Privacy policy

Version of November 19, 2026

This policy explains what personal data WYRLO processes, for what purpose, on what legal basis, for how long, with which providers, and what your rights are. It covers WYRLO's public website, developer space and API.

Contents

- Who is responsible
- Data protection officer
- Data processed
- Purposes and legal bases
- Mandatory data
- Retention periods
- Recipients and subprocessors
- Transfers outside the European Union
- Your rights
- Cookies and browser storage
- Security
- Changes

Who is responsible

For account, website, access request and quote request, billing and support data, the controller is Mayeul FLORY, sole trader (entrepreneur individuel; trade name: FUSION-IA), publisher of WYRLO, 49 chemin des Verrières, 69260 Charbonnières-les-Bains, France, reachable at contact@wyrlo.io.

For the data your application sends to the WYRLO API (questions, passages, answers, documents to index, traces), your organisation remains the controller, and WYRLO acts as a processor within the meaning of article 28 of the GDPR, under the data processing agreement.

If your organisation uses WYRLO to serve its own customers (end clients), each of these customers is generally the controller of its data, your organisation is its processor, and WYRLO is a sub-processor. Data subjects first contact the organisation that provides them with the service.

Data protection officer

WYRLO has not appointed a data protection officer. For any question about your personal data, write to contact@wyrlo.io.

Data processed

- Account data: name, work email address, organisation, role in the organisation, role given at sign-up (founder, developer…), sign-in information, two-factor authentication factors (name and date), email language (French or English, taken from the browser language at sign-up, editable in Account, Emails section).
- Sign-in with Google, if you choose it: Google sends us your name, email address, profile picture address and Google account identifier. This information is used only to create your account, sign you in and show your name to the members of your organisations; it is kept with your account, is never sold or passed on to third parties, and is used neither for advertising nor to train AI models. WYRLO's use and transfer of information received from Google APIs adheres to the Google API Services User Data Policy, including the Limited Use requirements.

- Breached password check: at sign-up and when changing a password, your browser sends the Pwned Passwords service of Have I Been Pwned the first 5 characters of the password's SHA-1 hash, never the password or its full hash (k-anonymity).
- Invitations: email address of the people invited to an organisation. WYRLO sends them the invitation link by email (at most 50 emails per organisation per 24 hours; beyond that, the link is only shown to the person who invites, who passes it on themselves).
- Access requests, if you request access: email address, page language, date of the request and date of confirmation (click on the link received by email; the link carries a random token of which only a fingerprint is kept); to limit abuse, a fingerprint of your IP address (computed with a secret key; the address itself is not recorded) and the time of each request.
- Request for the Enterprise and large partners plan, if you fill in the form: work email address, company, role, type of organisation, estimated number of end clients and volume of questions, ticked needs, timeline, message (500 characters at most), page language, date of the request and date of confirmation (click on the link received by email), then our exchanges and our quote; to limit abuse, a fingerprint of your IP address, kept 24 hours (the address itself is not recorded).
- Traces: for each verified question, the question, the answer, the confidence level, the decision, the language, the request identifier chosen by your application and, where applicable, the end client identifier and the user's feedback (useful answer or not); for each passage retrieved by your RAG, its identifier, its source (name of the original document), a fingerprint and its scores, and for the top 3 passages only, an excerpt of 600 characters at most.
- Trace masking: if your organisation keeps masking enabled (the default setting), traces are masked before storage; if it disables it, traces are kept in clear text. 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 (masking option, disabled by default); masking of people's names in the SDKs is still in preparation.

- 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.
- End clients, if your organisation serves its own customers with WYRLO: for each one, the identifier you choose, an optional display name, its status (active or suspended) and the number of verifications for the month. No question or text is attached to it. Do not put a person's name in it: the identifier only serves to separate your customers' data.
- Zero-copy index, if your project enables it: for each document sent for indexing, its identifier, its version, its tags and its number of passages; for each passage, its position in the document, a salted digital fingerprint specific to the project and a numerical representation (vector). The text sent is masked by WYRLO, used to compute the vectors at Mistral AI, then forgotten: it is never stored.
- Passage fingerprints: to recognise a passage already analysed without keeping its text, WYRLO keeps a digital fingerprint (SHA-256) of the passage, a numerical representation (vector)

computed on its beginning and its security verdict (injection detected or not).

- Drafted answer (/v1/answer, in preview): the question and the passages sent so that a cited answer can be drafted and then verified. With the model managed by WYRLO, they are masked and then sent to Mistral AI. With the model of your choice, WYRLO passes them on as they are, without masking, to the AI provider you designate (OpenAI, Anthropic, Mistral AI, Azure OpenAI or a compatible address), with your key; if you save this key for a project, it is stored encrypted. The drafted answer is then verified and recorded as a trace.
- Documents read by the SDKs: WYRLO's SDKs read files (PDF, DOCX, PPTX, XLSX) on your machine; only the text you then choose to index or have verified is sent to WYRLO. Server-side reading of scanned PDFs with Mistral AI's OCR is not yet open; when it opens, this policy will be updated before anything is sent.
- Improvement loop analyses: failure groups, missing topics and proposed fixes, which include example questions (masked if masking is enabled); weekly reports (topics and figures).
- Weekly report sent by email: recipient's email address, names of the organisation and the project, and aggregated indicators for each project (score, change since the previous week, number of questions analysed, of "I don't know", of automatic fixes applied, of missing topics and of fixes to make on your side), with a link to the report in the developer space. The email contains no excerpt of a question, answer or passage, and no topic name.
- Other service emails: welcome, opening of your access, monthly quota warnings and, once they open, spending cap and end-of-trial warnings, sent to owners and administrators: recipient's address, organisation name, usage figures and cap. No excerpt of a question or answer.
- Activity log: sensitive actions carried out in your organisation, with their author and date.

- Support exchanges: your messages to contact@wyrlo.io (directly or through the “Need help?” button) and our replies; the questions asked to the help assistant and its answers.
- Billing data, if you subscribe to a paid plan: name or company name, billing address, VAT number where applicable, billing email address, plan subscribed, billed usage (verifications beyond the included volume, active end clients), amounts, dates and status of payments, invoices. Payment is processed by Stripe: WYRLO neither receives nor keeps your full card number, only limited information (card type, last four digits, expiry date) so that you can recognise the saved payment method. Online payment is not yet open.
- Technical logs needed for the operation and security of the service: at our hosting providers, IP address, approximate location inferred from this address (country, region, city, network operator), date and time, requested address, response code, browser and technical fingerprint of the encrypted connection; for the API, the visible beginning of the API key (15 characters, never the whole key) and information about each request (organisation, decision, durations, language), never the content of questions, passages or answers. Calls made through api.wyrlo.io reach Supabase with a Vercel address, not yours.

Your documents are never stored. WYRLO sells no data and uses neither your traces, nor your documents, nor your questions to train AI models.

Purposes and legal bases

- Providing the service to your organisation: verifying answers against their sources, computing the confidence level, deciding to answer or to say “I don’t know”, detecting injections, indexing and searching without copying, drafting a cited answer at your request, separating your end clients’ data. Legal basis: performance of the

contract; for the data of your RAG's users, WYRLO acts on your instructions, as a processor.

- Adjusting each project's settings from its own traces (every night for paid plans, every week for the Free plan), with proof and rollback, and producing the weekly report. Legal basis: performance of the contract.
- Sending the weekly reliability report by email, on Mondays, when it flags something (fix applied, missing topic, fix to make on your side, drop in the score): by default to the organisation's owner only; each member chooses whether to receive it in Account, Emails section. Legal basis: performance of the contract.
- Creating and managing your account, your organisation, its members and its invitations. Legal basis: performance of the contract.
- Answering the questions asked to WYRLO's help assistant, based on our help centre: the question is masked by WYRLO, then an answer is drafted by Mistral AI and verified against the help centre's answers before being displayed. Legal basis: performance of the contract.
- Invoicing paid plans, collecting payments through Stripe, handling failed payments and, where applicable, recovering sums due. Legal bases: performance of the contract; legal obligation for issuing and keeping invoices; legitimate interest for debt recovery.
- Confirming your address and then writing to you when your access opens, if you ask for it: a confirmation email, then a single email when your access opens, no marketing. Your address only enters the list after you click the confirmation link. Legal basis: pre-contractual measures taken at your request.
- Responding to a request for the Enterprise and large partners plan: confirming your address, studying the request and, if it falls within this plan, offering you a quote. No marketing. Legal basis: pre-contractual measures taken at your request.

- Ensuring the security of the service and preventing abuse: number of requests limited per IP address, breached password check, activity log, technical logs. Legal basis: legitimate interest (protecting the service and its customers).
- Responding to your requests to support. Legal basis: legitimate interest, performance of the contract when the request concerns the subscribed service.

No processing is based on your consent: the website uses no cookie or tracker that would require it. WYRLO does not use traces for any purpose other than those above, and in particular not to train AI models.

Mandatory data

- An email address and a password, or sign-in with Google, are needed to create an account: without them, the account cannot be created. The name is optional.
- To request access, only the email address is needed. For a quote request, the work email address, the company and the type of organisation are needed to study it.
- For a paid plan, a billing address and a payment method are needed, under the contract and accounting obligations.

Retention periods

- Traces: the period chosen by your organisation, within the limit of its plan (14 days for Free, 30 for Developer, 90 for Production and Partner, or the period agreed in specific terms), then deleted automatically every night. If the plan changes to one with a shorter period, traces older than the new limit are deleted the following night.

- Passage fingerprints and security verdicts, without the text: same period as traces, counted from the last time the passage was received, then deleted automatically every night.
- Zero-copy index (positions, fingerprints and vectors, without the text): until the deletion of the document, the end client's space, the project or the organisation, or until your organisation empties the index.
- Example questions included in the improvement loop's analyses: removed at the same time as the corresponding traces. Analyses (failure groups, missing topics, fixes) and weekly reports, which keep only the titles of topics and fixes: for as long as the service is used, then deleted with the organisation; a topic or group that has no example left and does not come back for 180 days is deleted automatically.
- Accounts and organisations: for as long as the service is used. Anyone can delete their account at any time in Account, "Delete my account" section: it is then erased immediately, with its profile and memberships. An organisation's owner can delete it at any time in Organisation, Data section: its data (projects, traces, index, end clients, analyses) is then erased immediately.
  A closure requested at contact@wyrlo.io is carried out within 30 days.
- AI provider keys saved for a project (/v1/answer): encrypted, until your organisation removes them or the project is deleted.
- Sign-ins: sign-in sessions are deleted after 90 days without use (you then sign in again); confirmation, sign-in and password reset links: valid for 7 days at most, then deleted; unfinished sign-in requests: 1 day; then deleted automatically.
- Invitations: the invited person's email address is kept until 30 days after the invitation ends (accepted, cancelled or expired), then deleted automatically; it remains in the activity log until 1 year after the invitation was sent. The invitation link expires after 7 days.
- Activity log: 1 year, then deleted automatically.

- Access requests: unconfirmed request, 7 days after the request; confirmed request, until your access opens (the day we write to you), then three months after that email if you have not created an account, or 30 days after your account is created, and in any case at most 12 months after the request, then deleted automatically. You can ask to be removed at any time by writing to contact@wyrlo.io. IP address fingerprints of requests: 24 hours.
- Requests for the Enterprise and large partners plan: unconfirmed request, 7 days; request not followed up, 12 months after the last exchange; request that leads to a contract, for the term of the contract. IP address fingerprints: 24 hours. You can ask for your request to be deleted at any time by writing to contact@wyrlo.io.
- End clients: until the deletion of the end client, the project or the organisation; deletion immediately erases its index and its traces. The number of verifications for the current month is kept without an identifier until the invoice.
- Invoices: 10 years, under accounting obligations (article L. 123-22 of the French Commercial Code). No invoice is issued as long as no paid plan is subscribed.
- Billing data other than invoices: for the duration of the subscription, then 5 years after it ends, the limitation period for actions between professionals (article L. 110-4 of the French Commercial Code).
- Support exchanges: 3 years after the last contact.
- Questions asked to the help assistant: the masked question, the answer and the verification decision, 30 days, then deleted automatically every night; the date of the question, 24 hours (limit of 5 questions per day).
- Backup copies: WYRLO currently makes no automatic backup of its database. Full copies are made manually, occasionally, encrypted (AES-256) and kept offline by the publisher, for 90 days at most, solely to restore the service after an incident. Deleted data may therefore remain for at most 90 days in such a copy, without being used.

- Emails sent and sending logs, at our email provider (Resend): 30 days for the duration of the account, backup copies 7 days, erasure within 90 days after the end of the service, according to Resend's GDPR page.
- Our hosting providers' technical logs: at most 7 days at Supabase (API gateway, authentication, functions and database) and 1 day for function logs at Vercel. Supabase keeps its logs on its logging infrastructure, hosted by Google, whose storage location is not guaranteed to be in the European Union; any transfers are governed by standard contractual clauses (see the Subprocessors page).

Data retention at Resend (Resend's GDPR page)

Recipients and subprocessors

Data is only accessible to authorised people at WYRLO (currently, the publisher alone) and in your organisation, and to the technical subprocessors that help us provide the service. The publisher only accesses a customer's traces for the support that customer requests, for the security of the service or for a legal obligation. The list of subprocessors, their role, the data concerned and the place of processing are given on a dedicated page.

With /v1/answer and the model of your choice, the question and the passages are sent to the AI provider you designate, with your key: this provider is not a subprocessor of WYRLO; it acts under your own contract with it, under your responsibility, and may process the data outside the European Union.

For paid plans, Stripe processes payments on behalf of WYRLO. For its own purposes, in particular fraud prevention and compliance with its legal and regulatory obligations, Stripe acts as an independent controller, according to its privacy policy.

List of subprocessors Stripe's privacy policy

Transfers outside the European Union

The database and the functions are in Paris. Some providers are, however, established outside the European Union or may process data there:

- Vercel Inc. (United States): hosting of the website and of the API address, functions run in Paris;
- Resend (Plus Five Five, Inc., United States): emails sent from Ireland, sending account data stored in the United States;
- Supabase Pte. Ltd. (Singapore): database in Paris; possible transfers to the United States and Singapore for some service data, and technical logs kept at Google with no guaranteed location in the European Union; its calls go through Cloudflare's global network;
- Stripe: US group, for payments;
- Mistral AI (France): limited transfers possible to its own subprocessors outside the European Union and the EFTA countries;
- Have I Been Pwned (Australia): only a fragment of a password hash and the browser's IP address.

According to these providers' contracts, these transfers are governed by the European Commission's standard contractual clauses (decision 2021/914) and, for certified US companies, by the EU–US Data Privacy Framework. You can obtain a copy of these safeguards by writing to contact@wyrlo.io.

Your rights

The GDPR gives you the following rights over your data:

- access;
- rectification;
- erasure;
- restriction of processing;
- objection;
- portability;
- instructions on what happens to your data after your death.

Without writing to us, you can download a copy of your account data and delete your account from the Account page. To exercise your other rights, write to contact@wyrlo.io. We reply within one month.

For data contained in traces or in the index, first contact the organisation that uses WYRLO (or the end client it serves): it is the controller, and we help it respond to you.

WYRLO takes no decision producing legal effects concerning you, or similarly significantly affecting you, based solely on automated processing (article 22 of the GDPR). The “answer” or “I don’t know” decisions concern the answers of a customer organisation’s RAG, which remains responsible for them.

If you believe your rights are not respected, you can lodge a complaint with the French data protection authority (Commission nationale de l’informatique et des libertés, CNIL), 3 place de Fontenoy, TSA 80715, 75334 Paris Cedex 07, or online at cnil.fr, or with the data protection authority of your country of residence in the European Union.

Lodge a complaint with the CNIL CNIL website

Cookies and browser storage

No non-essential cookies: no analytics, no advertising, no tracking tools, on the website or in the developer space.

The public website sets no cookies. The sign-in and sign-up pages, then the developer space, only use sign-in session cookies, which are strictly necessary for the service (so they do not require consent), valid for 400 days at most and deleted when you sign out, plus a temporary cookie during sign-in with Google.

Your theme choice (light, dark or system) is kept in your browser, in localStorage; after an error, a technical reference is kept for 30 minutes in sessionStorage so you can give it to support. None of this is sent to our servers.

Once paid plans open, payment will take place on Stripe's pages; Stripe may use cookies there that are necessary for payment security and fraud prevention, described in its cookie policy.

Security

The technical and organisational measures that protect your data are described on the Security page. In the event of a personal data breach, WYRLO notifies the organisations concerned within 48 hours of becoming aware of it and, for the data it is the controller of, notifies the CNIL within 72 hours where the law requires it.

Security

Changes

This policy may change. The date of the current version is shown at the top of the page, and previous versions remain available in the version history. In the event of a significant change, we notify account holders by email before it takes effect.