

Advisory to Members

Customer Personal Data Protection and Consent Compliance Framework

(Compliance with the Digital Personal Data Protection Act, 2023 (DPDP Act))

The Retailers Association of India (RAI) issues this advisory to guide its members in establishing a legally compliant, operationally sound, and customer-centric framework for obtaining, managing, and enforcing customer consent for the processing of personal data.

With the enactment of the Digital Personal Data Protection Act, 2023, consent has become a central governance and compliance requirement for retail organizations operating in India.

This advisory is to ensure that:

- a) Customer data is processed lawfully, transparently, and ethically
- b) Core retail operations (sales, service delivery, fulfilment) are not disrupted
- c) The organization remains compliant with the Digital Personal Data Protection Act, 2023 (DPDP Act), applicable Rules, and relevant sectoral regulations.
- d) Institutional, operational, and legal risks are effectively mitigated

2. Regulatory Context

Under the DPDP Act 2023, consent is the primary lawful basis for processing personal data in India. In the retail context, customer information such as identity details, contact information, transaction history, payment details, and behavioural data qualifies as personal data and attracts statutory compliance obligations.

Members are advised to note that consent is no longer a routine checkbox or marketing formality. It is a **core compliance and accountability control** that determines:

- a) The lawfulness of data processing activities
- b) The organization's ability to demonstrate regulatory compliance during audits, inspections, or investigations

3. Scope of Applicability

This advisory applies to all retail functions and business units where customer personal data is collected, processed, stored, or shared, including but not limited to:

- a) Physical retail stores and point-of-sale (POS) systems
- b) E-commerce platforms and mobile applications
- c) Customer relationship management (CRM) systems
- d) Loyalty programs and membership schemes
- e) Marketing, promotions, and customer engagement initiatives
- f) Payments, billing, refunds, and fraud prevention
- g) Delivery, logistics, and fulfilment partners
- h) Customer support, call centres, and grievance handling
- i) Analytics, AI-enabled tools, and personalization engines
- j) Third-party service providers handling customer data

4. Core Principles of Consent Governance

Members are advised to ensure that all customer consent obtained meets the following standards:

- a) Free – Given voluntarily, without coercion or denial of goods or services
- b) Informed – Based on clear, understandable information regarding data usage; if data is shared with group entities or used for allied business interests, this must be explicitly disclosed
- c) Specific – Linked to clearly defined and limited purposes
- d) Unambiguous – Based on a clear affirmative action by the customer
- e) Purpose-limited – Not extendable beyond the stated and agreed purposes
- f) Revocable – Withdrawable by the customer at any time

All relevant purposes must be explicitly mentioned. A single blanket consent is insufficient to support multiple, unrelated, or evolving retail data uses.

5. What Consent Management Means in Retail Operations

Consent management is a continuous operational process, not a one-time document or form. It includes:

- a) Informing customers, in clear commercial and legal terms, how their data will be used
- b) Capturing, storing, and enforcing consent decisions across systems
- c) Ensuring data access and processing aligns with the specific consent provided

6. Purpose-Specific Consent Categories

Members should obtain consent separately, where applicable, for the following purposes:

- a) Customer registration and account management
- b) Processing sales transactions and order fulfilment
- c) Payment processing, billing, refunds, and fraud prevention
- d) Delivery, logistics coordination, and order tracking
- e) Customer support, complaints, and after-sales service
- f) Loyalty programs, reward points, and membership benefits
- g) Marketing communications, promotions, and personalized offers
- h) Sharing data with payment gateways, logistics partners, and service vendors
- i) Processing by third-party platforms, aggregators, or service providers
- j) Secondary use including analytics, business intelligence, research, AI-driven insights, and digital innovation

7. Consent Capture Mechanism

7.1 Mode of Capture: Consent may be captured through:

- a) Digital mechanisms via websites, mobile applications, POS systems, or CRM platforms (including link-based acceptance or OTP validation)
- b) Paper-based consent only where digital capture is not feasible, followed by timely entry into the system

7.2 Content of Consent Notice

Each consent notice must clearly state all applicable purposes listed in this document. The language shall be plain, consumer-friendly, operationally accurate, and legally precise.

8. Consent Withdrawal and Its Effect

Customers may withdraw consent at any time through:

- a) Customer support or helpdesk channels
- b) Digital customer portals or mobile applications (where available)
- c) Written requests addressed to customer care

Upon withdrawal:

- a) Further processing for the withdrawn purpose must cease
- b) Data required to be retained under applicable laws (tax, accounting, fraud prevention, or dispute resolution) shall be preserved
- c) No new or secondary use shall occur beyond lawful retention requirements
- d) Business continuity and legal compliance shall take precedence where mandated

9. Legal and Statutory Exceptions

Consent is not required where processing is necessary for:

- a) Compliance with legal or regulatory obligations
- b) Court orders or statutory directions
- c) Fraud prevention, security incidents, or lawful investigations
- d) Public interest or statutory reporting requirements

10. Recordkeeping

Members are advised to maintain auditable records evidencing:

- a) Date and time of consent
- b) Version of the consent notice provided
- c) Purpose(s) consented to
- d) Records of consent withdrawal, if any

11. Technology and Systems Integration

Consent management shall be embedded into:

- a) Retail IT systems, POS platforms, CRM, and digital channels
- b) Access to customer data shall be governed by role-based and purpose-based controls
- c) Systems shall prevent processing inconsistent with recorded consent

12. Roles and Responsibilities

Members should clearly define responsibilities, including:

- a) Legal & Compliance Team: - Policy oversight, regulatory interpretation, audits
- b) IT and Systems Team: – System design, access controls, data security
- c) Store Operations and Frontline Teams: – Accurate consent capture and customer communication
- d) Marketing and Analytics Teams – Use of data strictly within consented purposes

Mandatory training shall be conducted for both operational and non-operational staff.

13. Review and Continuous Improvement

This document shall be:

- a) Reviewed annually or upon regulatory change
- b) Updated to reflect new technologies, business models, or workflows
- c) Tested through internal audits, control assessments, and compliance reviews

14. Key Risks of Non-Compliance

Failure to implement effective consent management may expose the organization to:

- a) Monetary penalties under the DPDP Act (up to INR 250 Crores)
- b) Regulatory investigations and enforcement actions
- c) Civil, consumer, and contractual litigation
- d) Loss of customer trust and reputational damage

RAI advises all members to treat customer personal data protection as a strategic governance priority and to align internal policies, systems, and training programs with the principles outlined in this advisory.

This guidance is intended to support compliance readiness and operational resilience across the retail sector.

Disclaimer

1. This advisory is issued by the Retailers Association of India for general guidance and awareness purposes only. It is intended to assist member organizations in understanding and operationalizing key consent and personal data protection requirements under the Digital Personal Data Protection Act, 2023 and related regulations.
2. This document does not constitute legal advice, regulatory approval, or a definitive interpretation of the law. The applicability and implementation of the principles outlined herein may vary based on an organization's specific business model, operational structure, technological architecture, contractual arrangements, and risk profile.
3. The Retailers Association of India disclaims any liability arising from reliance on this advisory, including but not limited to regulatory actions, penalties, operational disruptions, or commercial impacts. Responsibility for compliance with applicable data protection and privacy laws rests solely with individual member organizations.