Security and data

Version of November 19, 2026

This is how WYRLO protects the data your application sends to it through the API. This page describes the service as it works today, real measures only.

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. Only the AI model you choose to draft an answer may process your data elsewhere, under your contract with it.

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.

No availability commitment (SLA) for now: a single environment, with no automatic backups.

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. Checks answers in French and English (an excerpt of 600 characters at most) and computes the index vectors: always on texts 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, at Supabase); encrypted manual backup copies
Access	Restricted to your organisation; each end client's data kept separate
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
- Answer drafted with your own model
- Encryption
- Strict isolation between organisations and between end clients
- API keys
- Activity log
- Website and browser
- Availability and continuity
- Certifications and audits
- Report a vulnerability

Where your data is

- WYRLO's database and functions (API, search, improvement loop): Supabase, eu-west-3 region (Paris). The API processes each request in Paris: a request received in another region is rejected without being read.
- API address (api.wyrlo.io) and remote MCP server: a route of the WYRLO website, at Vercel, run in Paris (cdg1 region). It forwards each call to WYRLO's functions in Paris, enforces the Paris region, does not pass on 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 of personal data: carried out by WYRLO itself, in its functions in Paris, before anything is sent to Mistral AI and, by

default, before storage. No other provider is involved, and masked values are never logged.

- Verification of answers in French and English, drafting by the model managed by WYRLO and zero-copy index vectors: Mistral AI, a French company, through its European endpoint. Mistral AI only receives texts masked beforehand by WYRLO.
- Other providers and places of processing: see the Subprocessors page.

Subprocessors

Your documents are never stored

For each question, WYRLO receives the question, the passage excerpts retrieved by your RAG and the answer. Your documents stay with you: they are not copied to us. With the zero-copy index, the text sent for indexing is masked, used to compute the vectors, then forgotten: WYRLO keeps the position of each passage, a fingerprint and its vector, never its text. The SDKs read your files (PDF, DOCX, PPTX, XLSX) on your machine.

Your data trains no model

WYRLO never uses your traces (questions, passage excerpts, answers) or your documents to train or fine-tune AI models, neither ours nor a third party's. They are used only to provide the service to your organisation: verification of answers, an improvement loop specific to each project, which measures the effect of its settings on your own questions, and a 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 keeps masking enabled (the default setting), traces are masked before storage; what goes to Mistral AI is masked in all cases. Rules, with a validity check where one exists (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 street number and street type, and recognisable API keys and tokens.

Not masked: names of people and companies, addresses without a street number or street type (a locality, for example) and any identifier with no recognisable form; dates, amounts and order numbers also remain, because the verification must be able to compare them. This detection is automatic and does not guarantee completeness: to remove other data, in particular names, mask it before sending. WYRLO’s SDKs can apply the same rules on your machine (option disabled by default).

If masking a trace fails, it is recorded without any text (scores, decision and durations only, with the mention “text not kept”). If your project chooses “traces without text”, no text is kept: decisions, confidence, scores and durations only. Only the top 3 passages keep an excerpt, of 600 characters at most.

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

Answer drafted with your own model

With /v1/answer (in preview) and the model of your choice, WYRLO passes the question and the passages, without masking, to the AI provider you designate, with your key. This provider processes the data under your own contract with it, possibly outside the European Union. If you save the key for a project, it is stored encrypted and is never displayed or logged. Mask the data on your side if necessary, or use the model managed by WYRLO, which only receives masked texts.

Encryption

Data is encrypted:

- in transit: HTTPS (TLS) mandatory between your application, the library, the API, the developer space 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, in order to be forwarded; neither of them keeps its content for WYRLO;
- at rest: AES-256 encryption of the database by our hosting provider Supabase; manual backup copies encrypted (AES-256) and kept offline.

Strict isolation between organisations and between end clients

Each organisation only sees its own data. Isolation is enforced by access rules at the database level, not only in the application code, and checked by automated tests before each release to production: a request can only read the rows of the signed-in person's organisation.

Within a project, each end client's data (index, search, traces) is separated by its identifier; search only covers the requested space. Deleting an end client immediately erases its index and its traces.

API keys

- An API key is shown only once, when it is created.
- Only its hash (SHA-256) is stored, with its visible beginning so you can recognise it: the key itself cannot be read back, not even by WYRLO.
- A key can be revoked at any time in the project's integration; 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 their author and date.

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

Website and browser

The website uses no non-essential cookies or tracking tools. It enforces HTTPS, prevents itself from being displayed in a third-party page, applies a content security policy and limits the information passed to other sites. Breached passwords are rejected (k-anonymity check); two-factor authentication is offered to every user.

Availability and continuity

WYRLO makes no availability commitment (no SLA). The service currently runs on a single environment, operated by a single person, with no on-call duty. A separate production environment will be recreated later.

No automatic backup of the database is made today: full copies are made manually, encrypted, checked by a test restore and kept offline, for 90 days at most.

If WYRLO does not respond in time, the SDKs let your RAG's answer through, marked as unverified. The status of the API, the website and emails is checked automatically every 5 to 15 minutes and published on the Status page. Each release to production passes automated tests, with a rollback prepared, and a written procedure governs incidents.

Service status

Certifications and audits

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

Report a vulnerability

Think you have found a flaw? Write to contact@wyrlo.io describing the problem and the steps to reproduce it.

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