Privacy Policy

How we protect your data.

Updated 5 Nov 2026

AT A GLANCE

You authorize the connection

A store administrator chooses whether to connect WooCommerce and can revoke access.

AI runs in the hosted service

Miyya sends product text and relevant conversation context to OpenAI for catalog search and shopping answers.

Your questions have a contact

Contact Niraltek for privacy enquiries, access requests or help with deletion.

01 Who this policy covers

Miyya is an AI shopping assistant operated by Niraltek Solutions Pvt. Ltd. This service notice covers the Miyya merchant portal, connected WooCommerce stores and conversations handled by the hosted assistant.

A merchant operates its own store and is responsible for its customer privacy notice, its authority to share store data, and responding to requests concerning its customers. Niraltek handles the account information needed to run Miyya and processes connected store information to deliver the service.

Visits to the Niraltek company website are covered separately by its website privacy policy. That website policy does not replace the service disclosures on this page.

02 Information the service processes

The information depends on the features you use.

- Account and connection details: store URL and name, connecting administrator email, account identifiers, and authorization information.
- Connection credentials: a read-only WooCommerce REST API key and the service credentials needed to maintain the authorized connection. Do not send these credentials in support messages or chat.
- Catalog information: product titles, descriptions, categories, attributes, variations, prices, stock status and image URLs.
- Catalog source records: complete WooCommerce product responses, including custom fields and plugin metadata, are retained for catalog processing. Selected custom-field text is used for search embeddings and AI answers. Keep secrets and unnecessary personal information out of product fields.
- Product reviews: after catalog imports, product updates and periodic background reconciliation, Miyya retrieves approved WooCommerce review responses. These responses can include reviewer names and email addresses, but product-review records store only review/product identifiers, text, rating, verified-purchase status and creation date. Review text can itself contain personal information. Selected excerpts and rating summaries can be used for AI answers.
- Store knowledge: published store pages and policies, coupons/offers, currency, shipping options and available payment method names used to answer store-policy questions. Payment gateway secret settings and shoppers' payment card details are not supplied as AI context.
- Conversation information: messages, conversation identifiers and relevant context used to answer follow-up questions.
- Shopping context: the current page or product and cart items, quantities and selected options. A WooCommerce cart token allows the service to read the current shopper cart when chat is used.
- Assistant feedback: chat ratings and comments when a user chooses to submit them, separately from imported product reviews. The plugin does not automatically report product-open or add-to-cart events for separate activity analytics.
- Order questions: the WordPress customer ID is sent to Miyya to issue a short-lived, store-bound customer token. When an order lookup is requested, the hosted service receives that customer's

WooCommerce order response, which can include billing, shipping, contact and payment-method details. It selects order-summary fields for the answer.

- Service administration: WordPress, WooCommerce and plugin versions, export capabilities, brand taxonomy, store timezone, operational records, service usage, billing and payment transaction records needed for the features you use. Requests expose IP addresses and usual HTTP metadata; portal sessions also record security information such as user agent.
- Service email: recipient email address and relevant account, store or billing details for invitations, sign-in and password-reset codes, store-link approval and billing notices. An initial invitation can include a temporary password; authentication messages can include a one-time code.

03 Why this information is used

Miyya uses connection and catalog information to link a store, synchronize products, build search embeddings and retrieve relevant product information. Conversation context supports answers, comparisons, recommendations and follow-up questions. Customer-scoped order access supports order-status answers.

Account, operational and usage information supports authentication, security, troubleshooting, support and service billing. A connection key is read-only: it does not authorize Miyya to edit your store products or orders.

04 AI processing and service providers

Miyya's hosted backend sends AI requests to OpenAI to turn product text into search embeddings and generate shopping answers. The WordPress site does not run these AI models and does not need its own AI provider key.

Keep chat free of information the assistant does not need. Do not send passwords, API secrets, payment card details or sensitive personal data in a conversation.

Miyya uses OpenAI for search embeddings and AI answers. Catalog indexing sends product text, including selected custom-field text; chat processing sends the query and relevant conversation, catalog, store and shopping context, including selected approved product-review excerpts and rating summaries needed to answer. Store connection secrets are not provided as AI prompts.

If a merchant opens a hosted-service checkout, Stripe processes billing contact information, store/order identifiers and payment-session details. Payment-card form entries go to Stripe. Miyya receives payment status, receipts/invoice information and limited payment-method metadata such as brand, last four digits and expiry to administer merchant purchases. The WordPress plugin does not collect payment-card form entries; customer order lookups can still return billing, shipping and payment-method information from WooCommerce.

Miyya uses Google's SMTP email service for account invitations, sign-in and password-reset codes, store-link approval messages and billing notices. Google receives the recipient address and the email body needed for that action, including a temporary invitation password or one-time code where applicable. These emails are sent by Miyya's server when those service actions occur; delivery metadata is logged.

Miyya also relies on infrastructure providers to operate the hosted service, each handling only what its function requires. Contact Niraltek for the current provider list and the regions where service data is processed; office locations on the Niraltek website do not establish where service data is hosted.

OpenAI service terms
OpenAI privacy policy
OpenAI API data controls
Stripe service terms
Stripe privacy policy
Google service terms
Google privacy policy

05 Connection, consent and disconnecting

A fresh plugin installation makes no Miyya service requests before an authorized administrator connects it. Selecting Allow & connect authorizes the disclosed connection and read-only API access. Catalog updates can then be delivered through WooCommerce webhooks, and the connected assistant checks service readiness and sends messages to the hosted service.

Previously authorized installations can recover a connection using saved store identity. Disconnecting revokes that recovery permission. You can also revoke the WooCommerce REST API key in WooCommerce settings.

Uninstall removes the plugin-stored site token, plugin settings and registered webhooks while retaining installation identity and the disconnect choice for secure recovery. The WooCommerce REST API key remains until you revoke it in WooCommerce. Disconnect stops local sharing immediately and requests hosted connection revocation and product/category cleanup. Retry Disconnect if remote cleanup fails. Other retained information, including encrypted WooCommerce credentials, store pages, conversations, sync history and account/billing records, is not deleted by this operation. Uninstalling alone makes no hosted cleanup request and does not clear visitors' browser storage.

06 Cookies and session information

The merchant portal uses a session cookie and authentication information to keep authorized access secure. The storefront stores a conversation identifier and conversation secret in localStorage, along with cart-command results; sessionStorage remembers widget state. These support conversation continuity and prevent repeated cart actions. Clearing local chat does not delete the hosted transcript.

The plugin does not automatically report product-open or add-to-cart events for separate activity analytics. Stripe can process its own session and fraud-prevention data when a merchant opens its payment flow.

Your store and the Niraltek company website may use their own cookies and third-party tools. Consult their respective notices for those activities.

07 Retention and deletion requests

Products and categories are removed when a remote disconnect completes. Other store information, credentials, conversation, account, usage, sync and billing records can remain until a separate deletion request is handled, subject to applicable recordkeeping needs. Removing a conversation from a browser or uninstalling the plugin does not erase all hosted records.

Operational logs include request paths, IP addresses, outcomes and timing. Diagnostic logging, when enabled by the service operator, can also record messages, context and answers. Backup and log retention depend on the service configuration. Contact Niraltek for the retention and deletion schedule that applies to a specific record type.

OpenAI may retain AI inputs and outputs under its API data controls and the controls configured for this service. Local chat deletion and disconnect do not themselves request immediate deletion of prior AI requests at OpenAI. The provider's API data-controls documentation is linked above; contact Niraltek for the service's current retention configuration.

For a Miyya account or connected-store request, email info@niraltek.com with your store URL and the nature of the request. Do not include API keys, passwords or full customer order details. Niraltek may need to verify your authority before acting.

If you are a shopper, contact the store first for questions about your order or store conversation. The merchant can identify the relevant store records and coordinate a request with Niraltek.

08 Security and international processing

Connections to the production Miyya service use HTTPS. Store connection credentials are delivered server to server rather than displayed in the connection screen. Customer identity for order questions is short-lived and scoped to the store.

Credentials are protected according to their role. Authentication password and bearer-token verifiers are hashed; replayable secrets such as WooCommerce consumer secrets are encrypted at rest and decrypted when needed. Connection identifiers and session credentials remain readable to the components that use them:

- Portal passwords used for authentication are stored as salted bcrypt hashes. Initial account invitations temporarily retain an encrypted, recoverable password so delivery can be retried. That password is sent by email, and its encrypted invitation copy is cleared after the email server accepts delivery. Password changes and resets store a new hash.
- Miyya stores the site token's SHA-256 verifier in its store record. The plugin stores the readable token in WordPress and sends it to Miyya over HTTPS to authenticate server requests.
- Portal sign-in session records store hashes of rotating refresh tokens. The browser receives the token in an HttpOnly cookie, which page scripts cannot read.
- Your WooCommerce consumer secret is encrypted at rest because the service must present it to your store. The consumer key is a stored connection identifier. Miyya's user interface masks these

credentials rather than returning them in full.

- Customer order lookups use a short-lived, store-bound signed token rather than storing shopper credentials.

09 Your choices and privacy requests

You can choose whether to connect a store, revoke connection credentials and decide whether to display the widget. Avoid including unnecessary personal data in product descriptions and conversations.

Depending on the law that applies, you may have rights to access, correct, obtain a copy of, or request deletion of personal information, or object to or restrict certain processing. Contact Niraltek to discuss a request; identity checks and lawful retention obligations may apply.

10 Contact and updates

For Miyya privacy enquiries, contact Niraltek Solutions at info@niraltek.com. For technical help, contact support@niraltek.com. Company contact details are available on the Niraltek website.

Updates to this policy will be published on this page with its last-updated date.