Privacy policy

Version of November 18, 2026

This policy explains which personal data WYRLO processes, why, for how long, and what your rights are. It covers the public website and the WYRLO service.

Contents

- Who is responsible
- Data protection officer
- Data we process
- Purposes
- Legal bases
- Retention periods
- Recipients and subprocessors
- Your rights
- Cookies and browser storage
- Security
- Changes

Who is responsible

For account and website 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 traces sent to the WYRLO API, your organisation remains the controller. WYRLO acts as a processor within the meaning of article 28 of the GDPR, under the data processing agreement.

Data protection officer

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

Data we process

- Account data: name, work email address, organisation, role in the organisation, role given at sign-up (founder, developer…), sign-in information, 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 adhere 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. The invitation link is passed on by the person who invites; WYRLO does not send it by email.
- Access requests, if you request access: email address and, if you provide them, organisation and intended use (500 characters at most), 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 stored) and the time of each request.

- Request for the Enterprise and major partners plan, if you fill in the form: work email address, company, role, type of organisation, estimated number of end customers 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); to limit abuse, a hash of your IP address, kept 24 hours (the address itself is not stored).
- Traces: the question asked, the answer produced, the confidence level and the decision; for each passage retrieved by your RAG, its identifier, its source (name of the original document) and its scores, and for the 3 best passages only, an excerpt of 600 characters at most. 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.
- End customers, 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 in the month. No question or text is attached to it. Do not put a person's name in it: the identifier only serves to keep your customers' data apart.

- Passage fingerprints: to recognise a passage already analysed without keeping its text, WYRLO keeps a digital fingerprint (SHA-256) of the passage, a numeric representation (vector) computed on its beginning and its security verdict (injection detected or not).
- Improvement loop analyses: failure groups, missing topics and suggested fixes, which include example questions (masked if masking is enabled); weekly reports (topics and figures).
- Weekly report sent by email: the recipient's email address, the organisation and project names, and aggregated indicators for each project (score, change since the previous week, number of questions analysed, of "I don't know" answers, of automatic fixes applied, of missing topics and of fixes to make on your side), with a link to the report in the customer workspace. The email contains no excerpt of any question, answer or passage, and no topic name.
- Monthly cap warnings, by email: address of owners and admins, organisation name, number of analysed questions and the month's cap. No excerpt of any question or answer.
- Activity log: sensitive actions performed in your organisation, with who did them and when.
- 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, amounts, dates and status of payments, invoices. Payments are processed by Stripe: WYRLO never receives or stores your full card number, only limited

information (card type, last four digits, expiry date) so that you can recognise the saved payment method. No paid plan is open yet.

- Technical logs needed to run and secure the service: at our hosting providers, IP address, approximate location derived from that address (country, region, city, network operator), date and time, requested address, response code, browser and a technical fingerprint of the encrypted connection; for the API, the first 10 characters of the API key (never the whole key) and information about each request (organisation, decision, processing time, 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. If you use the no-copy index, WYRLO receives the text to index, masks it, has Mistral AI compute its vectors, then forgets it: only the address, a fingerprint and the vector of each passage are kept.

Purposes

- Providing the service: checking answers against their sources, computing the confidence level, and deciding whether to answer or say “I don’t know”.
- Answering the questions asked to WYRLO’s help assistant, from our help centre: the question is masked by WYRLO, then an answer is drafted and checked against the help centre’s answers before it is displayed.
- Adjusting your organisation’s settings from its own traces (every night, or every week for the current access), and producing the weekly report.
- Sending the weekly reliability report by email, on Mondays, when it flags something (a correction applied, a missing topic, a fix to make on your side, a score drop): by default to the organisation’s

owner only; each member chooses whether to receive it in Account › Emails section.

- Managing your account, your organisation and, where relevant, your subscription.
- Invoicing paid plans, collecting payments through Stripe, handling failed payments and, where necessary, recovering amounts due.
- Keeping the service secure and preventing abuse: number of requests limited per IP address, in particular on access requests.
- Confirming your address and then writing to you when your access opens, if you ask: one confirmation email, then a single email when your access opens, no marketing. Your address is only added to the list after you click the confirmation link.
- Answering a request for the Enterprise and major partners plan: confirming your address, studying the request and, if it falls within this plan, offering you a quote. No marketing.
- Responding to your requests.

WYRLO does not use traces for any other purpose, and in particular not to train AI models.

Legal bases

- Performance of the contract: providing the service (including sending the weekly report by email), managing your account, subscribing to, paying for and invoicing paid plans.
- Pre-contractual steps taken at your request: access requests, requests for the Enterprise and major partners plan.
- Legitimate interest: security of the service, abuse prevention, activity log, replies to support requests, recovery of amounts due.
- Legal obligation: issuing and keeping invoices and accounting records.

- No processing is based on your consent: the website uses no cookie or tracker that would require it.
- An email address and a password, or signing in with Google, are required to create an account: without them, the account cannot be created. Your name is optional. To request access, only the email address is required.

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), then deleted automatically every 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.
- 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 is then erased immediately. An account closure requested at contact@wyrlo.io is carried out within 30 days. Backups, kept for 7 days, then disappear.
- Sign-ins: sign-in sessions are deleted after 90 days without use (you then sign in again); confirmation, sign-in and password

reset links: 7 days; 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 automatic deletion. 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 major partners plan: unconfirmed request, 7 days; request with no follow-up, 12 months after the last exchange; request that leads to a contract, for the duration of the contract. IP address hashes: 24 hours. You can ask for your request to be deleted at any time by writing to contact@wyrlo.io.
- End customers: until the end customer, the project or the organisation is deleted; deletion immediately erases its indexed documents and its traces. The number of verifications for the current month is kept until the invoice.
- Invoices: 10 years, under French accounting obligations (article L. 123-22 of the French Commercial Code). No invoice is issued until a 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 claims between businesses (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 a day).
- Database backups: daily, encrypted and kept for 7 days by our hosting provider Supabase. Deleted data disappears from them within 7 days at most.
- Emails sent and sending logs, at our email provider (Resend): 30 days while the account is active, backup copies 7 days, deletion within 90 days of the end of the service, according to Resend's GDPR page.
- Technical logs at our hosting providers: 7 days at Supabase (API gateway, authentication, functions and database) and 1 hour 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 covered by standard contractual clauses (see the Subprocessors page).

Data protection at Resend (Resend's GDPR page)

Database backups (Supabase documentation)

Recipients and subprocessors

Data is only accessible to authorised people at WYRLO and in your organisation, and to the technical subprocessors that help us provide the service. The list of subprocessors, their role, the data concerned and where it is processed is on a dedicated page.

Some of these providers are established outside the European Union or may process data there, in particular Vercel, Resend and Cloudflare (United States), as well as Supabase for its technical logs, kept at Google with no guaranteed location in the European Union. These transfers are covered by the European Commission's standard contractual clauses and, for certified US companies, by the EU–US Data Privacy Framework, according to these providers'

contracts. You can obtain a copy of these safeguards by writing to contact@wyrlo.io.
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, under its privacy policy. Each provider's privacy policy is linked from the Subprocessors page.

List of subprocessors Stripe privacy policy

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, contact the organisation that uses WYRLO first: it is the controller, and we help it respond to you.

WYRLO makes no decision that produces legal effects concerning you, or similarly significantly affects you, based solely on automated processing (Article 22 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 being respected, you can lodge a complaint with the French data protection authority, the Commission nationale de l'informatique et des libertés (CNIL), 3 place de Fontenoy, TSA 80715, 75334 Paris Cedex 07, France, 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 customer area.

The public website sets no cookies. The sign-in and sign-up pages, then the customer area, only use sign-in session cookies, which are strictly necessary for the service (so they need no 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. It is never sent to our servers.

When paid plans open, payment will take place on pages or components provided by Stripe; Stripe may use cookies there that are needed 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.

Security

Changes

This policy may change. The date of the current version is shown at the top of the page. In case of a significant change, we notify account holders by email before it takes effect.