Data processing agreement

Version of November 18, 2026

This data processing agreement (the “Agreement”) is entered into between the Customer, as controller, and Mayeul FLORY, sole trader (entrepreneur individuel; trade name: FUSION-IA), publisher of WYRLO, as processor within the meaning of article 28 of the GDPR. It follows the structure of the sample processing clauses published by the CNIL, the French data protection authority, adapted to WYRLO. It forms part of the terms of use: it applies as soon as the Customer sends traces to the WYRLO API.

Contents

1. Purpose
2. Description of the processing
3. Term
4. Purpose limitation, instructions and confidentiality
5. Sub-processors
6. Information of data subjects
7. Exercise of data subjects’ rights
8. Notification of personal data breaches
9. Assistance to the controller
10. Security measures
11. Data at the end of the Agreement
12. Data protection officer
13. Record of processing activities
14. Documentation and audits
15. Obligations of the controller
16. Liability and governing law

1. Purpose

This Agreement sets out the conditions under which WYRLO carries out, on behalf of the Customer, the personal data processing operations described in section 2.

The parties undertake to comply with the regulations applicable to this processing, in particular Regulation (EU) 2016/679 of 27 April 2016 (the “GDPR”) and French law no. 78-17 of 6 January 1978 on information technology, data files and civil liberties.

---

2. Description of the processing

- Nature of the operations: receiving the traces sent to the WYRLO API; no-copy indexing and search; analysis (prompt injection detection, answer checking, confidence level computation), masking, storage; analysis by the improvement loop, weekly report, deletion.
- Purpose: providing the Customer with the reliability service for its RAG, described in the terms of use.
- Data processed: questions, answers, confidence level, decision, language and date of each trace; for each passage, its identifier, its source (name of the original document), its scores and, for the 3 best passages, an excerpt of 600 characters at most; the digital fingerprints and numeric representations (vectors) of the passages, without their text; and the analyses derived from them (failure clusters, knowledge gaps, proposed fixes, reports); for the no-copy index, the address, a fingerprint and the vector of each passage, without its text; for each end client declared by the Customer, the identifier chosen by the Customer (no personal data expected), an optional display name, its status and the number of checks in the month.
- Data subjects: users of the Customer’s RAG, who ask the questions, and people mentioned in the questions, passages or answers.

- Retention: traces, period chosen by the Customer within the limit of its plan (14, 30 or 90 days), or period agreed in the special terms, then automatic deletion; examples included in the analyses are removed at the same time as the traces; passage fingerprints follow the same period, counted from the last time the passage was received; analyses and reports, which keep only the titles of topics and fixes, are kept for as long as the service is used.
- WYRLO never stores the Customer's documents. Users' account data is processed by WYRLO as controller, under the privacy policy, and is outside the scope of this Agreement.

---

3. Term

This Agreement takes effect when the Customer's organisation first sends traces. It applies for as long as the service is used, then until the data is deleted as provided in section 11.

---

4. Purpose limitation, instructions and confidentiality

WYRLO undertakes to:

- process the data only for the purpose described in section 2, and never on its own behalf, in particular not to train AI models;
- process the data in accordance with the Customer's documented instructions: the terms of use, this Agreement and the settings chosen by the Customer in its workspace (masking, retention period, reliability settings); if WYRLO considers that an instruction infringes the GDPR or other Union or Member State data protection provisions, it immediately informs the Customer;
- if WYRLO is required to transfer data to a third country or an international organisation under Union or Member State law to which it is subject, inform the Customer before the processing, unless that law prohibits it;

- guarantee the confidentiality of the data and ensure that the people authorised to process it have committed to confidentiality and receive the necessary data protection training;
- apply the principles of data protection by design and by default: masking enabled by default, shortest retention period by default, strict isolation between organisations.

---

5. Sub-processors

The Customer authorises WYRLO to use the following sub-processors for the processing described in section 2:

- Supabase Pte. Ltd.: database and API functions, eu-west-3 region (Paris);
- Vercel Inc. (United States): hosting of the customer workspace, through which the traces displayed there pass, and of the API address (api.wyrlo.io), through which calls pass, without storage; functions in the cdg1 region (Paris);
- Mistral AI SAS (Paris, France): live check of French and English answers (the question, the answer and an excerpt of the passages, after personal data has been masked by WYRLO; nothing is sent if masking fails), which can be turned off per organisation, and improvement loop processing on masked traces; calls through its European endpoint, with inference in the European Union and EFTA countries, data hosted in the European Union by default and possible limited transfers to its own sub-processors outside this region, according to Mistral AI's terms: https://legal.mistral.ai/terms/data-processing-addendum.

WYRLO informs the Customer by email of any intended addition or replacement at least 30 days in advance, stating the processing entrusted, the sub-processor's identity and contact details 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.

Each sub-processor is bound by contract to data protection obligations equivalent to those of this Agreement and provides sufficient security guarantees. WYRLO remains fully liable to the Customer for the performance of these obligations.

Where a sub-processor processes data outside the European Union or may access it from there, such as Vercel Inc., a US company, the transfer is covered by the European Commission's standard contractual clauses provided for in its data processing agreement and, where applicable, by the EU–US Data Privacy Framework.

Current list of subprocessors

6. Information of data subjects

The Customer is responsible for informing the data subjects, in particular the users of its RAG, when the data is collected.

7. Exercise of data subjects' rights

WYRLO helps the Customer respond to requests from data subjects exercising their rights (access, rectification, erasure, objection, restriction, portability). On the Customer's written request, WYRLO searches for, provides or deletes the traces concerned within a time that allows the Customer to respond within the one month set by the GDPR.

When a data subject sends a request directly to WYRLO, WYRLO forwards it to the Customer by email upon receipt.

8. Notification of personal data breaches

WYRLO notifies the Customer of any personal data breach within 48 hours at most of becoming aware of it, by email to the organisation's owners.

The notification comes with any documentation needed to allow 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 not all of this information can be provided at the same time, it is provided in phases without undue delay.

---

9. Assistance to the controller

WYRLO helps the Customer, by providing the information available to it, with data protection impact assessments and with prior consultation of the supervisory authority.

---

10. Security measures

WYRLO implements the following measures:

- database and API hosted in Paris (Supabase, eu-west-3 region); a request received in another region is refused without being read;

- encryption of data in transit (HTTPS) and at rest (AES-256 for the database and its backups, at Supabase);
- daily database backups, encrypted and kept for 7 days;
- strict isolation between organisations, through access rules at database level, checked by automated tests;
- masking of traces before storage, enabled by default;
- API keys stored only as a hashed fingerprint, revocable at any time;
- two-factor authentication offered to Users;
- admin keys and secrets kept on the server side only, never in the code or in the browser;
- activity log of sensitive actions, kept for 1 year;
- limited retention periods and automatic deletion of expired traces;
- no logging of the contents of queries, passages or answers.

Details of the measures (Security page)

11. Data at the end of the Agreement

When the service ends, through deletion of the organisation or termination, WYRLO deletes all of the Customer's traces and analyses within 30 days at most. If the Customer asks before termination, WYRLO returns a copy of its traces still kept, in a machine-readable format.

The data disappears from backups when they expire, within 7 days of its deletion at most. On request, WYRLO confirms the deletion in writing.

12. Data protection officer

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

13. Record of processing activities

WYRLO keeps a written record of all categories of processing activities carried out on behalf of the Customer, in accordance with article 30(2) of the GDPR.

14. 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 an auditor it appoints, and contributes to these audits.

Except in case of a data breach, an audit takes place at most once a year, with 30 days' written notice, at the Customer's expense, by an auditor bound by confidentiality who is not a competitor of WYRLO.

15. Obligations of the controller

The Customer undertakes to:

- have a legal basis for the processing and inform the data subjects;
- send WYRLO only the data needed, and no health data;
- document in writing any instruction regarding WYRLO's processing of the data, beyond the settings available in its workspace;
- ensure, beforehand and throughout the processing, that WYRLO complies with its obligations under the GDPR;

- supervise the processing, including through audits under the conditions of section 14.

---

16. Liability and governing law

Each party's liability is governed by article 82 of the GDPR and by the terms of use. In case of conflict between the terms of use and this Agreement on data protection, this Agreement prevails.

These terms are governed by French law. Failing an amicable agreement, any dispute shall be brought before the competent courts within the jurisdiction of the Lyon Court of Appeal, within the limits provided by law.

If your organisation needs a signed version of this Agreement, ask for it at contact@wyrlo.io.