SARAF AND PARTNERS
LAW OFFICES

REDESIGN PRIVACY

From Draft to Notified: DPDP Rules Kickstart the Compliance Journey

SARAF AND PARTNERS
LAW OFFICES

REDESIGN PRIVACY

Introduction

The Digital Personal Data Protection Act, 2023 (**DPDPA**) represents a landmark legislative initiative establishing a comprehensive regulatory framework for the processing of digital personal data in India. The DPDPA embodies fundamental principles of consent-based personal data processing, accountability of Data Fiduciaries, and the protection of Data Principal rights. Pursuant to the rule-making powers conferred under the DPDPA, the Ministry of Electronics and Information Technology (MEITY) initiated a consultative process by releasing the Draft Digital Personal Data Protection Rules, 2025 (**Draft Rules**) for public stakeholder comment. Following extensive deliberation and feedback from diverse stakeholder groups, MEITY notified the Digital Personal Data Protection Rules, 2025 ("**Final Rules**") on 13th of November 2025, thereby operationalizing the substantive and procedural provisions contained in the parent legislation. The Final Rules mark a significant step in operationalizing the DPDPA by translating its principles into clear, enforceable obligations for organizations.

Enforcement and Compliance Timeline through the Rules come into force in three stages.

- The **establishment of the Data Protection Board**, rule-making powers and select procedural provisions **take effect immediately**.
- **Consent Manager registration** and related obligations become operational after **12 months**.
- **Core compliance requirements** including notice, consent, security safeguards, retention, children's consent, grievance handling, and cross-border transfer— come into force in **18 months**.

Key Changes

The table below presents a structured comparison between the Draft Rules and the Final Rules, outlining how key obligations have evolved across the two versions. It distils the substantive changes in scope, process, and compliance requirements, providing a clear and concise reference for understanding the regulatory shifts introduced in the final framework.

Rules	Draft Digital Personal Data Protection Rules, 2025 (Draft Rules)	Digital Personal Data Protection Rules, 2025 (Final Rules)
Rule 1 - Commencement (When each rule becomes applicable)	The Draft Rules mentioned that the Rules covering notice requirements, government processing, security safeguards, children's consent, Significant Data Fiduciaries and functioning of the Data Protection board would operationalize on a later unspecified date while all other rules would start on publication. It did not specify the actual date or time gaps, leaving Data Fiduciaries uncertain about when compliance would be required.	The Final Rules give specific timelines for when each rule becomes operationalized and are listed below: • Immediately: Core Governance Rules. i.e., Data Protection Board Procedures and foundational provision (Rule 1, 2 and 17 to 21). • After 1 year: Consent Manager registration requirements, i.e., Rule 4. • After 18 months: Full enforcement, i.e., all compliance obligations with the commencement of penalties (Rule 3, 5 to 16 and 22-23).
Rule 2 - Definition Clause	The Draft Rules relied mainly on definitions in the Act and did not define terms like "***verifiable consent***", "***user account***" or "***techno-legal measures***".	The Final Rules explicitly defined the term ***user account*** as "*the online account registered by the Data Principal with the Data Fiduciary, and includes any profiles, pages, handles, email address, mobile number and other similar presences by means of which such Data Principal is able to access the services of such Data Fiduciary*" and clarified the meaning of verifiable consent and techno-legal measures.

Rules	Draft Digital Personal Data Protection Rules, 2025 (Draft Rules)	Digital Personal Data Protection Rules, 2025 (Final Rules)
Rule 5 - State's Processing of Personal Data (How the government may process data for schemes and services)	The State was permitted to process personal data for providing statutory or policy-based benefits. The corresponding standard in Draft Second Schedule, Item (d) required the State to make reasonable efforts only to ensure the accuracy of the personal data being used.	The Final Rules mandate that all processing under Rule 5 must comply with the strengthened requirements in Second Schedule. Item (d) now obligates the State to make reasonable efforts to ensure not just accuracy, but also the completeness and consistency of personal data.
Rule 6 - Security Safeguards (How organizations must protect personal data)	The obligation to implement access-control measures was framed as an absolute requirement, applying uniformly across all systems used by a Data Fiduciary or Data Processor. The rules did not differentiate between environments where the organization had full administrative control and environments where it lacked such control (e.g., cloud infrastructure or vendor-managed platforms).	A qualifier "wherever applicable" was introduced, which broadens and clarifies the scope of the access-control obligation.
Rule 8 - Data Retention & Erasure (How long data must be stored and when it must be deleted)	Under Rule 8, the draft mainly addressed deletion once the purpose was over. It required a 48-hour advance notice before deleting data.	The Final Rules introduce a major change: Rule 8(3) now requires Data Fiduciaries to retain all personal data, all associated traffic data, and all processing logs for at least one year after the processing occurs. This applies even if a user deletes their account or requests erasure.

Rules	Draft Digital Personal Data Protection Rules, 2025 (Draft Rules)	Digital Personal Data Protection Rules, 2025 (Final Rules)
Rule 10 - Verifiable Consent for Children (How Data Fiduciaries must confirm parental consent)	It contained four different verification scenarios involving identity documents, Digital Locker, and Government-authorized entities.	It clarifies the scope of an "***Authorized Entity***", i.e., an entity legally permitted to issue or verify age/identity details (including Digital Locker service providers).
Rule 11 - Consent for processing personal data of people with disabilities (How guardian's consent must be verified)	It combined consent requirements for persons with disabilities within the broader framework for children. This structure merged with two distinct categories and made it unclear whether a Data Fiduciary should follow the child-verification process or a separate guardian-verification process.	It establishes a separate Rule 11 that clearly distinguishes guardian consent for people with disabilities from parental consent under Rule 10. This rule requires Data Fiduciaries to verify that the consenting individual is a lawful guardian appointed or recognized under the Rights of Persons with Disabilities Act, 2016 or the National Trust Act, 1999. Processing is permitted only after confirming such legal authority through appropriate statutory documentation or government-issued proof of guardianship.
Rule 14 - Rights & Grievance Redressal (How Data Principal can raise concerns and how quickly companies must respond)	It required companies to publish their grievance-handling timelines but did not set any maximum period, allowing potentially very long response cycles.	It introduces a clear upper limit: companies must resolve all grievances within 90 days. This creates a uniform and enforceable service level.

Conclusion

The Final Rules transform the DPDPA from a high-level framework into a set of obligations that organizations can practically operationalize. With clearer definitions, streamlined processes, and a phased enforcement timeline, the Final Rules give Data Fiduciaries the structure they need to build compliance in a measured and strategic manner. The emphasis has shifted from interpreting broad statutory concepts to implementing specific controls whether through upgraded consent architectures, enhanced security safeguards, strengthened data-quality measures, or revised vendor arrangements. The clarity brought through the Final Rules allow organizations to map requirements to existing systems, identify gaps, and gradually mature their data-governance capabilities. Organizations now have a clear timeline for compliance and must begin mapping their data flows and create systems to ensure compliance to avoid hefty penalties of up to Rs. 250 crores. Ultimately, this approach supports smoother adoption, reduces compliance friction, and enables organizations to embed DPDPA obligations into their operational DNA in a sustainable and future-ready way.

For any query, you may reach out to **Akshayy S Nanda**, Partner (Competition Law and Data Privacy Practice) at Akshayys.Nanda@sarafpartners.com.

Contact us:
www.sarafpartners.com | **LinkedIn** | **X** | **Facebook** | **Instagram**

Our Offices:
Delhi NCR | **New Delhi** | **Mumbai** | **Bengaluru** | **Hyderabad**