client alert
November 14, 2025

cyril amarchand mangaldas
ahead of the curve

THE DPDP RULES 2025 : A FINAL ROADMAP TO IMPLEMENTATION

The Digital Personal Data Protection Rules, 2025 (**Final Rules**), issued under the Digital Personal Data Protection Act, 2023 (**DPDP Act**) were notified on November 13, 2025, and reflect the long-awaited final rulemaking, and tangible timelines for operationalizing the DPDP Act.

We have set out a high-level summary of the implementation timelines under the Final Rules, what has changed from the Draft Rules, and what is next.

Timelines

Broadly:

a. Substantive obligations will take effect after 18 months,
b. Consent management related stipulations come into effect after 12 months, and
c. A limited set of governance and institutional provisions (specifically, Rules 1, 2 and 17 to 21) have been brought into force immediately to set up the Data Protection Board (**Board**), and deal with its composition, inquiry procedures, terms of service for officers, and digital functioning.

Significantly, Rule 19 prescribes that all inquiries initiated by the Board must be completed within 6 months, unless extended (with recorded reasons) for periods not exceeding 3 months at a time. Strengthening the original construct under DPDP Act, Rule 20 clarifies that the Board will function as a "digital office" and may adopt techno-legal measures to conduct proceedings without requiring the physical presence of individuals, while retaining the power to summon and examine persons on oath and exercising powers of civil courts.

As indicated in Government's public statements, operationalizing DPDP Act to set up the Board is a strategic move towards implementation.

With the Board now empowered to constitute itself and begin adopting procedures, organizations should actively monitor Board-issued guidelines, notifications, and prepare for digital interactions, including secure document exchange and remote hearing readiness. While these provisions do not yet impose direct operational obligations on companies, they activate the enforcement framework under the DPDP Act and therefore merit strategic attention.

Key Changes

From an organization's perspective, some key changes from the Draft Rules (which we had previously analyzed here in our client alert) that may affect implementation are:

- **Broader, Mandatory Retention Thresholds:** All Data Fiduciaries (and their Data Processors) must retain personal data, traffic data and processing logs for 1 year from the date of processing for specified regulatory purposes. After this period, the data must be erased unless further retention is mandated by law including under third schedule. This creates overlapping obligations for entities (such as significant social media intermediaries) called out in the third schedule.

- **Reasonable security safeguards:** The Rules specify illustrative minimum safeguards "such as" encryption, access controls, monitoring and backups, suggesting these were mandatory minimums "where applicable". This may allow businesses to adopt a more flexible approach.

- **Child-facing services and advertising:** For organizations offering services to children, the Final Rules retain exceptions around verifiable consent, including allowing real-time tracking for child safety, and reinforce prohibitions on tracking, behavioral monitoring and targeted advertising that may have a detrimental effect on children for non-exempted categories.

- **Grievance redressal timelines:** The Final Rules now cap grievance redressal at 90 days, for both Data Fiduciaries and consent managers to respond to grievances. While a standard of reasonableness subsists, this may allow for a wider window than what currently exists under the Information Technology Act, 2000.

- **Consent notice - "specific" description of goods/services:** The Final Rules replace the earlier requirement for an *itemised* description of goods and services with a requirement for a *specific* description.

What Next?

The Final Rules do not significantly deviate from the Draft Rules, and continue to be detailed, prescriptive and operationally heavy. While businesses had expected the Final Rules to have certain relaxations, the core business-facing obligations remain largely intact.

Key areas that will require advance preparation include:

- **Privacy notices:** Clear, detailed, plain-language notices in multiple Indian languages with a specific description of personal data and purposes, and dedicated means for a Data Principal to exercise their rights and seek grievance redressal.
- **Consent flows:** Valid consent mechanisms, easy withdrawal, and separate flows for children and Person with Disability (**PwDs**), with different verification approaches for minors and PwDs.
- **Security safeguards:** Implementation of appropriate security measures, access controls, monitoring and mandatory 1 year log retention.
- **Breach reporting:** "Without delay" notifications to Data Principals and 2 layered reporting to the Board with detailed filings to the Board within 72 hours.
- **Grievance handling:** Internal processes calibrated to comply with the statutory ceiling of 90 days for grievance redressal as well as to enable verification modules prior to honoring Data Principal's requests.
- **Data Protection Impact Assessment (DPIAs) and Audit:** Significant data fiduciaries bracing for yearly DPIAs and audits.
- **Contracting with processors:** Ensuring that agreements with vendors and service providers appropriately flow down DPDP Act-compliant obligations, including security, breach support, deletion/return, log retention and cooperation duties.

Given this generous runway of 18 months, enforcement thereafter may be strict, and it will be imperative for organizations to make good use of this time.

While organizations have thus far preferred to wait till publication of the Final Rules, with DPDP Act now being in force with a definitive timeline for implementation, organizations must initiate and expedite their internal assessments, map data flows, complete gap assessments and begin roll out of their compliance roadmap including updating notices, policies and contracts, revisiting and revamping existing consent mechanisms, evaluating sufficiency and adequacy of security controls and incident-response processes well ahead of the effective date.

Key Contacts

Arun Prabhu
Partner – (Co-Head – Digital | TMT)
arun.prabhu@cyrilshroff.com

Mihir Rale
Partner – (Co-Head – Digital | TMT)
mihir.rale@cyrilshroff.com

Huzefa Tavawala
Partner (Head - Digital Disruption)
huzefa.tavawala@cyrilshroff.com

Anirban Mohapatra
Partner
anirban.mohapatra@cyrilshroff.com

Arya Tripathy
Partner
arya.tripathy@cyrilshroff.com

Cyril Amarchand Mangaldas
Advocates & Solicitors

100+ years of legacy | 1200 Lawyers | Over 220 Partners

Peninsula Chambers, Peninsula Corporate Park, GK Marg, Lower Parel, Mumbai 400 013, India
T +91 22 6660 4455 E cam.mumbai@cyrilshroff.com W www.cyrilshroff.com
Presence also in Delhi-NCR | Bengaluru | Ahmedabad | Hyderabad | Chennai | GIFT City | Singapore | Abu Dhabi