues for the duration of the Principal Agreement. It begins when the Controller starts using the platform and ends on termination or expiry of the Principal Agreement, subject to the deletion and return obligations set out in this Agreement and to any legal retention requirements.

4. Nature and purpose of the processing

Magif processes Personal Data for the purpose of operating and providing the platform to the Controller, including the following activities:

- Creating, configuring, hosting, and running AI agents built by the Controller;
- Enabling conversations between End Users and the Controller's agents, and generating agent responses through inference;
- Building and maintaining knowledge bases from content supplied by the Controller;
- Storing and retrieving conversation history, files, and configuration in the platform's databases and storage;
- Providing account management, authentication, support, and platform administration;
- Maintaining the security, integrity, availability, and correct functioning of the platform.

Magif does not process Personal Data for any purpose other than providing the platform and complying with the Controller's documented instructions, except where required by law as set out in this Agreement.

5. Categories of personal data

The Personal Data processed under this Agreement may include the following categories, depending on how the Controller configures and uses the platform:

- Account and identity data of the Controller's personnel, such as name, email address, and authentication credentials;
- End User identifiers and account data, such as name, email address, and connected-channel identifiers;
- Conversation content exchanged between End Users and the Controller's agents, including messages, prompts, and generated responses;
- Content supplied by the Controller to build agents and knowledge bases, which may itself contain Personal Data;
- Usage, technical, and log data, such as IP address, session identifiers, timestamps, and device or browser information;
- Support and correspondence data.

The Controller must not submit special categories of Personal Data (Article 9 GDPR) or data relating to criminal convictions and offences (Article 10 GDPR) unless the parties have agreed appropriate additional safeguards in writing.

6. Categories of data subjects

The Data Subjects whose Personal Data is processed under this Agreement may include:

- The Controller's personnel and authorised platform users;
- The Controller's clients and End Users who interact with the deployed agents;
- Any natural person whose Personal Data is contained in content that the Controller submits to build or operate agents.

The Controller determines which Data Subjects are affected through its configuration and use of the platform.

7. Documented instructions

Magif processes Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data, unless required to do so by Union or Member State law to which Magif is subject. Where such a legal requirement applies, Magif informs the Controller of that requirement before processing, unless the law prohibits such information on important grounds of public interest.

The Controller's instructions are set out in this Agreement, in the Principal Agreement, and in the configuration choices the Controller makes through the platform. Any additional or changed instructions must be agreed in writing.

Magif informs the Controller without undue delay if, in its opinion, an instruction infringes Applicable Data Protection Law. Magif is not obliged to carry out a legal assessment of the Controller's instructions.

8. Confidentiality

Magif ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

Access to Personal Data is limited to personnel who need access to perform their duties under the Principal Agreement, and such access is subject to appropriate access controls. The confidentiality obligation survives the termination of the individual's engagement and of this Agreement.

9. Security and technical and organisational measures

Taking into account the state of the art, the costs of implementation, and the nature, scope, context, and purposes of the processing, as well as the risks to the rights and freedoms of natural persons, Magif implements appropriate technical and organisational measures to ensure a level of security appropriate to the risk, in accordance with Article 32 GDPR.

These measures include, as appropriate, encryption of data in transit and at rest, access controls and authentication, network and application security, logging and monitoring, backup and recovery, and processes for regularly testing and evaluating the effectiveness of the measures.

A current description of the technical and organisational measures is maintained on the Trust Center security page at /trust/security. That page forms part of this Agreement and is

updated from time to time; Magif does not reduce the overall level of security during the term of this Agreement.

10. No model training and no independent reuse

Magif does not use Customer content or End User conversation content to train, fine-tune, or develop artificial intelligence or machine-learning models. Magif does not reuse Customer content or End User conversation content for its own independent purposes.

Content submitted to the platform is processed solely to provide the platform to the Controller and to follow the Controller's documented instructions. Magif's arrangements with its AI inference providers prohibit those providers from using content submitted through the platform to train their models.

This clause applies to conversation content, prompts, generated responses, knowledge bases, uploaded files, and agent configuration content that contain Personal Data processed on behalf of the Controller.

11. Subprocessors and vendor change mechanism

The Controller grants Magif general authorisation to engage Subprocessors to support the provision of the platform, subject to this clause.

Magif maintains a public register of its Subprocessors on the Trust Center at /trust/subprocessors. The register identifies each Subprocessor and the processing activity it supports.

Where Magif intends to add or replace a Subprocessor, it updates the public register and notifies the Controller of the change before it takes effect, giving the Controller a reasonable opportunity to object. The Controller may object to a change on reasonable data protection grounds. If the parties cannot resolve the objection, the Controller may terminate the affected part of the Principal Agreement in accordance with its terms.

Magif imposes on each Subprocessor, by written contract, data protection obligations that are no less protective than those set out in this Agreement, and remains fully liable to the Controller for the performance of each Subprocessor's obligations.

12. Data locations and international transfers

Core processing, including conversations, agent inference, knowledge bases, and the primary database, is carried out within the European Union. Certain services, including file storage and transactional email, are carried out in the United Kingdom, which benefits from an adequacy decision of the European Commission.

Because vendors, services, and locations may change over time, the current details of where Personal Data is processed are maintained on the Trust Center data residency page at /trust/data-residency, and the list of Subprocessors is maintained at /trust/subprocessors. These pages form part of this Agreement.

Where any transfer of Personal Data to a third country not covered by an adequacy decision is required, Magif ensures that an appropriate transfer safeguard under Chapter V GDPR is in place, such as the European Commission's Standard Contractual Clauses, together with any supplementary measures necessary to protect the Personal Data.

13. Assistance with data subject requests

Taking into account the nature of the processing, Magif assists the Controller by appropriate technical and organisational measures, insofar as this is possible, to fulfil the Controller's obligation to respond to requests from Data Subjects exercising their rights under Chapter III GDPR, including rights of access, rectification, erasure, restriction, portability, and objection.

If Magif receives a request directly from a Data Subject relating to Personal Data processed on behalf of the Controller, Magif does not respond to the request other than to acknowledge receipt where required, and promptly forwards the request to the Controller, unless otherwise instructed or legally required.

14. Assistance with compliance obligations

Taking into account the nature of the processing and the information available to Magif, Magif assists the Controller in ensuring compliance with its obligations under Articles 32 to 36 GDPR, including obligations relating to security of processing, notification of Personal Data Breaches, communication of breaches to Data Subjects, data protection impact assessments, and prior consultation with the supervisory authority.

15. Personal data breach cooperation

Magif notifies the Controller without undue delay after becoming aware of a Personal Data Breach affecting Personal Data processed on behalf of the Controller.

The notification includes, to the extent available to Magif, a description of the nature of the breach, the categories and approximate number of Data Subjects and records concerned, the likely consequences, and the measures taken or proposed to address the breach and mitigate its effects. Where the information cannot all be provided at once, it may be provided in phases without further undue delay.

Magif takes reasonable steps to contain and remediate the breach and cooperates with the Controller so that the Controller can meet its own notification obligations to supervisory

authorities and Data Subjects.

16. Deletion and return of personal data

On termination or expiry of the Principal Agreement, and at the choice of the Controller, Magif deletes or returns all Personal Data processed on behalf of the Controller, and deletes existing copies, unless Union or Member State law requires storage of the Personal Data.

Deletion and return are carried out in accordance with the documented retention rules published on the Trust Center privacy and retention page at /trust/privacy, which forms part of this Agreement.

Personal Data held in encrypted backups is not immediately erasable and expires on a rolling window of at most one year, after which it is permanently deleted. During that window, backup data is retained only for the purpose of restoration and is not used for any other purpose.

17. Audit and provision of compliance information

Magif makes available to the Controller all information necessary to demonstrate compliance with the obligations set out in Article 28 GDPR and this Agreement, and allows for and contributes to audits, including inspections, conducted by the Controller or an auditor mandated by the Controller.

The Controller may satisfy its audit rights primarily by reviewing the documentation and information published on the Trust Center, including the security, data residency, subprocessor, and retention pages, and any certifications or reports Magif makes available.

Where the Controller reasonably requires further assurance, an audit may be conducted subject to reasonable notice, no more than once per year except where required by a supervisory authority or following a Personal Data Breach, during business hours, and in a manner that does not disrupt Magif's operations or compromise the confidentiality or security of other customers' data.

18. Liability and precedence

Each party's liability arising out of or related to this Agreement is subject to the limitations and exclusions of liability set out in the Principal Agreement.

This Agreement supplements the Principal Agreement. In the event of any conflict between this Agreement and the Principal Agreement in relation to the processing of Personal Data, this Agreement prevails.

19. Governing law and jurisdiction

This Agreement is governed by the law that governs the Principal Agreement. In the absence of a governing-law clause in the Principal Agreement, this Agreement is governed by French law, without prejudice to the mandatory application of the GDPR and Applicable Data Protection Law. The courts having jurisdiction under the Principal Agreement have jurisdiction over disputes arising out of this Agreement.

20. Contact details

Questions and notices relating to this Agreement and to data protection may be addressed to the Processor:

- VW-CODING, SASU, operating the platform magif.ai
- 121 quai de Valmy, 75010 Paris, France
- RCS Paris 914 650 387

The Trust Center at /trust provides the canonical, current documentation referenced in this Agreement, including the subprocessor register (/trust/subprocessors), data residency (/trust/data-residency), security and technical and organisational measures (/trust/security), and retention and deletion (/trust/privacy).

Signatures

Processor

Magif (VW-CODING, SASU)

Name:

Title:

Signature:

Date:

Controller (Customer)

Legal entity:

Registered address:

Name:

Title:

Signature:

Date:

How to execute this agreement

Download or print the current agreement, complete the customer details and sign it. Send the signed copy to support@magif.ai. An authorised Magif representative will countersign and return the executed agreement.

1. Open the full contract on this page.
2. Print it or download the PDF.
3. Fill in the controller / customer company details.
4. Sign it.
5. Email the signed copy to support@magif.ai.
6. Magif countersigns.
7. Magif returns the fully executed copy.

No NDA is required.