The Great Digital Reset
7 Ways India's New DPDP Regime Reclaims Your Rights from Big Tech

We have all been participants in a lopsided digital experiment: the silent "social contract" where we trade our most intimate data for the convenience of an app, usually by clicking "I Agree" on a document we never read. For years, the internet has felt like a digital Wild West, with users effectively serving as raw material for corporate algorithms.

That power dynamic is finally facing a reckoning. The **Digital Personal Data Protection (DPDP) Act, 2023**, and the recently unveiled **2025 Rules** represent the most significant shift in India's digital landscape to date. These Rules are the missing piece of the puzzle, operationalizing the Act's broad promises and transforming you from a mere "user" into a **Data Principal**—an individual with enforceable legal rights. Meanwhile, tech companies are rebranded as **Data Fiduciaries**, a term that imposes a legal obligation of trust akin to that of a doctor or a lawyer.

As India moves toward this new era of digital sovereignty, here is how the new regime fundamentally rewires your life online.

1. The Legal "She": A Default for Inclusivity

In a striking departure from centuries of patriarchal legal drafting, India's data law has made feminine pronouns the default. Under Section 2(y), the law uses "she" and "her" to refer to all individuals, irrespective of their actual gender.

This is not a mere linguistic quirk; it is a profound signal about inclusivity in India's digital future. By explicitly stating that *"she" in relation to an individual includes the reference to such individual irrespective of gender* [Section 2(y)], the Act subverts traditional drafting norms where "he" was the catch-all for humanity. It sets a progressive tone for a law designed to protect a diverse population of nearly a billion connected citizens.

2. Death to the "Dark Pattern": The Comparability Standard

We've all experienced the "Dark Pattern" trap: an app makes it effortless to sign up with a single tap, but requires a labyrinthine journey through menus or even a physical phone call to opt out. The new regime kills this tactic through a strict legal standard of **comparability**.

Under Section 6(4), your right to withdraw consent must be just as easy as your right to give it. Rule 3(c)(i) takes this further, mandating that the **communication link** for withdrawal must be presented in the same notice as the initial consent request. If you joined with one tap, the "unsubscribe" or "withdraw" button must be just as accessible. You can no longer be forced to hunt for your privacy settings; the door to leave must be as wide as the door to enter.

3. Your Personal Privacy Agent: The "Consent Manager"

Managing privacy across a dozen different social, banking, and shopping apps is a full-time job no one wants. To solve this, the law introduces a new category of entity: the **Consent Manager** [Section 2(g)]. Registered with the Data Protection Board, these entities act as a single point of contact to manage, review, and withdraw your consent across multiple platforms.

While adding a "middleman" sounds counter-intuitive, these managers are governed by strict **fiduciary capacities** [First Schedule, Part B, Item 8]. Crucially, they are legally barred from "reading" the data they manage; they handle the permissions, not the content [First Schedule, Part B, Item 2]. To prevent "fly-by-night" operations from handling your rights, the government has set a high bar for entry: a minimum net worth of **INR 2 crore** [First Schedule, Part A, Item 4]. This ensures these agents have the technical and operational capacity to defend your interests against corporate giants.

4. Rights with "Bite": The Legal Duty of the User

In a move that distinguishes India's law from the EU's GDPR, the DPDP Act makes rights a two-way street. As a Data Principal, you are granted significant protections, but you also carry legal **Duties** [Section 15]. You are prohibited from impersonating others, suppressing material information for state-issued IDs, or—most notably—filing frivolous grievances.

There is a real "bite" to these responsibilities. Under Section 28(12), if the Data Protection Board determines a complaint is false or frivolous, it has the power to issue a warning or even **impose costs** on the complainant. While this is intended to prevent the system from being clogged by bad-faith actors, policy advocates are already asking: Will the threat of legal costs "chill" legitimate grievances from users who are afraid to speak up?

5. Absolute Child Safety: Beyond the Tracking Ban

The Act treats children (anyone under 18) as a protected class, imposing a "hard ban" on any data processing likely to cause a "detrimental effect" on their well-being [Section 9(2)]. This includes a total prohibition on tracking, behavioural monitoring, and targeted advertising directed at kids [Section 9(3)].

To enforce this, companies must obtain **verifiable consent** from parents [Rule 10]. The 2025 Rules specify "techno-legal" methods for this, such as using **virtual tokens** from a **Digital Locker** or checking reliable identity details. While business models for EdTech and social media will have to be completely rebuilt, the law does provide common-sense exemptions for safety: schools and crèches are still permitted to track children for security and educational purposes [Fourth Schedule, Part A].

6. Justice at Your Fingertips: The Digital Office

The era of waiting years in dusty courtrooms for a privacy ruling may be over. The Data Protection Board is designed to be a "Digital Office," where the entire lifecycle of a complaint—from filing to the final decision—is **digital by design** [Section 28].

Under Rule 20, the Board is empowered to adopt **"techno-legal measures"** that conduct proceedings without requiring your physical presence. While the Board retains the power to

summon individuals and examine them on oath—just like a civil court—the goal is a streamlined, paperless justice system. It is an ambitious attempt to solve the geographical and bureaucratic hurdles that typically plague the Indian legal system.

7. The 3-Year Expiry: "Use It or Lose It"

Data is often described as the "new oil," but under India's new rules, it now has an expiration date. For the first time, major platforms face a "use it or lose it" mandate. According to Rule 8 and the Third Schedule, data fiduciaries must erase personal data after three years of inactivity if the "specified purpose" is no longer being served.

This rule is strictly targeted at the biggest players:

- **E-commerce platforms** with over 2 crore registered users.
- **Social media intermediaries** with over 2 crore registered users.
- **Online gaming intermediaries** with over 50 lakh registered users.

However, accountability remains a priority. Even if primary data is erased, **Rule 8(3)** and the accompanying illustrations clarify that **processing logs** must be retained for at least **one year** from the date of the transaction. This ensures that if a data breach or dispute occurs, there is still a trail for the Board to investigate.

8. Conclusion: A Global Blueprint or a New Gatekeeper?

India has officially transitioned from a data "Wild West" to a highly regulated ecosystem. By mandating "one-click" consent withdrawal and creating a digital-first justice system, India is positioning itself as a global leader in digital rights.

Yet, the journalist in me must ask the hard question: will this new structure truly democratize privacy, or will the high barriers to entry—like the INR 2 crore requirement for Consent Managers—simply create a new class of corporate gatekeepers? As we step into our roles as "Data Principals," we must decide if we are ready for the legal responsibilities that come with our new rights. The social contract has been rewritten; now we must see if it can be enforced.

Desai Saksena & Associates

Chartered Accountants

- 40+ years of practice in India
- 5 Partners
- 3 offices in India, 1 in Doha and 1 in Dubai
- Global Presence
- 500+ Clients Globally
- 50+ Professionals
- Member of Integra International

Call Us at
91-022-66261600

Make A Quote
contact@dsaca.co.in

Visit our Website
www.dsaca.co.in

Mumbai (Fort)

First Floor, Laxmi Building,
Sir P.M. Road, Fort,
Mumbai – 400001
Tel: +022-66261600/17
Email: **contact@dsaca.co.in**

Mumbai (Goregaon)

119, Shivam Chambers, 1st Floor,
S V Road, Goregaon (W),
Mumbai 400 062
Tel: +022-49791142
Email: **contact@dsaca.co.in**

Doha, Qatar

Al Rufaa Tower, 1st Floor,
Office No.1,2&3, Old Salata,
PO Box: 30653, Doha – Qatar
Mob: +974 66 039 427
Contact: **naresh@aksaa.qa**
Website: **www.aksaa.qa**

Dubai, UAE

BurJuman, Business Tower-
Office No. 45, Level 18, Bur
Dubai, Dubai-UAE
Mob: +971 55 492 0306
Contact: **contact@dsaca.net**
Website: **www.dsaca.ae**