How Rosetta handles personal data under the GDPR and the CCPA

For merchants evaluating the **Rosetta: AI Upsell Suite** Shopify app. This overview summarises how the app processes your shoppers' personal data, the commitments we make to you as your processor and service provider, and the security measures behind them. The binding terms are in our Privacy Policy and Data Processing Addendum, both available to you on request.

Your processor and service provider
For shopper data, you decide; we act only on your instructions, under a GDPR Article 28 and CCPA service-provider addendum.

Hosted in Singapore
Databases, application servers and backups all sit in one region. No other component holds personal data elsewhere.

Encrypted, access-controlled
Encryption in transit and at rest, including backups. Multi-factor authentication and named accounts for all production access.

Never sold, never shared for ads
We do not sell personal information or share it for cross-context behavioural advertising.

Breach notice within 72 hours
We notify you without undue delay, and in any case within 72 hours of becoming aware of a breach affecting your data.

Deletion built in
Shopify's mandatory privacy webhooks handled; data erased from live systems on uninstall; backups rotate out within 30 days.

1. Who is responsible for what

Shopper data — you are in control

Everything the app observes on your storefront is processed on your behalf. Under the **GDPR** you are the controller and we are your **processor**; under the **CCPA** you are the business and we are your **service provider**. You decide why the data is collected and how long it is used; we act on your documented instructions — our terms and your configuration of the app.

Your account data — we are responsible

For the account, billing-status and support information you give us, we act as controller (GDPR) and business (CCPA), under our Privacy Policy. Payment details stay with **Shopify Billing**; we receive only subscription status and amounts.

2. GDPR — our processor commitments

Our Data Processing Addendum sets out the terms Article 28 requires. In summary, we will:

- process personal data only on your documented instructions, and tell you if the law requires otherwise;

- keep everyone authorised to process it under confidentiality obligations;
- apply the technical and organisational measures in section 5;
- engage subprocessors only from the published list, with **30 days' notice** of any change in the app and by email, and a right for you to object and, if we cannot resolve it, to terminate the affected service;
- help you answer data subject requests, carry out impact assessments and meet your own breach-notification duties;
- notify you of a personal data breach **within 72 hours** of becoming aware of it;
- delete the data at the end of the service (section 7);
- answer reasonable questions about our processing and allow an audit once a year on 30 days' notice.

International transfers. Where personal data leaves the UK or EEA for a country without an adequacy decision, the transfer is governed by the European Commission's **Standard Contractual Clauses (Module Two, controller to processor)** and, for UK data, the **UK International Data Transfer Addendum**, both incorporated into the DPA. As a Singapore company we also apply the PDPA's transfer limitation obligation.

Data subject rights. The app implements Shopify's mandatory privacy webhooks — `customers/data_request`, `customers/redact` and `shop/redact` — so access and erasure requests resolve through your Shopify admin. If a shopper contacts us directly, we refer them to you and let you know.

3. CCPA — our service-provider commitments

For personal information of California residents, our DPA contains the terms the CCPA requires of a service provider. We will:

- **not sell or share** the personal information;
- use it only for the business purposes in the DPA — providing, personalising and measuring the storefront tools — and not outside our direct business relationship with you;
- not combine it with personal information from other sources, except as the CCPA regulations permit a service provider;
- provide the same level of privacy protection the CCPA requires of you, and tell you promptly if we can no longer meet our obligations;
- let you take reasonable steps to check our use, and to stop and remediate any use you have not authorised;
- help you respond to requests to know, delete and correct;
- bind each of our own service providers to restrictions no less protective;
- keep any aggregated statistics deidentified and never attempt to reidentify them.

We collect no **sensitive personal information** as the CCPA defines it: no government identifiers, passwords, financial account or card numbers, or precise geolocation. Sign-in runs through Shopify, and card details never reach us.

4. What the app processes

CATEGORY	WHAT IT INCLUDES	WHY
Catalog and merchandising	Products, variants, prices, inventory, collections, discounts	Choosing what to show
Orders	Order contents and history	Attributing revenue to each tool; improving recommendations
Customer records	Shopify customer ID and, where your store exposes them, name, email, phone and address	Recognising a returning shopper
Storefront behaviour	Pages and products viewed, searches, cart changes, widget interactions — through our theme app embed and a Shopify web pixel	Personalising the storefront
Device and connection	Browser and device type; IP address, from which we derive approximate (country or region) location only	Localising currency, language and shipping messages
Browser identifiers	A returning-shopper identifier and an experiment bucket	Recognition and A/B testing

No special category data is requested or used, and the app may not be configured to collect it.

AI shop assistant

The assistant sends the shopper's message, relevant catalog context and pseudonymous session signals to a large-language-model provider — **Anthropic** by default, **OpenAI** as an alternative. **No name, email address, phone number, delivery address, order history or customer record is sent.** Both accounts are on commercial API terms, under which submitted content is not used to train models, and **zero data retention** is enabled. Recommendations, nudges and bundles run on our own models and infrastructure.

Personalisation across stores — off unless you turn it on

Each merchant decides in the dashboard whether its shoppers' preferences may inform other participating Rosetta stores. It is **off by default**. Where enabled, only a pseudonymous identifier and preferences travel — never name, email, phone or address — and **no merchant ever sees another merchant's data**. Switching it off removes that store's contribution from the pool.

5. Security measures

- Encryption of personal data in transit (TLS) and at rest, including backups.
- Authentication to the app through Shopify OAuth; multi-factor authentication and named individual accounts for all production access — no shared logins.
- Access limited to personnel who need it for their role; each store's data segregated by store identifier.
- Backups taken regularly, with a restore tested **monthly**.
- Dependency patching and vulnerability scanning on a regular cycle.
- Security and data-protection training for staff.
- Logging and error monitoring; change management through version control and peer review.

Certification. We are working toward **SOC 2** and **ISO 27001**. We do not hold either today, and further detail of our controls is available under a confidentiality agreement.

6. Subprocessors

SUBPROCESSOR	PURPOSE	LOCATION
Shopify	Source platform; store hosting, checkout and billing	Per Shopify's terms
Anthropic	Large language model for the shop assistant	Per provider terms (may include the US)
OpenAI	Alternative large language model	Per provider terms (may include the US)
DigitalOcean	Cloud hosting and object storage	Singapore
Mailgun	Transactional email to merchants	Per provider terms
Sentry	Application error monitoring	Per provider terms
ipapi	IP-to-approximate-location lookup	Per provider terms

This list is complete: no other analytics, support, logging or monitoring tool has access to personal data.

7. Retention and deletion

- Shopper and storefront data is kept only while the app is installed.
- On uninstall, on a `customers/redact` request, or on termination, it is erased from live systems immediately.
- Backup images are kept for no more than **30 days**, used only for disaster recovery, then destroyed on rotation. If a backup is ever restored, every erasure made since it was taken is re-applied straight away.

8. Contact

Rosetta.AI Holding Pte. Ltd. (UEN 202012131D), 114 Lavender Street, #11-83, CT Hub 2, Singapore 338729.
Privacy questions, data requests and our Data Protection Officer (appointed under Singapore's PDPA): **hey@rosetta.ai**

This overview summarises our practices and commitments for information purposes. The binding terms are those in the Rosetta Privacy Policy and Data Processing Addendum, which prevail over this summary.