
Privacy Policy

Mind Web Concierge

Last Updated

03/03/2026

Data Controller

For the purposes of the General Data Protection Regulation (EU) 2016/679 (“GDPR”), the entity operating Mind Web Concierge (“we”, “us”, “our”) acts as the Data Controller in relation to the processing of personal data described in this Policy.

For any data protection inquiries, please contact us through the official website contact channels.

Scope of This Policy

This Privacy Policy explains how information is collected, processed, stored, and protected when users interact with the Mind Web Concierge chat feature.

The Service is designed to operate primarily through anonymous interactions and does not require user registration.

Categories of Data Processed

Data Provided by Users

- Messages, questions, and prompts submitted by users.
- Any information voluntarily included in those messages.

Users are not required to provide personal data. If voluntarily included, it is processed solely to generate a response.

Automatically Collected Technical Data

- Session ID
- IP address
- Screen resolution
- Platform
- Timezone
- Language
- Browser type

This data is used strictly for system functionality, security, abuse prevention, and performance optimization.

Authentication & Token Management

The plugin processes administrator credentials (username, password) and authentication tokens to securely connect with backend services. Tokens are securely stored, automatically refreshed when expired, and used exclusively for authenticated API communication.

Mind Spaces Integration

When enabled, notebook identifiers, category IDs, indexing configurations, and external connection data are processed to retrieve and manage knowledge repositories.

Content Indexing (WordPress & WooCommerce)

When indexing is enabled, post content, product data, metadata, URLs, header structures, and configuration parameters are securely transmitted to the RAG service for embedding and retrieval purposes.

AI Question Processing (Streaming)

User questions, category IDs, optional conversation IDs, and retrieval parameters are securely transmitted to the RAG API via encrypted streaming connections.

Subscription & Payment Processing (Stripe)

For subscription management, the system processes App GUID, product ID, customer email (for trials), subscription ID, invoice number, and subscription status.

Payment data such as credit card numbers is processed directly by Stripe and is not stored by Mind Web Concierge.

LLM Configuration Management

Administrators may configure Artificial Intelligence (AI) models used by the service. This may include storing configuration details such as the model name, provider, API keys, base API URLs, and indexing configurations required for AI processing.

The Service may utilize AI models provided by external providers, including OpenAI (ChatGPT models), in order to generate responses, summarize content, or process user queries.

When AI processing is performed:

- Requests may include user prompts or indexed content necessary to generate a response.
- API keys required to authenticate with AI providers are securely stored and never publicly exposed.
- Communications with AI providers occur over encrypted HTTPS connections.
- AI providers process data solely for the purpose of generating responses to user requests.

For more information about OpenAI's privacy practices, please refer to: <https://openai.com/privacy>

Infrastructure & Service Endpoints

Service	Endpoint
RAG API Service	https://rag.smartprocesses.cloud
Mind Spaces Service	https://spaces.smartmind.services
Subscription API	https://subscriptions.smartprocesses.cloud/api

All communications occur over HTTPS using secure authorization headers.

Legal Basis for Processing (Article 6 GDPR)

- Article 6(1)(f) – Legitimate Interest (security and service functionality)
- Article 6(1)(b) – Performance of a Service
- Consent, where applicable (e.g., cookies)

Data Retention

Chat logs and related technical data are retained only as long as necessary for system performance, quality improvement, and legal compliance.

Data Sharing & Third-Party Processors

We engage trusted infrastructure providers including cloud hosting, AI service providers, knowledge base infrastructure, and Stripe for subscription management. All processors operate under GDPR-compliant agreements.

Data Security

Security measures include encrypted HTTPS communication, token-based authentication, secure credential storage, access controls, and monitoring mechanisms.

AI-Generated Content Disclaimer

Responses are generated by automated AI systems based on indexed website content and approved knowledge sources. Responses may not always be complete or error-free and do not constitute professional advice.

Changes to This Privacy Policy

We may update this Privacy Policy to reflect legal, technical, or service-related changes. Updates will be published with a revised “Last Updated” date.

Contact

For questions regarding this Privacy Policy or data protection matters, please contact us through the official website contact channels.