VyReel Privacy Policy

Effective from June 16, 2026 to present

OPTIVOX (PRIVATE) LIMITED · vy-reel.com/privacy-policy

This Privacy Policy explains how **VyReel** ("we", "us", or "our") collects, uses, shares, and protects personal data in connection with the VyReel marketing website at **vy-reel.com** and the **VyReel Shopify application** (the "App"). It is published at **https://vy-reel.com/privacy-policy**.

1. Introduction & scope

VyReel is an embedded Shopify app that lets a Shopify merchant add shoppable short-form video ("reels") to their storefront. Merchants can upload videos or import their own social videos, attach products, and publish reels to their store; the App also measures storefront engagement and attributes resulting sales.

This is the **privacy policy for the VyReel app** — it explains how we (OPTIVOX (PRIVATE) LIMITED) handle data for the merchants who install VyReel and for their storefront visitors, whose data we process on each merchant's behalf (see Section 2).

This policy covers:

- Personal data of **merchants** (our direct customers — the Shopify store owners and their staff who install and use the App).
- Personal data of the merchant's **storefront visitors and customers** that we process on the merchant's behalf to deliver the App's functionality.
- Content a merchant imports from **their own Instagram or TikTok** accounts, and any personal data incidentally embedded in that content.

2. Our role: controller vs. processor

VyReel acts in two distinct roles, and your rights and our obligations differ depending on which applies.

- **As a controller — merchant account, store, and billing data.** When we collect and use data about the merchant, their store, their app configuration, their billing and usage, and their support requests, VyReel is an **independent data controller**. We determine the purposes and means of that processing.

- **As a processor / service provider — storefront-visitor and customer data.** When we process personal data relating to a merchant's storefront visitors or customers — for example, engagement events generated when shoppers view reels, or order-attribution data read from the merchant's Shopify store — VyReel acts as a **processor (service provider)** on the **merchant's documented instructions**. The **merchant is the controller** of that data. This processing is governed by our merchant terms and Data Processing Addendum ("DPA"). Storefront visitors who wish to exercise data-subject rights over this data should refer to the **merchant's own privacy policy** and direct their requests to the merchant; we will assist the merchant as described in Section 9.

We do **not** use storefront-visitor or customer data for our own independent purposes, and we do **not** combine or profile data across different merchants' stores (see Section 5).

---

3. Definitions

- **Personal data / personal information** — information that identifies or relates to an identifiable individual.
- **Controller** — the party that determines the purposes and means of processing personal data.
- **Processor / service provider** — a party that processes personal data on behalf of, and under the instructions of, a controller.
- **Sub-processor** — a third party engaged by a processor to help deliver the service, which itself processes personal data.
- **Data subject / consumer** — an individual to whom personal data relates (e.g., a merchant user or a storefront visitor).
- **Merchant** — a Shopify store owner (and their authorized staff) who installs and uses the App.
- **Storefront visitor** — a person who visits a merchant's online store where VyReel reels are displayed.
- **Processing** — any operation performed on personal data (collection, storage, use, disclosure, deletion, etc.).
- **Sale / share** — as defined under U.S. state privacy laws (CCPA/CPRA), including disclosures for cross-context behavioral advertising.
- **GPC** — Global Privacy Control, a browser signal communicating an opt-out preference.

4. Personal data we collect

We collect only the data described below. We do **not** read customer names, email addresses, phone numbers, or postal/shipping addresses from a merchant's orders, and we do **not** set cookies, use `localStorage`, or fingerprint storefront visitors beyond the limited signals described in Section 4.3.

4.1 As controller — merchant and store data

Data	Source	Notes
Shopify store ("shop") domain	Shopify OAuth	Identifies the installing store.
Shopify Admin API access token (offline) and granted scopes, plus refresh token	Shopify OAuth	Used to make Admin API calls on the merchant's behalf.
Merchant user identity: user ID, first name, last name, email, account-owner / collaborator flags, email-verified flag, locale	Shopify session (when Shopify provides it)	Stored in our session and shop records.
Billing, subscription, plan, applied-charge, and usage-counter / quota data	Shopify Billing + App usage	Used to operate plans, caps, and billing.
Support correspondence	Directly from the merchant	When a merchant contacts us.
Marketing-site data (e.g., contact-form submissions; limited, consent-based site analytics/cookies)	vy-reel.com visitors	See Section 8.

4.2 As processor — order-attribution data (Protected Customer Data)

To attribute storefront sales to reels, the App reads a **minimized** set of order data from the merchant's store via the Shopify Admin API (`read_orders`), and via the `orders/create` webhook:

- Order ID; order line-item product ID, quantity, and discounted line-item amount; and store-wide order counts.
- Cart line-item attribution properties that the App itself sets (an attributed reel/collection reference).

We do **not** request, read, or store any customer identifier from orders — **no** customer name, email, phone, or address. This order data is **Protected Customer Data** under Shopify's program; we handle it in accordance with Section 11 (Security) and the minimization, purpose-limitation, and retention commitments throughout this policy.

4.3 As processor — storefront engagement data (VideoEvent)

When a storefront visitor interacts with a reel, the App records engagement events on the merchant's behalf. For each event we collect:

- The event type (impression, play, complete, product click, add-to-cart, purchase), the reel/video ID, and (where relevant) a product reference.
- An **anonymous session identifier** — a random UUID generated in the browser's `sessionStorage` and cleared when the browser session ends. It is not a cookie and is not tied to a persistent profile.
- A **hashed (SHA-256) IP address**. We do **not** store the raw IP address.
- The visitor's **User-Agent** string (truncated) and **Referrer** URL (truncated).
- A server-side timestamp.

These signals are used for engagement counts, storefront play-count badges, usage metering, security, and rate-limiting. The hashed IP and session ID are also used transiently for abuse-prevention / rate-limiting.

4.4 Imported social content (merchant's own Instagram / TikTok)

When a merchant chooses to import content, they provide their **own** social handle or a public post link. On the merchant's instruction, the App fetches **publicly available** content for that handle/post via third-party services (see Section 7): the video file URL, thumbnail/cover and animated preview, the caption/title (truncated), duration, and the remote post ID/URL.

- We do **not** ask for, receive, or use the merchant's (or anyone's) Instagram/TikTok login credentials, and we do **not** access private or non-public social data.
- The App requires the merchant to confirm they only import content they **own or have the rights to use**. We import only the merchant's own, authorized accounts/content — we do **not** perform arbitrary or unauthorized scraping of third-party stores or websites.
- Any personal data incidentally embedded in imported content (for example, a caption) is processed only to display the merchant's reel on their storefront.

Uploaded merchant brand assets (e.g., custom font files) are stored in the merchant's Shopify Files.

---

5. How we use data (purposes of processing)

We use personal data for the following purposes:

- **Operate and provide the App** — authenticate the merchant via Shopify OAuth, render reels on the storefront, manage reels/collections/products, and provide core functionality.
- **Import and process media** — fetch the merchant's own social content, transcode it, and publish playable renditions to the merchant's store.
- **Engagement analytics (on the merchant's behalf)** — produce view/play/click/add-to-cart counts and storefront play-count badges.
- **Sales attribution (on the merchant's behalf)** — attribute orders to reels and compare tagged vs. untagged sales.
- **Billing, plans, and usage metering** — meter usage, enforce plan caps, and administer subscriptions and charges via Shopify Billing.
- **Security, abuse prevention, and debugging** — rate-limiting, fraud/abuse prevention, integrity, and troubleshooting.
- **Support** — respond to and resolve merchant requests.
- **Product analytics and marketing for the marketing site** — limited, consent-based analytics and merchant-directed communications relating to vy-reel.com.

We use processor-side data (Sections 4.2–4.3) **only** to provide the service to the merchant on whose behalf it was collected. Specifically, we do **not**:

- use storefront-visitor or customer data for our own marketing, advertising, or profiling;
- sell or share personal data, or use it for cross-context behavioral advertising;
- combine or profile data across different merchants ("no cross-merchant data use"); or
- use merchant or storefront-visitor data to train machine-learning or AI models.

---

6. Legal bases for processing (GDPR / UK GDPR)

Where the GDPR or UK GDPR applies and VyReel is the **controller** (merchant data), we rely on:

- **Performance of a contract** — to provide the App to the merchant, authenticate access, operate features, and administer billing.
- **Legitimate interests** — to secure the service, prevent fraud and abuse, debug, and perform product analytics and service improvement; we balance these interests against your rights and interests.
- **Consent** — for marketing emails and non-essential marketing-site cookies/analytics; you may withdraw consent at any time.
- **Legal obligation** — to meet tax, accounting, and lawful-request obligations.

For **processor-side** data (storefront-visitor and order-attribution data), the **merchant** is the controller and is responsible for establishing the legal basis and any required consents for that processing. We act on the merchant's instructions.

---

7. How we share data — disclosures & sub-processors

We do **not sell personal data**, and we do **not share personal data for cross-context behavioral advertising.** We disclose personal data only as described below.

7.1 Sub-processors

We use the following sub-processors to operate the App. Each receives only the data needed for its function and is bound by contract to confidentiality and data-protection obligations consistent with this policy and our DPA.

Sub-processor	Function	Data it receives
Shopify	App platform: Admin API, Files, metaobjects, App Proxy, Billing	Store/merchant identity, app content and media, minimized order-attribution data, billing data.
Google Cloud	Compute (Cloud Run app + media-processing worker), object storage (Cloud Storage), and task queue (Cloud Tasks)	Uploaded/imported source videos; processing job metadata (IDs/URLs only). Stored in the **Mumbai, India** region.
Neon	Managed PostgreSQL database	Merchant/store records, sessions, reel/collection data, engagement events (incl. hashed IP, User-Agent, Referrer), and billing records. Hosted in the **Singapore** region.
Upstash	Managed Redis — rate-limiting (always) and, where enabled, a transient event buffer and play-counter	Hashed IP, anonymous session ID, and (when buffering is enabled) User-Agent and Referrer, held transiently.
ScrapeCreators	Primary service used to fetch public social content from the merchant's own provided handle/link	The merchant-provided handle/post URL; returns public post media and metadata.
Apify	Fallback service used to fetch public social content when the primary service is unavailable	The merchant-provided handle/post URL; returns public post media and metadata.

We may update this list as our service evolves. For **processor-side data**, we will provide merchants with reasonable advance notice of new sub-processors as set out in the DPA, so that they may object where applicable. Merchants can request the current sub-processor list and DPA at support@vy-reel.com.

7.2 Other disclosures

- **Legal and safety** — where required by law, legal process, or a lawful request, or to protect the rights, safety, and security of VyReel, our merchants, or others.
- **Corporate transactions** — in connection with a merger, acquisition, financing, or sale of assets, subject to this policy continuing to govern the personal data.

We do not use any advertising-network, fingerprinting, or third-party web-analytics SDKs in the storefront integration (no Google Analytics or similar in the reel tracking).

---

8. Cookies & tracking

- **Marketing site (vy-reel.com).** We use limited, consent-based cookies/analytics on our marketing site, with a consent mechanism where required (e.g., an EU cookie banner). We honor the **Global Privacy Control (GPC)** signal as an opt-out for the marketing site.
- **Storefront integration.** The App's storefront engagement tracking does **not** use cookies or `localStorage`. It uses an anonymous, per-session identifier stored in the browser's `sessionStorage` (cleared at the end of the browser session). This storefront tracking runs under the **merchant's controllership**; the merchant determines consent requirements for their store. We honor the merchant's instructions in our processor capacity.

---

9. Your rights

9.1 Merchants and individuals whose data we control

Depending on your location, you may have the following rights regarding the data for which VyReel is the controller:

- **GDPR / UK GDPR** — access, rectification, erasure, restriction, portability, objection, and withdrawal of consent, and the right to lodge a complaint with a supervisory authority.
- **CCPA / CPRA and similar U.S. state laws** — to know/access, delete, and correct personal information; to opt out of "sale"/"share"; to limit the use of sensitive personal information; the right to **non-discrimination** for exercising your rights; and the right to **appeal** a denied request.

We honor the **GPC** signal as a valid opt-out of "sale"/"share" where applicable. Because we do not sell or share personal data, there is no such activity to opt out of, but we will honor any opt-out preference.

To exercise these rights, contact us at **support@vy-reel.com**. We will verify your request as required by law, may act through an authorized agent where permitted, and will respond within the timeframes required by applicable law (generally within **30 days** under the GDPR/UK GDPR and **45 days** under the CCPA/CPRA, subject to permitted extensions).

9.2 Storefront visitors and customers (data we process for a merchant)

For personal data we process **as a processor on a merchant's behalf** (engagement and order-attribution data), the **merchant is the controller**. If you are a storefront visitor or customer, please direct access, correction, or deletion requests to the **merchant** (the store), in accordance with the **merchant's own privacy policy**. When a merchant forwards us such a request, we will assist the merchant and act on their instructions as their processor.

In particular, we support the Shopify mandatory compliance webhooks that implement these rights:

- `customers/data_request` — when a customer asks a merchant for their data, Shopify notifies the App. Because the App stores **no customer PII**, there is no customer profile to return; we acknowledge the request and log it. The merchant remains responsible for responding to the customer.
- `customers/redact` — when a customer's data is to be deleted, Shopify notifies the App. As the App holds **no customer PII** keyed to that customer, there is nothing to erase from a customer profile; we acknowledge and log the request.
- `shop/redact` — sent after a merchant uninstalls; we erase the relevant store data as described in Section 12.

We verify the authenticity of these webhooks (HMAC validation; invalid requests are rejected), acknowledge them with a success (2xx) response, and, where a request requires us to delete data, complete that deletion **within 30 days**, except where we are legally required to retain certain data.

Note on compliance logs: to maintain an audit trail of these requests, the App records the Shopify-provided webhook payload (which may contain customer identifiers that Shopify includes, such as a customer ID or email) in an append-only internal audit log. This log is retained as a security/compliance record.

---

10. International data transfers

VyReel operates a globally distributed infrastructure. Personal data is stored and processed primarily in **India** (Google Cloud, Mumbai region — media storage and compute) and **Singapore** (Neon

PostgreSQL), in addition to the regions used by Shopify and our other sub-processors.

Where personal data is transferred out of the European Economic Area, the United Kingdom, or Switzerland, we rely on appropriate safeguards, including the **EU Standard Contractual Clauses (SCCs)** and, for UK transfers, the **UK International Data Transfer Agreement / Addendum**, together with supplementary measures where appropriate. For processor-side transfers, our merchant DPA incorporates the SCCs. We will provide details of the relevant transfer mechanism on request at support@vy-reel.com.

---

11. Data security

We maintain technical and organizational measures designed to protect personal data, including measures aligned with Shopify's Protected Customer Data requirements:

- **Encryption in transit** — all data exchanged between clients, the App, and our backend is encrypted using TLS.
- **Encryption at rest** — data stored in our database, object storage, and backups is encrypted at rest.
- **Data minimization** — we collect and process only the minimum personal data needed to provide the App's functionality (for example, we read no customer identifiers from orders, and we store only a hashed IP rather than a raw IP).
- **Access controls / least privilege** — staff access to personal data, and in particular to Protected Customer Data, is restricted on a need-to-know basis; database roles are scoped to least privilege (for example, engagement and billing records are insert-only at the database-role level).
- **Separation of environments** — test and production data are kept separate.
- **Token handling** — Shopify access tokens are stored securely and used only to operate the App on the merchant's behalf.
- **Logging, monitoring, and access logs** — we maintain access logging for systems that process Protected Customer Data and monitor for anomalies.
- **Data-loss-prevention and incident response** — we maintain data-loss-prevention measures and a security incident-response process, and require strong authentication for staff accounts.
- **Breach notification** — in the event of a personal-data breach, we will notify Shopify, affected merchants/controllers, and supervisory authorities as and where required by applicable law and our agreements.

No method of transmission or storage is completely secure, and we cannot guarantee absolute security.

---

12. Data retention

We retain personal data only for as long as necessary for the purposes described in this policy, or as required by law. Retention is tied to the App lifecycle:

- **Active use.** While the App is installed, we retain merchant, store, reel/collection, engagement, attribution, and billing data to provide the service.
- **On uninstall (`app/uninstalled`).** When a merchant uninstalls the App, we delete the merchant's **session record** immediately and stamp the store record as uninstalled. We then enqueue cleanup of the merchant's **source video files in object storage (Google Cloud Storage)**.
- **On `shop/redact`** (sent by Shopify ~48 hours after uninstall). We erase the store's data within 30 days: we delete the **merchant's session** (its Shopify access token and the merchant's name, email, and user ID), the store's **database records** — reels, engagement/`VideoEvent` events (including the order-attribution events) and collections — and we scrub the shop's **source video files in object storage**. We retain only **billing, financial, and compliance records** — the billing and one-time-charge (top-up) ledger, the minimal store-billing identity, and our append-only audit log — where permitted by law. The storefront-side assets that were published to the merchant's own Shopify store (metaobjects and Shopify Files) cannot be removed by us after uninstall, because we no longer hold an access token to the store; a merchant who wants those removed too should run the in-app full-purge **before** uninstalling.
- **In-app full purge.** While the App is installed, a merchant can trigger a full purge from within the App. This is the most complete path: it deletes the store's database records (reels, engagement/`VideoEvent` records, and collections), **also** removes the storefront-side metaobjects and Shopify Files (which the post-uninstall `shop/redact` cleanup cannot reach), and scrubs the object-storage sources. Merchants may also contact us at support@vy-reel.com to request deletion.
- **Customer-rights webhooks.** As described in Section 9.2, `customers/data_request` and `customers/redact` are honored within 30 days; because we store no customer PII keyed to individual customers, these generally result in acknowledgment and logging.
- **Billing, usage, and audit records.** Aggregated usage/metering counters (not the granular per-event engagement records — those are deleted on `shop/redact`), billing-period and one-time-charge records, and audit logs are maintained as append-only billing/compliance records and may be retained for the period required for billing, accounting, tax, and legal purposes.

- **Transient data.** Rate-limiting and event-buffer entries held in Redis are short-lived and expire automatically.

Where we are legally required to retain certain data, we will retain it for the minimum required period and then delete or anonymize it.

---

13. Children's data

The App and the marketing site are not directed to children, and VyReel does not knowingly collect personal data from children (under 16 under the GDPR, or under 13 under U.S. COPPA-style frameworks). Whether a storefront's audience includes children is determined by the merchant as controller of their store. If we become aware that we have inadvertently collected personal data from a child, we will delete it.

---

14. Automated decision-making & profiling

VyReel does **not** carry out automated decision-making that produces legal or similarly significant effects on individuals (GDPR Article 22 / CPRA). Engagement analytics are aggregate, merchant-facing metrics and are not used to make solely-automated decisions about individual storefront visitors.

---

15. Changes to this policy

We may update this policy from time to time. If we make material changes, we will provide notice by appropriate means (for example, by email to merchants and/or an in-app or marketing-site notice) before the changes take effect. The "Last updated" date at the top reflects the latest version. Continued use of the App or the marketing site after the effective date of an update constitutes acceptance of the updated policy.

---

16. Contact us

For privacy questions, to exercise your rights, or to request our Data Processing Addendum or current sub-processor list, contact us:

- **Legal entity:** OPTIVOX (PRIVATE) LIMITED
- **Registered address:** 126, D-2, WAPDA Town, Lahore, Pakistan
- **Contact email:** support@vy-reel.com

If you are in the EEA, the UK, or Switzerland, you also have the right to lodge a complaint with your local data-protection supervisory authority.

Effective date: June 16, 2026 · **Last updated:** June 16, 2026