Sécurité et données

Version du 19 novembre 2026

Voici comment WYRLO protège les données que votre application lui transmet par l'API. Cette page décrit le service tel qu'il fonctionne aujourd'hui, mesures réelles seulement.

L'essentiel

Vos documents restent chez vous : WYRLO ne les stocke jamais.

L'historique des questions est masqué (réglage activé par défaut), puis conservé pendant la durée choisie par votre organisation, dans la limite de son offre (14 à 90 jours).

Traitement en France et dans l'Union européenne ; base de données à Paris. Seul le modèle d'IA que vous choisissez pour rédiger une réponse peut traiter vos données ailleurs, selon votre contrat avec lui.

Aucun entraînement d'IA sur vos données.

Accès réservé à votre organisation, avec des rôles par membre.

Contrat de sous-traitance (RGPD) disponible.

Certifications : aucune pour l'instant, ni audit externe.

Aucun engagement de disponibilité (SLA) pour l’instant : un seul environnement, sans sauvegarde automatique.

Le détail, pour votre DSI et votre DPO

Le chemin de vos données

Votre RAG

Vos documents y restent : WYRLO ne les stocke jamais.

↓ question, extraits, réponse

API WYRLO

Paris (eu-west-3). Une requête reçue dans une autre région est refusée sans être lue.

pendant le traitement

Masquage intégré

Dans les fonctions de WYRLO, à Paris, avant tout envoi à Mistral AI et avant stockage.

Mistral AI

Point d’accès européen. Vérifie les réponses en français et en anglais (extrait de 600 caractères au plus) et calcule les vecteurs de l’index : toujours des textes masqués au préalable par WYRLO.

↓ masquage

Historique masqué

Durée choisie par votre organisation, dans la limite de son offre (14 à 90 jours), puis supprimée chaque nuit.

Sous-traitants

Les faits

Hébergement	Paris (région eu-west-3) pour la base de données et les fonctions
Documents	Jamais stockés
Historique des questions	Masqué, conservé selon votre offre (14 à 90 jours)
Chiffrement	En transit (HTTPS) et au repos (AES-256 pour la base, chez Supabase) ; copies de sauvegarde manuelles chiffrées
Accès	Réservé à votre organisation ; données de chaque client final séparées
Entraînement	Aucun : vos traces n'entraînent aucun modèle, ni le nôtre ni celui d'un tiers.
Clés d'API	Stockées sous forme d'empreinte, affichées une seule fois, révocables à tout moment.
Suivi	Aucun cookie non essentiel ni outil de suivi, sur le site comme dans l'espace client.
Certifications	Aucune pour l'instant, ni audit externe. Supabase et Vercel publient leurs propres rapports.

Contrat de sous-traitance Demander le contrat de sous-traitance

Sur cette page

- Où sont vos données
- Vos documents ne sont jamais stockés
- Vos données n'entraînent aucun modèle
- Masquage des traces, durée limitée
- Réponse rédigée avec votre propre modèle
- Chiffrement
- Isolation stricte entre organisations et entre clients finaux
- Clés d'API
- Journal d'activité
- Site et navigateur
- Disponibilité et continuité
- Certifications et audits
- Signaler une vulnérabilité

Où sont vos données

- Base de données et fonctions de WYRLO (API, recherche, boucle d'amélioration) : Supabase, région eu-west-3 (Paris). L'API traite chaque requête à Paris : une requête reçue dans une autre région est refusée sans être lue.
- Adresse de l'API (api.wyrlo.io) et serveur MCP distant : une route du site de WYRLO, chez Vercel, exécutée à Paris (région cdg1). Elle transmet chaque appel aux fonctions de WYRLO à Paris, impose la région de Paris, ne transmet pas votre adresse IP, et ne stocke ni ne journalise le contenu des appels. Les appels passent ensuite par le réseau de Cloudflare, prestataire de Supabase, jusqu'aux fonctions à Paris.
- Masquage des données personnelles : fait par WYRLO lui-même, dans ses fonctions à Paris, avant tout envoi à Mistral AI et, par

défaut, avant stockage. Aucun autre prestataire n'y participe, et les valeurs masquées ne sont jamais journalisées.
- Vérification des réponses en français et en anglais, rédaction par le modèle géré par WYRLO et vecteurs de l'index sans copie : Mistral AI, entreprise française, par son point d'accès européen. Mistral AI ne reçoit que des textes masqués au préalable par WYRLO.
- Autres prestataires et lieux de traitement : voir la page Sous-traitants.

Sous-traitants

Vos documents ne sont jamais stockés

Pour chaque question, WYRLO reçoit la question, les extraits de passages retrouvés par votre RAG et la réponse. Vos documents restent chez vous : ils ne sont pas copiés chez nous. Avec l'index sans copie, le texte envoyé à indexer est masqué, sert à calculer les vecteurs, puis est oublié : WYRLO garde la position de chaque passage, une empreinte et son vecteur, jamais son texte. Les SDK lisent vos fichiers (PDF, DOCX, PPTX, XLSX) sur votre machine.

Vos données n'entraînent aucun modèle

WYRLO n'utilise jamais vos traces (questions, extraits de passages, réponses) ni vos documents pour entraîner ou affiner des modèles d'IA, ni les nôtres ni ceux d'un tiers. Elles servent uniquement à fournir le service à votre organisation : vérification des réponses, boucle d'amélioration propre à chaque projet, qui mesure l'effet de ses réglages sur vos propres questions, et rapport hebdomadaire.

Cet engagement figure dans les conditions générales d'utilisation et dans le contrat de sous-traitance.

Contrat de sous-traitance

Masquage des traces, durée limitée

Si votre organisation garde le masquage activé (réglage par défaut), les traces sont masquées avant stockage ; ce qui part chez Mistral AI est masqué dans tous les cas. Des règles, avec un contrôle de validité quand il existe (clé d'un IBAN, d'une carte ou d'un NIR), repèrent puis remplacent par une marque (« [EMAIL_1] », par exemple) : les adresses e-mail, numéros de téléphone, IBAN, numéros de carte bancaire, numéros de sécurité sociale français (NIR), adresses IP, numéros de passeport et de carte d'identité (quand un mot-clé les annonce), adresses postales avec numéro et type de voie, clés d'API et jetons reconnaissables.

Ne sont pas masqués : les noms de personnes et d'entreprises, les adresses sans numéro ni type de voie (un lieu-dit, par exemple) et tout identifiant sans forme reconnaissable ; les dates, montants et numéros de commande restent aussi, car la vérification doit pouvoir les comparer. Ce repérage est automatique et ne garantit pas l'exhaustivité : pour retirer d'autres données, notamment les noms, masquez-les avant l'envoi. Les SDK de WYRLO peuvent appliquer les mêmes règles sur votre machine (option désactivée par défaut).

Si le masquage d'une trace échoue, elle est enregistrée sans aucun texte (scores, décision et durées seulement, avec la mention « texte non conservé »). Si votre projet choisit « traces sans texte », aucun texte n'est gardé : décisions, confiance, scores et durées seulement. Seuls les 3 meilleurs passages gardent un extrait, de 600 caractères au plus.

Les traces sont conservées pendant la durée choisie par votre organisation, dans la limite de son offre (14 à 90 jours), puis supprimées automatiquement chaque nuit.

Réponse rédigée avec votre propre modèle

Avec /v1/answer (en préversion) et le modèle de votre choix, WYRLO transmet la question et les passages, sans masquage, au fournisseur d'IA que vous désignez, avec votre clé. Ce fournisseur traite les données selon votre propre contrat avec lui, éventuellement hors de l'Union européenne. Si vous enregistrez la clé pour un projet, elle est conservée chiffrée et n'est jamais affichée ni journalisée. Masquez les données de votre côté si nécessaire, ou utilisez le modèle géré par WYRLO, qui ne reçoit que des textes masqués.

Chiffrement

Les données sont chiffrées :

- en transit : HTTPS (TLS) obligatoire entre votre application, la bibliothèque, l'API, l'espace développeurs et nos hébergeurs. Un appel à api.wyrlo.io est déchiffré puis rechiffré par la route de Vercel (Paris) et par le réseau de Cloudflare, prestataire de Supabase, pour être transmis ; aucun des deux n'en conserve le contenu pour WYRLO ;
- au repos : chiffrement AES-256 de la base de données par notre hébergeur Supabase ; copies de sauvegarde manuelles chiffrées (AES-256) et gardées hors ligne.

Isolation stricte entre organisations et entre clients finaux

Chaque organisation ne voit que ses propres données. L'isolation est appliquée par des règles d'accès au niveau de la base de données, pas seulement dans le code de l'application, et vérifiée par des tests automatisés avant chaque mise en production :

une requête ne peut lire que les lignes de l'organisation de la personne connectée.

Dans un projet, les données de chaque client final (index, recherche, traces) sont séparées par son identifiant ; la recherche ne porte que sur l'espace demandé. La suppression d'un client final efface aussitôt son index et ses traces.

Clés d'API

- Une clé d'API n'est affichée qu'une seule fois, à sa création.
- Seule son empreinte (SHA-256) est stockée, avec son début visible pour la reconnaître : la clé elle-même ne peut pas être relue, y compris par WYRLO.
- Une clé peut être révoquée à tout moment dans l'intégration du projet ; créez-en une nouvelle pour la remplacer.

Journal d'activité

Les actions sensibles, comme la création d'une clé d'API ou un changement de réglage, sont enregistrées dans un journal d'activité, avec leur auteur et leur date.

Sont journalisées les créations, modifications et suppressions d'organisations, de membres et de rôles, d'invitations, de projets, de clés d'API, de clients finaux, de réglages de fiabilité et de corrections. Le journal est consultable par les propriétaires et les administrateurs de l'organisation, et conservé 1 an, puis supprimé automatiquement.

Site et navigateur

Le site n'utilise aucun cookie non essentiel ni outil de suivi. Il impose HTTPS, interdit son affichage dans une page tierce, applique une politique de sécurité du contenu et limite les informations transmises aux autres sites. Les mots de passe divulgués sont refusés (vérification par k-anonymat) ; la double authentification est proposée à chaque utilisateur.

Disponibilité et continuité

WYRLO ne prend aucun engagement de disponibilité (aucun SLA). Le service fonctionne aujourd'hui sur un seul environnement, exploité par une seule personne, sans astreinte. Un environnement de production distinct sera recréé plus tard.

Aucune sauvegarde automatique de la base n'est faite aujourd'hui : des copies complètes sont faites à la main, chiffrées, vérifiées par une restauration d'essai et gardées hors ligne, au plus 90 jours.

Si WYRLO ne répond pas à temps, les SDK laissent passer la réponse de votre RAG, marquée non vérifiée. L'état de l'API, du site et des e-mails est contrôlé automatiquement toutes les 5 à 15 minutes et publié sur la page Statut. Chaque mise en production passe des tests automatiques, avec un retour arrière préparé, et une procédure écrite encadre les incidents.

État des services

Certifications et audits

WYRLO n'a pas encore de certification ni d'audit de sécurité externe. Ses principaux hébergeurs, Supabase et Vercel, publient leurs propres rapports de conformité.

Signaler une vulnérabilité

Vous pensez avoir trouvé une faille ? Écrivez à contact@wyrlo.io en décrivant le problème et les étapes pour le reproduire.

Merci de ne pas rendre la faille publique avant sa correction. Nous accusons réception sous 5 jours ouvrés et vous tenons informé jusqu'à la correction.