

Olvio — Privacy Policy

Last updated: 2026-04-24

1. Who we are

Olvio is an AI shopping agent for Shopify product pages. It is published and operated by:

Topicimes

3 Avenue René Laennec, 72000 Le Mans, France

SIRET: 90496525800018

President: Louis Jodon de Villeroché

Contact: help@olvio.ai

In this policy, "Olvio", "we", "us", and "our" refer to Topicimes acting as the publisher of the Olvio Shopify app.

2. Data Protection Officer

Topicimes has voluntarily appointed a Data Protection Officer responsible for overseeing compliance with this policy and with applicable data protection regulations:

Louis Jodon de Villeroché

Data Protection Officer, Topicimes

Email: help@olvio.ai

You can reach the Data Protection Officer at any time for questions about this policy, to exercise your rights, or to report a data protection concern.

3. Scope of this policy

This policy describes the data processed when the Olvio Shopify app is installed on a merchant's Shopify store, when shoppers interact with the Olvio widget on the merchant's storefront, and when visitors browse Olvio's public pages at olvio.ai.

Three categories of users are covered:

- **Merchants** — Shopify store owners or staff who install and configure Olvio.
- **Shoppers** — visitors of a merchant's storefront who may interact with the Olvio widget on a product page.
- **Website visitors** — visitors of olvio.ai (landing pages, help center).

Olvio does not require shoppers to create an account, log in, or share personal information. The widget does not ask for names, emails, phone numbers, or addresses, and the underlying AI is instructed never to request or store such information.

4. Our role (Controller and Processor)

Topicimes acts in two distinct roles under the GDPR, depending on the data category:

- **Data controller** — for merchant account data (Shopify identifiers, plan, configuration, encrypted credentials) and for operational logs strictly necessary to run the service.

- **Data processor (GDPR Article 28)** — for shopper interaction data processed on behalf of the merchant (conversations, widget events, question logs, order attribution). The merchant remains the data controller for this category and is responsible for informing shoppers and collecting any necessary consent on their storefront.

The Data Processing Agreement governing processor activities is included in our Terms of Service and contains every clause required by GDPR Article 28(3). A standalone Data Processing Addendum is available on request at help@olvio.ai.

5. Information we collect and store

Olvio only stores data that is strictly necessary to deliver the service. The sections below list every data category we persist in our own infrastructure.

5.1 Merchant data

When a merchant installs and configures Olvio, we store:

- **Shop identifiers** — the Shopify .myshopify.com domain, the storefront primary domain, and the Shopify-issued access token.
- **AI provider credentials** — the API key the merchant supplies for their chosen AI provider. Keys are encrypted with AES-GCM (256-bit) and cryptographically bound to the shop domain as additional authenticated data before being written to our database. They are never displayed back in full.
- **Widget configuration** — colors, typography, corner radii, custom CSS, label, title, avatar image, and translation overrides set by the merchant.
- **AI context** — the business description, product categories, and response guidelines entered by the merchant in the AI Setup page.
- **Billing state** — current plan, Shopify AppSubscription identifier, billing cadence (monthly / yearly), and trial status.
- **Session data** — Shopify authentication sessions issued during OAuth, used to call the Admin API on the merchant's behalf. Deleted automatically when the app is uninstalled.

5.2 Shopper interaction data

Shopper data is always stored under an anonymous, client-generated session identifier. We do not collect names, emails, phone numbers, or addresses.

- **Anonymous session ID** — a random identifier generated locally by the widget and stored in the shopper's browser under the key "olvio_sid". Used to correlate widget events and conversations within a shopping session.
- **Widget events** — impressions, opens, message sends, add-to-cart signals, per product and timestamp. Pre-engagement events are logged without any session identifier.
- **Conversations** — the sequence of messages exchanged between the shopper and Olvio on a product page, including optional feedback. No shopper-identifying fields are stored.
- **Question logs** — the text of each question sent by a shopper, associated with the product page and a timestamp. Used to power the merchant's analytics dashboard (recurring topics).
- **Order attribution** — when a Shopify order is placed after a chat session, we record the order identifier, the line-item product identifiers, the order total (in cents), and the

currency. We do not receive or store the buyer's name, email, phone, or shipping address. This data is obtained from Shopify's orders/create webhook and filtered at ingestion.

5.3 Catalog data

To answer shopper questions accurately, Olvio ingests the merchant's Shopify catalog content:

- **Products** — title, description (HTML and stripped text), vendor, product type, tags, status, price range, currency, images, SEO fields, variants, metafields, and collections.
- **Online store content** — public pages and blog articles from the merchant's storefront.
- **File-reference metafield content** — text extracted from documents attached via the "custom.olvio_knowledge_file" Shopify metafield (PDF, DOCX, XLSX).

Catalog data is ingested at first install, kept in sync in real time via Shopify webhooks (products/create, products/update, products/delete), and reconciled nightly.

5.4 Website visitor data (olvio.ai)

Visitors of olvio.ai may be subject to analytics cookies and similar technologies, disclosed through a cookie consent banner displayed on first visit. Only cookies that are strictly necessary to operate the website are set before consent is given. All other cookies (analytics, marketing) are loaded only after the visitor explicitly accepts them.

5.5 Sources of data

We collect data from the following sources, in accordance with GDPR Article 14:

- Directly from the merchant — when installing Olvio, entering API keys, and configuring the widget.
- From Shopify — via OAuth, Admin API, and webhooks, with the merchant's authorization granted at install.
- Directly from shoppers — via the widget on the merchant's storefront, under an anonymous session identifier.

6. Special category data

Olvio does not collect, store, or process special categories of personal data as defined in GDPR Article 9 (health, biometric, genetic, political opinions, religious beliefs, racial or ethnic origin, sexual orientation, trade-union membership).

The AI system prompt explicitly forbids shoppers from sharing such information and instructs the AI not to repeat it if it is shared inadvertently. Conversations are stored as-is; we recommend merchants inform their shoppers not to share sensitive personal information in the widget.

7. How we use this data

- Deliver the core app functionality — rendering the chat widget on product pages, answering shopper questions, and recommending products.
- Operate the merchant admin — displaying catalog sync status, conversation history, insights, and billing state.

- Sync with Shopify — reacting to product create/update/delete, app subscription updates, and order creation events in real time.
- Improve the service — aggregating anonymous usage signals to surface recurring topics and catalog blind spots to the merchant.
- Comply with legal obligations — enforcing Shopify's GDPR compliance webhooks and our contractual obligations as a data processor.

We do not sell personal data. We do not use shopper data or conversation content to train AI models.

8. AI providers (merchant's choice)

Olvio uses a bring-your-own-key model. Each merchant selects an AI provider (currently Anthropic Claude, OpenAI ChatGPT, or Google Gemini) and supplies their own API key for that provider.

When a shopper sends a message through the widget, the merchant's prompt and conversation context are routed from our Worker to the merchant's chosen AI provider using the merchant's own API key. We do not proxy, re-use, aggregate, or train on this content. We do not hold a commercial or contractual relationship with the AI provider on the merchant's behalf — the merchant has their own agreement directly with the provider they selected.

The processing, retention, and international transfer of the prompt and response by the AI provider are governed by that provider's own terms and privacy policy. Before entering an API key, merchants are responsible for reviewing the selected provider's data practices.

Olvio stores the conversation record (messages and timestamps) in our own database as described in Section 5.2, under the retention rules of Section 11. Olvio does not store the raw API request or response payloads beyond this conversation record.

9. EU AI Act (Regulation 2024/1689)

Olvio is an artificial intelligence system within the meaning of Article 3 of the EU AI Act. Topicimes and the merchant have complementary responsibilities under the Act:

- **Topicimes (provider)** — responsible for the technical compliance of the AI system, its documentation, and its availability as a safe and conforming tool. This includes maintaining technical documentation, applying risk management, ensuring human oversight mechanisms, and cooperating with supervisory authorities as required.
- **Merchant (deployer)** — responsible for how the system is used on their storefront, for defining the purposes of use, and for ensuring that deployment complies with applicable regulations and with their own terms of service.

Olvio qualifies as a limited-risk AI system under the Act. In accordance with the transparency obligations of Article 50, every shopper interaction with the widget displays the disclaimer “Olvio is an AI and can make mistakes” so that shoppers are always informed they are communicating with an AI, not a human. This disclaimer is locked and cannot be removed by merchants through widget customization.

10. Automated decision-making and profiling

Olvio uses AI to generate contextual product recommendations and answers. These responses are informational and do not constitute automated decision-making with legal effects or similarly significant effects on shoppers within the meaning of GDPR Article 22.

Shoppers always remain free to add to cart, continue browsing, leave, or ignore any recommendation.

Olvio does not build individual profiles of shoppers across sessions or stores. Conversations are stored per session only for the retention window applicable to the merchant's plan (Section 11).

11. Data retention

Retention applies to conversation-related data (conversations, question logs, widget events, order attributions) and depends on the merchant's plan. Retention periods are enforced by automated deletion and reflect the data minimization principle of GDPR Article 5(1)(e):

Plan	Conversation data retention
Starter	30 days from the event timestamp.
Growth	90 days from the event timestamp.
Scale	365 days from the event timestamp.
Custom	Negotiated per contract (defaults to no automatic purge).

A daily scheduled task enforces these periods by deleting records older than the applicable cutoff. Catalog data (products, sync state) is retained for the duration of the app installation.

When a merchant uninstalls Olvio, Shopify delivers a "shop/redact" webhook approximately 48 hours later. Upon receipt, we permanently delete all data associated with that shop across our database and vector index: conversations, question logs, widget events, order attributions, knowledge files, products, embeddings, and the shop record itself.

12. Sub-processors

Topicimes engages the following sub-processors to deliver the Olvio service. All are bound by data processing agreements providing GDPR-equivalent protections, including the European Commission's Standard Contractual Clauses of 4 June 2021 where required.

Provider	Purpose	Location of primary data storage
Cloudflare, Inc.	Application hosting (Workers), database (D1), vector index (Vectorize), edge caching (KV), rate limiting, and embeddings (Workers AI).	European Union (WEUR region, Western Europe). Edge compute may execute on the closest Cloudflare data center to the requester.
Intercom R&D Unlimited Company	In-app support messenger embedded in the Olvio merchant admin.	Ireland (European Union).

Shopify Inc. is the app distribution platform on which Olvio runs. The merchant has a direct agreement with Shopify for their store and grants Olvio authorized access via OAuth. Shopify is not a sub-processor of Topicimes in the meaning of GDPR Article 28.

AI providers selected by the merchant (Anthropic, OpenAI, Google) are not sub-processors of Topicimes. They are the merchant's own sub-processors under the merchant's direct agreement with the provider. See Section 8 for details.

13. Data security

- **Encryption in transit** — all traffic to and from the Olvio Worker uses HTTPS/TLS.
- **Encryption at rest (secrets)** — AI provider API keys are encrypted with AES-GCM 256-bit before being written to the database, with the shop domain bound as additional authenticated data so ciphertexts cannot be transplanted between shops.
- **Multi-tenant isolation** — every database query that touches shop-scoped data is constrained by the shop identifier. Isolation is enforced at query level on every read, update, and delete operation.
- **Rate limiting and origin checks** — storefront widget requests are validated against the shop's declared domain. Per-shop rate limits protect against abuse.
- **Webhook authentication** — every Shopify webhook is HMAC-verified before any data is written.
- **Principle of least privilege** — Olvio requests only the read_products, read_orders, and read_themes OAuth scopes from Shopify.

14. Security incidents and breach notification

If a personal data breach occurs, Topicimes will notify the affected merchants without undue delay and, where feasible, no later than 72 hours after becoming aware of it, in line with GDPR Article 33. The notification will describe the nature of the breach, the categories and approximate number of records affected, the likely consequences, and the measures taken or proposed to address the incident.

Where a breach is likely to result in a high risk to shoppers, Topicimes will assist merchants in notifying affected individuals, as required by GDPR Article 34.

To report a suspected breach, contact the Data Protection Officer at help@olvio.ai.

15. Cookies and browser storage

Olvio uses browser storage in a targeted, transparent way:

- **Merchant admin and shopper widget** — no HTTP cookies are set. The widget uses localStorage to persist a random anonymous session identifier (key: olvio_sid) and sessionStorage to cache transient chat state and product suggestions for the current session. Neither is used for cross-site tracking, and no third-party analytics or advertising scripts are injected on merchant storefronts.
- **olvio.ai public pages** — a cookie consent banner is displayed to visitors on first arrival. Only cookies that are strictly necessary to operate the website are set before consent. Analytics and marketing cookies are loaded only after the visitor explicitly accepts them through the banner. Consent can be withdrawn at any time.

16. International data transfers

Primary data storage (Cloudflare D1, Vectorize, KV) is configured to reside in the Western Europe region. Support interactions via Intercom are stored in the European Union.

Cloudflare's edge compute may process requests from the data center closest to the requester; such transit processing does not result in persistent storage outside the primary region.

Transfers of personal data outside the European Economic Area, when they occur, rely on the Standard Contractual Clauses approved by the European Commission on 4 June 2021,

supplemented by technical measures (encryption in transit and at rest for secrets) and contractual commitments from each sub-processor.

Transfers to AI providers selected by the merchant are not governed by this policy and are the responsibility of the merchant and the provider they chose (see Section 8).

17. Your rights under GDPR

If you are located in the European Economic Area, the United Kingdom, or Switzerland, you have the following rights regarding your personal data:

- Right of access to the data we hold about you.
- Right to rectification of inaccurate or incomplete data.
- Right to erasure (the "right to be forgotten") in the cases provided by law.
- Right to restriction of processing.
- Right to data portability.
- Right to object to processing based on legitimate interest.
- Right not to be subject to a decision based solely on automated processing (see Section 10).
- Right to lodge a complaint with a supervisory authority. In France, the authority is the Commission Nationale de l'Informatique et des Libertés (CNIL, [cnil.fr](https://www.cnil.fr)).

Shoppers: because we do not store identifying information about shoppers, requests for access, deletion, or correction typically cannot be fulfilled on a per-person basis. Shoppers can clear all widget data from their device by clearing their browser's localStorage and sessionStorage for the merchant's domain.

Merchants: you can exercise your rights by uninstalling Olvio (which triggers automatic deletion via Shopify's shop/redact webhook approximately 48 hours later) or by contacting the Data Protection Officer at help@olvio.ai. We respond to requests within one month of receipt, extendable once by a further two months for complex requests with notice to you.

18. Children's privacy

Olvio is a B2B product intended for Shopify merchants and their shoppers. It is not directed to children under 16, and we do not knowingly collect personal data from children. If a merchant operates a storefront that targets children, it is the merchant's responsibility to comply with applicable legislation.

19. Changes to this policy

We may update this policy from time to time. The "Last updated" date at the top of this document reflects the most recent revision. For material changes affecting merchant data, we will notify active merchants through the Olvio admin interface before the change takes effect.

20. Contact

For any question regarding this policy or your personal data:

Louis Jodon de Villeroché

Data Protection Officer, Topicimes

3 Avenue René Laennec, 72000 Le Mans, France

Email: help@olvio.ai

We aim to respond to every data subject request within one month of receipt, as required by GDPR.