Security and data

Version of November 18, 2026

Here is how WYRLO protects the data your application sends it through the API. This page describes the service as it works today.

The essentials

- Your documents stay with you: WYRLO never stores them.
- Question history is masked (on by default), then kept for the period chosen by your organisation, within the limit of its plan (14 to 90 days).
- Processed in France and the European Union; database in Paris.
- No AI is trained on your data.
- Access restricted to your organisation, with roles per member.
- Data processing agreement (GDPR) available.
- Certifications: none yet, and no external audit.

The details, for your IT and data protection teams

The path of your data

Your RAG

Your documents stay there: WYRLO never stores them.

↓ question, excerpts, answer

WYRLO API

Paris (eu-west-3). A request received in another region is refused without being read.

during processing

Built-in masking

In WYRLO's functions, in Paris, before anything is sent to Mistral AI and before storage.

Mistral AI

European endpoint: European Union and EFTA, according to Mistral AI. Checks answers in French and English: an excerpt of 600 characters at most, masked beforehand by WYRLO.

↓ masking

Masked history

Period chosen by your organisation, within the limit of its plan (14 to 90 days), then deleted overnight.

Subprocessors

The facts

Hosting	Paris (eu-west-3 region) for the database and functions
Documents	Never stored
Question history	Masked, kept according to your plan (14 to 90 days)
Encryption	In transit (HTTPS) and at rest (AES-256 for the database and its backups, at Supabase)
Access	Restricted to your organisation
Training	None: your traces train no model, neither ours nor a third party's.
API keys	Stored as a fingerprint, shown only once, revocable at any time.
Tracking	No non-essential cookie or tracking tool, on the website or in the customer workspace.
Certifications	None yet, and no external audit. Supabase and Vercel publish their own reports.
Data processing agreement	Request the data processing agreement

On this page

> Where your data is
>
> Your documents are never stored

Your data trains no model
Trace masking, limited retention
Encryption
Strict isolation between organisations
API keys
Activity log
Website and browser
Certifications and audits
Report a vulnerability

Where your data is

- Database and WYRLO functions (API, waitlist, improvement loop): Supabase, eu-west-3 region (Paris). The API processes every request in Paris: a request received in another region is refused without being read.
- API address (api.wyrlo.io): a route of WYRLO's web application, at Vercel, running in Paris (cdg1 region). It forwards each call to WYRLO's functions in Paris, enforces the Paris region, does not forward your IP address, and neither stores nor logs the content of calls. Calls then go through the network of Cloudflare, Supabase's provider, to the functions in Paris.
- Masking personal data: done by WYRLO itself, in its functions in Paris, before anything is sent to Mistral AI and before storage. No other provider is involved, and the masked values are never logged.
- Checking French and English answers: Mistral AI, a French company, through its European endpoint (inference in the European Union and EFTA countries, according to Mistral AI). Mistral AI only receives texts masked beforehand by WYRLO.
- Web application: Vercel, functions in the cdg1 region (Paris).
- Other providers and processing locations: see the Subprocessors page.

Subprocessors

Your documents are never stored

For each question, WYRLO receives the question, excerpts of the passages retrieved by your RAG, and the answer. Your documents stay with you: we never copy them. With the no-copy index, the text sent for indexing is masked, used to compute the vectors, then forgotten: WYRLO keeps the address of each passage, a fingerprint and its vector, never its text.

Your data trains no model

WYRLO never uses your traces (questions, passage excerpts, answers) or your documents to train or fine-tune AI models, whether ours or a third party's. They are used only to provide the service to your organisation: answer checking, the improvement loop specific to your organisation, which measures the effect of its settings on your own questions, and the weekly report.

This commitment is set out in the terms of use and in the data processing agreement.

Data processing agreement

Trace masking, limited retention

If your organisation has enabled masking (enabled by default), traces are masked before storage. Rules, with a validity check where one exists (the check digits of an IBAN, a card or a NIR), detect and then replace with a marker ("[EMAIL_1]", for example): email addresses, phone numbers, IBANs, bank card numbers, French

social security numbers (NIR), IP addresses, passport and identity card numbers (when a keyword announces them), postal addresses with a number and a street type, and recognisable API keys and tokens. Not masked: names of people and companies, addresses without a number or street type (a locality, for example) and any identifier without a recognisable form; dates, amounts and order numbers also stay, because verification must be able to compare them. This detection is automatic and does not guarantee completeness: to remove other data, names in particular, mask it before sending; WYRLO's SDKs can do this on your machine. If masking a trace fails, it is stored without any text (scores, decision and timings only, marked "text not kept"). If your project chooses "traces without text", no text is kept: decisions, confidence, scores and timings only. Only the 3 best passages keep an excerpt, of 600 characters at most.

They are kept for the period chosen by your organisation, within the limit of its plan (14 to 90 days), then deleted automatically every night.

Encryption

Data is encrypted:

- in transit: HTTPS (TLS) is mandatory between your application, the library, the API, the customer workspace and our hosting providers. A call to api.wyrlo.io is decrypted and re-encrypted by the Vercel route (Paris) and by the network of Cloudflare, Supabase's provider, to be forwarded; neither keeps its content for WYRLO;
- at rest: AES-256 encryption of the database and its daily backups, kept for 7 days, by our hosting provider Supabase.

Strict isolation between organisations

Each organisation only sees its own data. Isolation is enforced by access rules at database level, not just in the application code: a query can only read rows that belong to the signed-in person’s organisation.

API keys

- An API key is shown only once, when it is created.
- Only its hashed fingerprint is stored: the key itself cannot be read back, not even by WYRLO.
- A key can be revoked at any time in the project’s integration page; create a new one to replace it.

Activity log

Sensitive actions, such as creating an API key or changing a setting, are recorded in an activity log with who did them and when.

The log records the creation, modification and deletion of organisations, members and roles, invitations, projects, API keys, reliability settings and fixes. It can be viewed by the organisation’s owners and admins, and is kept for 1 year, then deleted automatically.

Website and browser

The website uses no non-essential cookies and no tracking tools. It enforces HTTPS, refuses to be displayed inside third-party pages and limits the information passed on to other sites.

Certifications and audits

WYRLO does not have any certification or external security audit yet. Its main hosting providers, Supabase and Vercel, publish their own compliance reports.

Report a vulnerability

Think you have found a security flaw? Write to contact@wyrlo.io with a description of the issue and the steps to reproduce it.

Please do not make the vulnerability public before it is fixed. We acknowledge receipt within 5 working days and keep you informed until it is fixed.