BLOGS

Navigating the Digital Frontier: A Primer on the DPDP Draft Rules, 2025

Khushi Malviya · 13 Sep 2025

Introduction

As our lives become increasingly interwoven with the digital realm, the need to safeguard personal data has become paramount. Recognizing this, and building upon the foundation laid by the Digital Personal Data Protection Act (DPDP Act), the anticipated **Draft Digital Personal Data Protection (DPDP) Rules, 2025** promise to flesh out the operational details of India's data protection framework.

These rules, once finalized, will be crucial for both individuals (Data Principals) seeking to control their digital footprint and organizations (Data Fiduciaries) tasked with processing personal data responsibly. This primer offers a comprehensive overview of what you can expect from these Draft Rules.

Decoding Key Definitions: Who's Who in the Data Ecosystem

Understanding the key players is fundamental to grasping the DPDP framework. The Draft Rules will likely refine and clarify these roles:

- Data Principal: This is you- the individual whose personal data is being processed. You are the subject of data protection and holder of the rights under the DPDP Act.
- Data Fiduciary: This is the organization or entity that determines the purpose and means of processing personal data. Think of companies, government bodies, and even individuals in certain contexts. Data Fiduciaries bear the primary responsibility for complying with the DPDP framework.
- Data Processor: This entity processes data on behalf of the Data Fiduciary. Cloud service providers, marketing agencies working for a company, or payroll processors would typically fall into this category. Processors have specific obligations but are ultimately guided by the

Data Fiduciary's instructions.

- Personal Data: This is any data about an individual that can identify them, directly or indirectly. It's broad, encompassing names, addresses, contact details, online identifiers, financial information, health data, and much more. The Draft Rules may further clarify sensitive personal data categories, if any, requiring heightened protection.
- Processing: This is a wide-ranging term encompassing virtually any operation performed on personal data, including collection, storage, organization, structuring, use, disclosure, alteration, erasure, or destruction.

Data Principal Rights

The Draft Rules are expected to detail the procedures and mechanisms for exercising these rights:

- Right to Access Information: You have the right to request information from a Data Fiduciary about what personal data they hold about you, the purposes of processing, and other relevant details. The Rules will likely specify the format and timeframe for responses.
- Right to Correction and Erasure (Right to Rectification and Right to be Forgotten): You can request correction of inaccurate or incomplete data. You can also request erasure of your personal data when it is no longer necessary for the purposes for which it was collected, or if your consent is withdrawn (where consent is the basis for processing). The Rules may outline exceptions and procedures for these requests.
- Right to Grievance Redressal: Every Data Fiduciary must establish a grievance redressal mechanism to address complaints from Data Principals regarding data processing. The Draft Rules will likely detail the process, timelines, and escalation pathways, potentially involving internal officers and the Data Protection Board.
- Right to Nominate: You can nominate another individual to exercise your rights under the DPDP Act on your behalf, particularly in cases of incapacity (e.g., mental incapacity, demise). The Rules will likely specify the process for nomination and the scope of the nominee's authority.
- Right to Data Portability (Potential): While not explicitly stated in the initial Act, future rules might elaborate on data portability, allowing individuals to receive their data in a structured, commonly used, and machine-readable format and potentially transmit it to another Data Fiduciary. This remains to be seen in the Draft Rules, 2025.

Obligations on Data Fiduciaries

The Draft Rules will place significant responsibilities on Data Fiduciaries to ensure compliance with the DPDP framework. These obligations are crucial for building a trustworthy data ecosystem:

- Notice and Consent Framework: Data Fiduciaries will need to provide clear and accessible notices to Data Principals before collecting their personal data. These notices must be in easily understandable language, specifying the purpose of collection, the data being collected, and the rights of the Data Principal. The Rules will likely detail the required content of the notice, consent mechanisms (e.g., consent managers), and valid consent conditions (free, specific, informed, unambiguous, and revocable).
- Data Security and Breach Management: Data Fiduciaries are obligated to implement reasonable security safeguards to protect personal data from breaches. The Draft Rules may specify minimum security standards, data localization requirements for certain sensitive data, and procedures for reporting data breaches to the Data Protection Board and affected Data Principals. Timelines and specific information to be included in breach notifications are expected to be detailed.
- Grievance Redressal Mechanism: As mentioned earlier, establishing a robust grievance redressal mechanism is mandatory. The Rules will likely prescribe details about the structure, process, and timelines for handling complaints, ensuring accessibility and fairness for Data Principals.
- Significant Data Fiduciaries (SDFs): Enhanced Obligations: The Act recognizes “Significant Data Fiduciaries” – entities handling large volumes of sensitive personal data, posing a higher risk. The Draft Rules are anticipated to define criteria for designating SDFs (potentially based on data volume, sensitivity, and impact). SDFs may be subject to more stringent obligations, such as data protection impact assessments, audits, and appointing data protection officers.
- Processing Children’s Data: The DPDP Act and Rules will likely have specific provisions for processing children’s data, requiring verifiable parental consent and stricter data protection measures due to children’s vulnerability. The Rules will likely define age thresholds for children and specify mechanisms for age verification and parental consent.

Exemptions and Legitimate Uses

While the DPDP framework prioritizes data protection, it also recognizes the need for certain exemptions and legitimate uses of data in specific circumstances. The Draft Rules will clarify these exceptions, ensuring a balance between privacy and operational needs:

- Legitimate Uses: The Act allows for processing data without consent for certain "legitimate uses," such as for specified legal purposes, for the State to provide benefits or services, for medical emergencies, for responding to disasters, and for employment-related purposes. The Draft Rules will likely elaborate on the scope and limitations of these legitimate uses, preventing misuse and ensuring they are genuinely necessary and proportionate.
- Security and Law Enforcement: Exemptions may exist for processing data for national security, law enforcement, and prevention of crime. However, these exemptions are expected to be narrowly defined and subject to safeguards to prevent overreach.
- Research and Statistical Purposes: Processing data for bonafide research, statistical, and archival purposes may also be exempt from certain provisions, subject to conditions to ensure privacy is still respected (e.g., anonymization, de-identification).

Enforcement and Penalties

The DPDP framework will be enforced by the Data Protection Board of India (DPB), a regulatory body established under the Act. The Draft Rules are crucial for outlining the DPB's powers, procedures, and enforcement mechanisms:

- Data Protection Board (DPB): The DPB will act as the regulator, adjudicating on compliance, investigating breaches, and imposing penalties. The Rules may detail the DPB's structure, composition, and operational procedures.
- Inquiries and Investigations: The DPB will have the power to conduct inquiries and investigations into data processing practices and alleged violations of the DPDP Act and Rules. The Rules will likely outline the process for initiating investigations, gathering evidence, and conducting hearings.
- Penalties and Directions: Non-compliance can lead to significant financial penalties. The Act itself specifies penalties up to INR 250 crore. The Draft Rules might provide further guidance on penalty calculation and may also empower the DPB to issue directions to Data Fiduciaries to rectify non-compliant practices, cease processing, or take other remedial measures.

- Appeals: Data Fiduciaries will likely have the right to appeal against DPB orders to higher judicial forums, ensuring a system of checks and balances.

Conclusion

The Draft DPDP Rules, 2025, are poised to be a critical instrument in operationalizing India's data protection framework. By providing detailed procedures, clarifying obligations, and empowering individuals with enforceable rights, these rules aim to create a more responsible and trustworthy digital ecosystem.

For Data Principals, this means greater control over their personal data and recourse if their rights are violated. For Data Fiduciaries, it signifies a shift towards data responsibility, requiring proactive compliance measures and a commitment to transparent and ethical data processing.