Vishwaas.ai

## Industry Brief

# E-Commerce & D2C

DPDP Act Compliance for Online Retail, Marketplaces & Direct-to-Consumer Brands

# Why E-Commerce Has the Broadest DPDP Exposure Per Customer Interaction

An e-commerce platform or D2C brand processes personal data at every touchpoint — website visit, app download, account creation, purchase, return, review, support ticket, and marketing interaction. Multiply this by millions of daily active users and the compliance surface is enormous.

More critically, e-commerce companies are the most aggressive users of third-party data sharing: advertising networks, marketing analytics platforms, affiliate partners, logistics aggregators, payment gateways, and cross-border technology vendors all receive personal data as part of normal operations. Under the DPDP Act 2023, every one of these handoffs requires either documented consent or a registered Data Processing Agreement — and the data principal's right to withdraw is enforceable against all of them.

The good news for e-commerce: the DPDP Act does not prohibit data-driven marketing. It requires that consent for it is **genuine, specific, and easily withdrawable** — and that the company can prove it when asked.

# The Four E-Commerce Compliance Challenges

## Challenge 1: Cookie and Tracker Consent Is No Longer Optional

E-commerce websites deploy an average of 40–80 third-party trackers: Google Analytics, Meta Pixel, Google Ads, Hotjar, CleverTap, Mixpanel, affiliate tracking scripts, and retargeting pixels. Each of these places cookies or fingerprints the user's browser for purposes that extend well beyond delivering the shopping experience.

Under the DPDP Act, trackers that collect personal data — including hashed email, device fingerprint, or any identifier that can be linked back to an individual — require purpose-specific, affirmative consent before activation. A pre-ticked "I accept cookies" banner does not satisfy this requirement.

| Tracker Category | Examples | Consent Required? |
|---|---|---|
| Strictly necessary | Session cookie, shopping cart | No — operational necessity |
| Analytics / performance | Google Analytics, Mixpanel, Hotjar | Yes — explicit |
| Marketing / retargeting | Meta Pixel, Google Ads, Criteo | Yes — explicit |
| Affiliate / partner tracking | Impact, Commission Junction | Yes — explicit |
| Personalisation | Dynamic Yield, Insider | Yes — explicit |
| Social media plug-ins | Facebook Like, Twitter Share | Yes — explicit (loads third-party scripts) |

Vishwaas AI solution: The Cookie Consent SDK (banner.js, ~20KB gzipped) is a drop-in embeddable script that intercepts all non-essential trackers, presents a DPDP-compliant consent banner, and activates each tracker category only when the user explicitly consents. The banner renders in the user's browser language (22 Indian languages supported). Consent choices are stored in the Vishwaas AI ledger — hash-chained, timestamped, and auditable.

## Challenge 2: Marketing Consent Must Be Separate From Purchase Consent

The most pervasive DPDP compliance failure in Indian e-commerce is the bundled consent model: account registration (or checkout) includes a pre-ticked checkbox that simultaneously covers order confirmation emails, promotional SMS, WhatsApp marketing, and retargeting ads. The data principal has not meaningfully consented to marketing — they have accepted terms.

The DPDP Act requires consent to be: - Specific to each purpose - Affirmative — silence, pre-ticking, or opt-out-by-default does not constitute consent - Not conditional — a customer cannot be required to consent to marketing as a condition of making a purchase

This means e-commerce companies must design their consent flows to separate:

| Purpose | Data Used | Must Be Separate? |
|---|---|---|
| Order fulfilment and service communications | Name, email, phone, address | No (contractual necessity) |
| Promotional email marketing | Email | Yes — explicit opt-in |
| SMS / WhatsApp marketing | Phone | Yes — explicit opt-in |
| Push notifications (app) | Device token | Yes — explicit opt-in |
| Retargeting / personalised ads | Browsing behaviour, purchase history | Yes — explicit opt-in |
| Sharing with brand/seller partners | Purchase data | Yes — explicit opt-in |
| Sharing with logistics partners | Name, address, phone | Contractual (DPA required) |

**Vishwaas AI solution:** The Consent Campaign module enables e-commerce platforms to re-collect properly structured consent from their existing customer base — a required step for any company migrating from a bundled consent model. Campaigns target customers by consent gap (e.g., all customers who have not given explicit SMS marketing consent), deliver a consent request in their preferred language, and feed responses back into the consent ledger in real time.

## Challenge 3: Third-Party Data Sharing at E-Commerce Scale

A mid-sized Indian e-commerce platform shares customer data with an average of 15–30 external parties:

- **Payment gateways** (Razorpay, Paytm, PhonePe): name, phone, email, order amount
- **Logistics partners** (Delhivery, BlueDart, Shadowfax): name, full address, phone
- **Marketing platforms** (CleverTap, MoEngage, WebEngage): email, phone, purchase history, browsing behaviour
- **Advertising networks** (Google, Meta, Criteo): hashed email, device ID, purchase events
- **Affiliate networks:** click IDs, conversion data
- **Seller ecosystem** (marketplace model): buyer contact data for order fulfilment
- **Return/reverse logistics**: name, phone, address
- **Customer support tools** (Freshdesk, Intercom): email, order history, support tickets
- **Cross-border analytics vendors** (US/EU-hosted): purchase behaviour, demographic segments

Each of these relationships requires either documented consent (for discretionary sharing) or a Data Processing Agreement that restricts the processor to the stated purpose.

Under **DPDP Act Section 8** and the data processor framework, sharing personal data with a party that then uses it beyond the agreed scope makes the original Data Fiduciary co-liable.

**Vishwaas AI solution:** The Vendor Management module maintains a registry of all third-party data processors with DPA status, data categories in scope, risk tier, and cross-border transfer flag. The Data Map module documents which personal data flows to which vendor. Vendors processing data cross-border are flagged pending the publication of DPDP Rules on cross-border transfer restrictions.

### Challenge 4: The Minor Customer Problem

E-commerce platforms have significant underage user bases — particularly in gaming, edtech-adjacent lifestyle categories, and gifting. The DPDP Act Section 9 prohibits processing the personal data of a child (under 18) without verifiable parental consent, and prohibits behavioural tracking or targeted advertising directed at children entirely.

This is an operational challenge for platforms that do not collect date-of-birth at registration:

- Age cannot be verified from most standard registration flows
- Platforms that do know a user is under 18 must obtain guardian consent before any processing
- Targeted advertising to minors is categorically prohibited — not a consent question, a prohibition

**Vishwaas AI solution:** The Consent module supports a is_minor flag and guardian_principal_id linkage on data principal records. Where a minor's age is known, guardian consent is collected and linked to the child's profile. The purpose catalogue allows advertising and profiling purposes to be restricted from minor profiles at the data model level — ensuring tracking scripts are never activated for known minor users regardless of banner interaction.

## E-Commerce Use Cases — Vishwaas AI in Action

### Use Case 1: Horizontal Marketplace — Cookie Consent + Marketing Consent Overhaul

**Scenario:** A top-10 Indian e-commerce marketplace has 50 million registered users. Its current consent model is: a single checkbox at registration covers all marketing, and the cookie banner is a "notice only" banner that activates all trackers on page load.

**Current risk:** DPBI investigation triggered by a user complaint about targeted advertising after explicitly opting out. The company cannot produce evidence that any specific user consented to Meta Pixel tracking or marketing SMS. Potential penalty: ₹250 crore (Schedule 1, item 3 — processing without consent).

**With Vishwaas AI:** 1. Cookie SDK deployed in one script tag — intercepts all non-essential trackers until consent is given 2. Consent campaign targets all 50M existing users: email + app push inviting them to set their preferences in their preferred language 3. Users who do not respond retain only "strictly necessary" cookie permissions — their trackers remain blocked 4. Each consent choice is stored as a hash-chained record with TSA timestamp — DPBI-ready evidence for every user 5. Consent propagation fires to Meta, Google, CleverTap in real time when a user withdraws; they are removed from retargeting audiences within 5 seconds

## Use Case 2: D2C Beauty Brand — WhatsApp Marketing and Right to Erasure

**Scenario:** A D2C beauty brand runs its primary marketing through WhatsApp Business. It has 800,000 opted-in WhatsApp contacts. Customers regularly ask to be removed — but "removed from WhatsApp" is handled manually and does not trigger deletion from the CRM, email list, or analytics platform.

**With Vishwaas AI:** 1. WhatsApp opt-in consent is captured as a distinct purpose (mkt_whatsapp) in the Consent module 2. The brand's CRM (Zoho), email platform (Mailchimp), and analytics tool (Mixpanel) are registered as downstream applications with webhook endpoints 3. When a customer withdraws WhatsApp marketing consent — via the portal, a reply keyword, or a DPR request — the propagation layer fires webhooks to all three systems within 5 seconds 4. The customer is simultaneously removed from WhatsApp campaigns, email marketing lists, and analytics segments — no manual intervention required 5. If the customer subsequently submits an erasure DPR, the unified profile shows all three systems holding data; erasure jobs are dispatched to each

## Use Case 3: Cross-Border E-Commerce — International Vendor Compliance

Scenario: A fashion e-commerce platform uses Shopify (US), Klaviyo (US) for email, Google Analytics 4 (US-hosted), and Afterpay (Australia) for BNPL. Customer data — including purchase history and browsing behaviour — flows to all four cross-border vendors as part of normal operations.

With Vishwaas AI: 1. All four vendors are registered in the Vendor module with cross_border_transfer: true and the destination country noted 2. Data categories flowing to each vendor are documented in the Data Map 3. Consent purposes for marketing and analytics include disclosure of cross-border transfer — satisfying DPDP Act Section 5's notice requirement that the principal be informed of cross-border transfers before consent is sought 4. When DPDP Rules on cross-border transfer restrictions are published, the Vendor module's flagged entries provide a ready-made inventory for compliance gap assessment

# Regulatory Alignment

| Regulation | Relevant Obligation | Vishwaas AI Module |
|---|---|---|
| DPDP Act §§11–12 | Notice of purposes, data categories, processors, cross-border transfers | Notice Module — multilingual, standalone, DPDP Rules Rule 3 format |
| DPDP Act §6 | Specific, affirmative, unbundled consent per purpose | Consent Module — purpose catalogue; Cookie SDK |
| DPDP Act §6(4) | Withdrawal must be as easy as giving consent | Portal — consumer-facing consent toggle; Propagation — real-time downstream sync |
| DPDP Act §8 | Data processor agreements; purpose limitation | vendor Module — DPA registry, data category scope |
| DPDP Act §9 | No processing of child data without guardian consent; no ad targeting of children | Consent Module — minor flag, guardian linkage, purpose restriction |
| DPDP Act §9 | No processing of child data without guardian consent; no ad targeting of children | Consent Module — minor flag, guardian linkage, purpose restriction |
| DPDP Act §8(6) | Breach notification within 72 hours | Breach Module — countdown, notification workflow |
| DPDP Act §§11–12 | Right to access, correction, erasure across all processors | DPR Module — unified erasure orchestration; identity graph |
| DPDP Act §13 | 30-day grievance SLA | DPR Module — SLA tracking, DPBI escalation |
| RBI Payment Aggregator Guidelines | Customer data protection for payment flows | Vendor Module — payment processor DPAs; Consent Module |
| Consumer Protection (E-Commerce) Rules 2020 | Seller data handling; no unfair data practices | Notice Module + Consent Module |

# Why E-Commerce and D2C Teams Choose Vishwaas AI

he Cookie SDK is production-ready in one day: A single <script> tag deployment. The SDK intercepts all third-party trackers, renders the consent banner in the user's language, and stores every consent decision in the hash-chained ledger. No engineering sprint required — the compliance team can deploy it independently.

Consent campaigns reach your existing base: Most e-commerce companies have 3–10 years of customer data collected under invalid consent models. Vishwaas AI's Consent Campaign module lets you re-collect valid consent from your existing base — segmented by consent gap, delivered in the customer's preferred language, tracked to completion.

Real-time propagation protects against post-withdrawal liability: Every email sent, every retargeting ad served, every push notification delivered after a withdrawal is a DPDP Act violation. Vishwaas AI's < 5 second propagation SLA means your marketing platforms are updated before the next campaign dispatch cycle runs.

One DPR request reaches every system: E-commerce companies have the most fragmented customer identity landscape — the same customer in the CRM, the OMS, the returns portal, the loyalty platform, and the marketing tool. Vishwaas AI's identity unification engine links all of these. A single erasure request reaches every system; the DPR module tracks completion across each.

+1 888 208 5076
+91 901 926 6824

sales@crossidentity.com

www.crossidentity.com