# Data processing agreement

Version of November 19, 2026 · in force on December 19, 2026

This data processing agreement (the “Agreement”) is entered into between the Customer and Mayeul FLORY, sole trader (entrepreneur individuel; trade name: FUSION-IA), publisher of WYRLO, processor within the meaning of article 28 of the GDPR. It follows the structure and options of the European Commission’s standard contractual clauses between controllers and processors (Implementing Decision (EU) 2021/915), drafted for WYRLO. It forms part of the terms of use: it applies as soon as the Customer sends data to the WYRLO API. A signed version, reproducing the standard clauses word for word with the annexes below, can be requested at contact@wyrlo.io.

## Contents

1. Purpose, parties and order of precedence
2. Roles and processing chain
3. Description of the processing
4. Instructions, purpose limitation and confidentiality
5. Drafting with the Customer’s model
6. Sub-processors
7. International transfers
8. Security of processing
9. Exercise of data subjects’ rights
10. Notification of data breaches
11. Assistance to the controller
12. Documentation and audits
13. Obligations of the Customer
14. Term, end of the Agreement and fate of the data
15. Annex: security measures
16. Contact
17. Liability and governing law

## 1. Purpose, parties and order of precedence

The Agreement sets out the conditions under which WYRLO processes, on behalf of the Customer, the personal data described in article 3, in accordance with Regulation (EU) 2016/679 (the "GDPR") and French law no. 78-17 of 6 January 1978.

In the event of a conflict between the Agreement and another contractual document (terms of use, terms of sale, Partner plan terms, specific terms), the Agreement prevails for everything relating to data protection.

## 2. Roles and processing chain

- Direct Customer: the Customer is the controller of the data it sends to the API; WYRLO is its processor.
- Partner and End clients: when the Customer uses WYRLO to serve its own End clients, each End client is in principle the controller, the Customer (Partner) is its processor, and WYRLO is a sub-processor of the Partner (article 28(4) of the GDPR). If the Customer processes the data on its own behalf, it is the controller.
- In the second case, the Partner warrants that it has obtained from each End client written authorisation to use WYRLO and its sub-processors, and that it imposes on it data protection obligations at least equivalent to the Agreement. The Partner remains WYRLO's sole point of contact: it passes WYRLO's information and notifications on to its End clients without delay, and their instructions on to WYRLO.
- An End client may accede directly to the Agreement, with the consent of the Partner and WYRLO, by signing the signed version (docking clause of the standard clauses).

## 3. Description of the processing

- Nature of the operations: receipt of the data sent to the API; masking; injection detection; verification of answers, computation of the confidence level and decision; drafting of a cited answer on request (/v1/answer); zero-copy indexing and search; limited storage of traces; analysis by the improvement loop and report; separation by End client; deletion.
- Purpose: providing the Customer with the service described in the terms of use: no-copy indexing and search of its documents, and checking of its AI's answers, as well as the other functions described in article 3 of the terms of use. Never training an AI model, nor any purpose of WYRLO's own.
- Categories of data: questions, answers, confidence level, decision, language and date of each trace, request and End client identifiers, user feedback (useful answer or not); for each passage, its identifier, its source (name of the original document), a fingerprint and its scores, and for the top 3 passages an excerpt of 600 characters at most; fingerprints and vectors of the passages, without their text; for the zero-copy index, positions, fingerprints and vectors of the passages, without their text; analyses drawn from traces (failure groups, missing topics, proposed fixes, reports); for each End client, the identifier chosen by the Customer, an optional display name and its status. With the "traces without text" setting, no text is kept.
- Data subjects: users of the Customer's application (or of its End clients), who ask the questions, and people mentioned in the questions, passages, indexed documents or answers.
- Sensitive data: none. The Customer undertakes not to send data covered by articles 9 and 10 of the GDPR without having masked it on its side (terms of use, article 7).
- Duration: traces kept for the period chosen by the Customer within the limit of its plan (14, 30 or 90 days) or the period agreed in specific terms, then deleted automatically every night; examples included in analyses, removed with the traces; passage

fingerprints, same period counted from their last receipt; zero-copy index, until the deletion of the document, the space, the project or the organisation; analyses and reports, for as long as the service is used.
- WYRLO never stores the Customer's documents. Users' account data is processed by WYRLO as controller, according to the privacy policy, and does not fall under the Agreement.

---

## 4. Instructions, purpose limitation and confidentiality

WYRLO undertakes to:

- process the data only on documented instructions from the Customer: the terms of use, the Agreement, the Customer's calls to the API and the settings chosen in its space (masking, traces without text, retention period, AI verification, drafting model, End clients); if WYRLO considers that an instruction infringes the GDPR or another Union or Member State data protection provision, it immediately informs the Customer;
- process the data only for the purpose in article 3, never on its own behalf, and in particular not to train AI models;
- if WYRLO is required to process data under Union or Member State law, inform the Customer before the processing, unless that law prohibits it;
- guarantee the confidentiality of the data; the only person currently authorised to access it is the publisher, bound by confidentiality, who only accesses a Customer's traces for the support that Customer requests, for the security of the service or for a legal obligation;
- take data protection into account by design and by default: masking enabled by default, text sent to Mistral AI always masked, shortest retention period of the plan by default, strict isolation between organisations and between End clients.

## 5. Drafting with the Customer’s model

When the Customer requests, through /v1/answer, an answer drafted by the AI provider it designates, WYRLO passes the question and the passages to that provider, without masking, with the Customer’s key. This transfer is an instruction from the Customer: the provider is not a sub-processor of WYRLO, it acts under the Customer’s contract with it, and the Customer is answerable for that provider’s place of processing and safeguards. The key, if the Customer saves it for a project, is stored encrypted and is used only for these calls.

## 6. Sub-processors

The Customer gives WYRLO general authorisation to engage sub-processors. At the date of the Agreement, they are:

- Supabase Pte. Ltd. (Singapore): database, authentication and API functions, eu-west-3 region (Paris);
- Vercel Inc. (United States): developer space, through which the displayed traces pass, and API address (api.wyrlo.io), through which calls pass without being stored; functions in the cdg1 region (Paris);
- Mistral AI SAS (Paris, France): live verification of answers in French and English, drafting by the model managed by WYRLO, computation of the zero-copy index vectors and improvement loop processing, always on texts masked by WYRLO (nothing is sent if masking fails); calls through its European endpoint.

WYRLO’s other providers (Resend for emails, OVH for the support mailbox, Stripe for payments) receive no data covered by the Agreement.

WYRLO informs the Customer by email of any intended addition or replacement at least 30 days in advance, specifying the processing

entrusted, the identity of the sub-processor and the date of the change. The Customer may object in writing during this period; failing agreement, it may terminate free of charge before the change takes effect. A Partner passes the information on to its End clients. Each sub-processor is bound, by contract, to data protection obligations equivalent to those of the Agreement. WYRLO remains fully liable to the Customer for the performance of these obligations.

Up-to-date list of subprocessors

## 7. International transfers

Data is processed in the European Union. Where a sub-processor may access it from a third country (Vercel Inc., a US company; Supabase for some service data and its technical logs; Mistral AI's sub-processors outside the European Union and the EFTA countries), the transfer is governed by the standard contractual clauses of decision 2021/914 provided for in its data processing agreement and, where applicable, by the EU–US Data Privacy Framework. WYRLO makes no other transfer without instructions from the Customer (article 5).

## 8. Security of processing

WYRLO implements the technical and organisational measures in the "Security measures" annex (article 15). It reviews them at each significant change to the service and does not reduce them without informing the Customer.

## 9. Exercise of data subjects' rights

WYRLO helps the Customer respond to requests to exercise data subjects' rights (access, rectification, erasure, restriction, objection, portability). On the Customer's written request, WYRLO searches for the traces containing a given text, provides a copy of them or deletes them, within 10 business days, so that the Customer can respond within the month provided for by the GDPR. The Customer can also, without waiting, delete an End client, a project or its organisation, which immediately erases the corresponding data.

When a data subject sends a request directly to WYRLO, WYRLO forwards it to the Customer (or the Partner) by email upon receipt, without responding to it itself.

---

## 10. Notification of data breaches

WYRLO notifies the Customer of any personal data breach covered by the Agreement within 48 hours at most of becoming aware of it, by email to the organisation's owners. A Partner passes it on without delay to its End clients concerned.

The notification comes with any documentation useful to enable the Customer, where necessary, to notify the breach to the competent supervisory authority and to inform the data subjects. It describes at least:

- the nature of the breach, the categories and approximate number of data subjects and records concerned;
- the contact point from which more information can be obtained;
- the likely consequences of the breach;
- the measures taken or proposed to address it and mitigate its effects.

Where all this information cannot be provided at the same time, it is provided in phases, without undue delay.

---

## 11. Assistance to the controller

WYRLO assists the Customer, by providing the information available to it (in particular the Security page, the list of subprocessors, the Artificial intelligence page and, on request, its security file), in carrying out data protection impact assessments and in the prior consultation of the supervisory authority.

---

## 12. Documentation and audits

WYRLO makes available to the Customer the documentation needed to demonstrate compliance with its obligations and to allow for audits, including inspections, by the Customer or by an auditor mandated by it, and contributes to these audits. It keeps a record of the processing activities carried out on behalf of its customers (article 30(2) of the GDPR).

Except in the event of a data breach or a request from a supervisory authority, an audit takes place at most once a year, after 30 days' written notice, at the Customer's expense, by an auditor bound by confidentiality who is not a competitor of WYRLO.

---

## 13. Obligations of the Customer

The Customer undertakes to:

- have a legal basis for the processing and inform the data subjects, in particular the users of its application and, where applicable, its End clients, of the use of WYRLO and its subprocessors;
- send WYRLO only the data that is necessary, and no data covered by articles 9 and 10 of the GDPR without masking on its side;
- not put a person's name in an End client's identifier;

- document in writing any instruction beyond the settings available in its space;
- ensure, beforehand and throughout the processing, compliance with the obligations of the GDPR on the part of WYRLO, including through audits under the conditions of article 12.

---

## 14. Term, end of the Agreement and fate of the data

The Agreement takes effect when the Customer's organisation first sends data and applies for as long as the service is used, then until the data is deleted.

At the end of the service: deletion of the organisation by its owner immediately erases all its data; after a termination requested by email or decided by WYRLO, the data is deleted at the latest 30 days afterwards. Deleting an End client immediately erases its index and its traces. If the Customer requests it before the end, WYRLO returns a copy of its traces still kept, in a machine-readable format.

WYRLO currently makes no automatic backups; a manual backup copy, encrypted and kept offline, may contain deleted data for at most 90 days, without being used other than for restoration. On request, WYRLO provides written confirmation of the deletion.

---

## 15. Annex: security measures

WYRLO implements the following measures, described in more detail on the Security page:

- database and API functions hosted in Paris (Supabase, eu-west-3 region); a request received in another region is rejected without being read;
- encryption of data in transit (HTTPS mandatory) and at rest (AES-256 for the database, at Supabase); encrypted manual

backup copies (AES-256);
- strict isolation between organisations through access rules at the database level, checked by automated tests before each release to production; separation of each End client's data in its own space;
- built-in masking, in WYRLO's functions in Paris, before anything is sent to Mistral AI and, by default, before storage; traces without text as an option;
- API keys stored only as a hash (SHA-256), revocable at any time; the Customer's AI provider keys encrypted;
- two-factor authentication offered to Users;
- administration keys and secrets kept only on the server side, never in the code, the browser or the logs;
- activity log of sensitive actions, kept for 1 year;
- limited retention periods and automatic deletion every night;
- no logging of the content of questions, passages or answers;
- written incident management procedure, rollback prepared for each release to production.

Details of the measures (Security page)

---

## 16. Contact

WYRLO has not appointed a data protection officer. For any question about the Agreement or personal data: contact@wyrlo.io.

---

## 17. Liability and governing law

Each party's liability is governed by article 82 of the GDPR and by the terms of use.

This Agreement is governed by French law. Failing an amicable agreement, any dispute will be brought before the competent courts within the jurisdiction of the Lyon Court of Appeal, within the limits provided by law.

Any change to the Agreement is notified by email to account holders at least 30 days before it takes effect.