



THE **|** FRACTIONAL
CMO **|** COMPANY.

December 2025

White paper

Data Responsibility in India: What the DPDP Act Means for Modern Marketers

For years, digital marketing in India grew on a simple equation: more data = better targeting.

A dark blue background featuring a glowing, undulating digital wave composed of numerous small, glowing blue and purple dots connected by thin lines, creating a sense of depth and motion.

Every click, cookie, device ID and transaction detail was treated as fuel for growth.

But as digital maturity increased, so did consumer discomfort.

People began asking questions like, “Who is tracking me?”, “Why am I seeing these ads?”, “How long is my data stored?”

With the introduction of the **Digital Personal Data Protection (DPDP) Act**, India has entered a new era of **data responsibility, consumer rights and transparent marketing**. And for marketers, this is not merely a compliance exercise — it is a fundamental shift in how growth must be built.

This paper is a practical guide to what **you can / cannot / should / should not do** under India’s new data environment, with a clear comparison to GDPR and a marketer-friendly playbook. Hope you find it useful!

Tell us what you think on contact@fractionalcmo.company

Why the DPDP Act is a Big Turning Point for Marketing in India

Unlike the earlier ecosystem that allowed wide use of identifiers, cookies and loosely-governed third-party data, the DPDP Act ensures:

- Explicit consent for using personal data
- Clear purpose for which data will be used
- Defined retention periods
- Rights for users to access, correct or erase their data
- Strict rules for children's data
- Higher accountability for companies acting as data fiduciaries

For marketers, this means:

No more grey areas in targeting

No more overreliance on third-party data

No more “collect everything and decide later”

No more agency-owned ad accounts without governance later”

It pushes companies to shift from data exploitation to data stewardship.

DPDP vs GDPR: What Marketers Should Know

Global brands familiar with GDPR will find the DPDP Act conceptually aligned. Local Indian companies will experience the biggest behavioural change. Here's the simplified marketer comparison:

01

Consent

- **GDPR:** granular, informed, opt-in
- **DPDP:** needs to be explicit, specific, documented, and revocable

02

Purpose Limitation

Both require you to state why you're collecting data and restrict reuse.

Example:

If you collect data for account creation, you cannot automatically add that person into your marketing automation workflow without separate consent.

03

Data Minimisation & Retention

- **GDPR:** minimal data, short retention
- **DPDP:** similar - delete or anonymise once purpose is fulfilled

04

Children's Data

DPDP is stricter - prohibits profiling or targeted ads for children.

05

Cross-Border Data Transfers

Both require safeguards; DPDP will follow a “trusted countries” list.

Bottom line:

If you're GDPR-compliant, you are largely aligned with DPDP expectations. If you're not, you will need to rewire how your marketing, CRM and ad tech pipelines work.

The Practical Realities for Marketers in India

DPDP doesn't make marketing harder ... it makes it cleaner, predictable and future-proof.

Here is what fundamentally changes in your day-to-day operations:

- Retargeting and lookalike audiences require consented data
- First-party data becomes the core asset, not a support system
- CRM hygiene becomes essential
- Martech stacks need review
- Agencies cannot own data or platform access without controls
- Anonymised insights become more relevant than identity-based insights
- Consent logs become as essential as campaign logs



Do's / Don'ts - marketer edition (DPDP 2025)

✓ DO — What You Must Start Doing Immediately

1. Treat Consent as a Growth Asset

- Build clear consent forms
- Ask only for necessary details
- Provide easy opt-out options
- Maintain consent logs
- Meta Ads
- CRM integrations
- Pixels
- Server-side tracking setups

2. Build a Strong First-Party Data Engine

Use:

- Loyalty programs
- Newsletters
- Logged-in experiences
- Preference centres
- Interactive content (zero-party data)

5. Rely More on Anonymised / Aggregate Signals

This enables:

- Cohort-based targeting
- Contextual advertising
- AI-driven recommendations without personal data misuse

6. Update Vendor & Agency Contracts

Include:

- Data processing clauses
- Purpose limitation
- Retention limits
- Access controls
- Audit rights

3. Strengthen CRM + CDP Hygiene

- Deduplicate data
- Mark consent status
- Delete outdated personal data
- Track retention periods
- Restrict access by roles

4. Ensure All Ad Accounts Are Brand-Owned

Agencies can access, but cannot own your:

- Google Ads

Do's / Don'ts - marketer edition (DPDP 2025)

✗ DO NOT — Practices That Are No Longer Acceptable

1. Do NOT Collect Data Without Explaining Why

Vague consent statements won't work.

2. Do NOT Reuse CRM Data for New Purposes

Data collected for transactions cannot be used for ads unless separately consented.

3. Do NOT Upload Databases Into Ad Platforms Without Permission

Custom audience uploads now require documented consent.

4. Do NOT Use Purchased Third-Party Databases

Buying lists or scraping websites is explicitly risky — and often illegal.

5. Do NOT Retain Data Forever

You must define:

- how long
- for what reason
- when it will be deleted

6. Do NOT Mix Children's Data Into Marketing Pipelines

No tracking, targeting or behavioural analytics.

7. Do NOT Allow Agencies to Run Platform Accounts Independently

Your brand must own:

- all access
- all integrations
- all data

Can Do / Cannot Do — Under the DPDP Act

CAN DO — With the Right Safeguards

- ✓ Personalisation (only for consented users)
- ✓ Retargeting (with documentable consent)
- ✓ Cross-border processing (if whitelisted or contractually safeguarded)
- ✓ AI-driven audience modelling (using anonymised or consented data)
- ✓ Lookalikes (only if the seed list is consented)
- ✓ Analytics & measurement (in anonymised form)
- ✓ Marketing automation (for consented customers)

CANNOT DO — Even If the Tech Allows It

- ✗ Behavioural targeting of children
- ✗ Hidden tracking pixels without user knowledge
- ✗ Covert data enrichment
- ✗ Inferential profiling without consent
- ✗ Screen scraping or unauthorized third-party data imports
- ✗ Using personal data for purposes not stated during collection
- ✗ Granting vendors or agencies unrestricted access to customer data

Where Indian Marketing Goes From Here

In the short term, teams will feel the operational weight:

- New forms
- New scripts
- New CRM fields
- New vendor contracts
- New governance reviews

But in the long run, DPDP forces a shift toward quality over **quantity**.

The brands that win will be the ones that:

- Build deeper customer trust
- Get higher engagement from consented audiences
- Rely on genuine relationships instead of intrusive tracking
- Build durable first-party data assets
- Reduce wasted ad spend
- Strengthen brand reputation and compliance resilience

The Future: Not Less Marketing, Just Better Marketing

DPDP doesn't end performance marketing.

It ends **indiscriminate marketing**.

This is the moment where Indian marketers move from:

- Broad targeting → Thoughtful segmentation
- Third-party lists → Direct customer relationships
- Agency dependency → Brand data ownership
- Grey-area dashboards → Transparent ecosystems
- Data hoarding → Data responsibility

Marketing in India is evolving and this time, the evolution will make your brand stronger, not weaker. (And who would have thought compliance would do this!)