Retail & E-Commerce

DPDPA 2023 Implementation Handbook

Digital Personal Data Protection Act, 2023 • India

For retail chains, online marketplaces, food delivery, fashion brands, loyalty programs, and last-mile delivery.

1. Overview & Applicability

Retail and e-commerce entities collect a rich tapestry of personal data — purchase history, location, preferences, payment details, and browsing behaviour. As consumer-facing businesses, their compliance directly impacts millions of customers. Loyalty programs, personalised marketing, and third-party seller data sharing are key compliance hotspots. Food delivery and fashion platforms that profile minors face additional obligations.

2. Key Definitions Under DPDPA

These definitions govern how the Act applies to your sector:

Purchase Data	Order history, product preferences, cart data — personal data when linked to an identified customer.
Payment Data	Credit/debit card details, UPI IDs, wallet information — sensitive financial data.
Location Data	Delivery address, real-time GPS location for last-mile delivery — personal data.
Behavioural Data	Browsing patterns, wishlist, search history, time spent on product pages — personal data.
Loyalty Data	Loyalty points, tier status, purchase frequency — used for profiling and marketing.
Third-Party Seller	Sellers on your marketplace who receive customer data for order fulfillment — require DPAs.

3. Core Compliance Obligations

Every entity in this sector that processes personal data must comply with the following obligations:

1. **Marketing Consent**
   Transactional consent (for order processing) does NOT cover promotional emails, SMS, or push notifications. Obtain separate, explicit marketing consent.
2. **Loyalty Program Governance**
   Clearly disclose how loyalty data is used. If shared with brand partners, obtain consent. Allow customers to opt out of loyalty profiling.
3. **Third-Party Seller Data**
   Customer data shared with sellers for order fulfillment must be governed by a DPA. Sellers cannot use this data for independent marketing.
4. **Payment Data Security**
   Comply with PCI-DSS. Never store CVV numbers. Tokenise card data. Implement 3D Secure authentication.
5. **Delivery Partner Data**
   Address and contact details shared with last-mile delivery partners must be governed by a DPA and restricted to delivery purposes only.
6. **Recommendation Engine**
   If you use AI for product recommendations based on personal data, disclose this in your privacy notice and allow opt-out.
7. **Returns & Refunds**

	Data collected during returns (reason, product photos) must be limited to returns management and deleted after completion.
8	**Customer Reviews** Do not use customer review data for profiling or share with third parties without consent.

4. Implementation Checklist

Use this checklist to track your DPDPA compliance readiness:

- ☐ Separate transactional consent from marketing consent in checkout, account creation, and loyalty enrollment flows.
- ☐ Audit your loyalty program — how is data used, who has access, is it shared with partners?
- ☐ Execute DPAs with all third-party sellers, delivery partners, payment gateways, and analytics vendors.
- ☐ Implement a clear marketing opt-out mechanism in every promotional communication.
- ☐ Build a customer rights portal — access purchase history, correct data, request account deletion.
- ☐ Publish a plain-language privacy notice on your website, app, and checkout page.
- ☐ Appoint a Grievance Officer and display contact details at checkout and on your contact page.
- ☐ Audit all personalisation and recommendation systems — document data used and allow opt-out.
- ☐ Implement PCI-DSS compliant payment processing — never store raw card data.
- ☐ Review children's data — if your platform sells to minors, implement age verification and parental consent.
- ☐ Train customer service teams to handle data rights requests (access, deletion, correction).
- ☐ Conduct an annual vendor audit of all data processors and refresh DPAs.

5. Applicable Penalties

The Data Protection Board of India (DPBI) may impose the following penalties for non-compliance:

Rs. 250 Crore	Failure to implement reasonable security safeguards resulting in a personal data breach
Rs. 200 Crore	Breach of obligations related to processing children's personal data
Rs. 150 Crore	Failure to fulfill obligations as a Significant Data Fiduciary (SDF)
Rs. 50 Crore	Failure to comply with Data Principal rights or other provisions of the Act

6. Implementation Roadmap

Follow this phased approach to achieve full DPDPA compliance:

1	**Month 1: Customer Data Map** Map all customer touchpoints — web, app, store, loyalty — and data collected at each.
2	**Month 2: Consent Redesign** Rebuild checkout and account flows to separate transactional vs. marketing consent.
3	**Month 3: Vendor DPAs** Audit and execute DPAs with sellers, delivery partners, payment gateways, and analytics tools.
4	**Month 4: Customer Rights** Build self-service rights portal. Set up Grievance Officer process.
5	**Month 5: Security & Training** Enhance payment security, train customer service and marketing teams.
6	**Month 6+: Monitor** Annual loyalty program audit and vendor review cycle.

📣 Marketing teams often assume that a customer who bought from you has consented to all communications. Under DPDPA, this is incorrect — separate, specific consent is required for each marketing channel.