STRIDE LEGAL

STRIDE LEGAL

STRIDE LEGAL INSIGHTS

ALL YOU NEED TO KNOW ABOUT THE DIGITAL PERSONAL DATA PROTECTION RULES, 2025

I.INTRODUCTION:

On 13 November 2025, the Central Government notified the Digital Personal Data Protection("**DPDP**") Rules, 2025 ("**Rules**") operationalising the DPDP Act, 2023("**Act**"). These Rules finally establish the procedural backbone for India's new data protection regime, outlining phased implementation, new consent standards, security obligations, compliance timelines, and a strengthened adjudicatory framework through the Data Protection Board of India ("**DPB**").

This newsletter provides a clear breakdown of the Rules and their implications for businesses, digital platforms, and Significant Data Fiduciaries.

II.BACKGROUND:

India's journey toward a structured data protection regime began after the

Supreme Court recognised privacy as a fundamental right in 2017. Several drafts and iterations followed, eventually leading to the DPDP Act, 2023. The Act, however, required detailed rules before it could operate in practice.

The notification of the DPDP Rules, 2025 now provides a definitive roadmap for compliance and implementation.

III.THE PHASED IMPLEMENTATION (RULE 1)

The Rules will be enforced through a staggered timeline to provide organizations a structured runway for compliance. The implementation is broadly divided into three phases:

1. IMMEDIATE EFFECT –

Provisions related to the administrative establishment of the Data Protection Board (DPB) of India, including rules for the appointment of its chairperson and members.

2. 12-MONTH HORIZON –

Provisions governing the registration and obligations of Consent Managers are set to be enforced one year from now.

3. 18-MONTH HORIZON –

The core operational provisions of the Rules will be enforced 18 months from now. This grace period applies to the compliance requirements, including data breach reporting procedures, security safeguards and Consent Mechanisms.

IV. KEY OBLIGATIONS FOR ALL DATA FIDUCIARIES

The Rules introduce several new, specific mandates for all entities processing personal data.

1. NEW CONSENT FRAMEWORK –

The Rules mandate a new standard for privacy notices and consent verification. The notice provided to a Data Principal must be a standalone document, in plain language, and must provide an itemised list of all personal data being collected. It must also include a clear method for consent withdrawal. For users under the age of 18, Fiduciaries must obtain verifiable consent from a parent or lawful guardian. Rule 10 outlines acceptable methods, including the use of Digital Locker, authorised tokens, or existing verified parental accounts.

2. DATA BREACH REPORTING

A strict 72-hour timeline is now mandated under Rule 7 reporting a data breach to the DPB. The affected users must be notified without delay if the breach is likely to result in harm.

3. MANDATORY DATA ERASURE

Rule 8 mandates that certain fiduciaries (e.g., e-commerce, social media) must erase a user's personal data after three (3) years of continuous inactivity. A 48-hour notice must be sent to the user before this erasure.

4. SECURITY SAFEGUARDS

Rule 6 mandates all data fiduciaries to implement appropriate data security measures, such as encryption, masking, to secure personal data. The security logs are to be retained for a period of one year to enable the detection and investigation of breaches.

V. EXEMPTIONS

1. CHILDREN'S DATA

While Rule 10 imposes strict verifiable parental consent obligations, Rule 12 provides certain exemptions. These exemptions apply to specific classes of data fiduciaries, such as educational institutions and healthcare professionals, provided the processing is necessary for the health protection or in the child's best interest.

2. PROCESSING FOR STATE SERVICES AND RESEARCH

Rule 5 allows the government and its agencies to process data when providing services like subsidies or licenses.

Similarly, Rule 16 allows processing data without consent when it is necessary for research, archiving, or statistical purposes.

VI. THE 'SIGNIFICANT DATA FIDUCIARY' (SDF) REGIME

Rule 13 subjects Significant Data Fiduciaries (SDFs) to a higher accountability regime. They are required to conduct an annual Data Protection Impact Assessment (DPIA) and a separate annual Audit, with reports from both submitted to the DPB. In a new mandate for AI Governance, Rule 13(3) requires SDFs must "observe due diligence to verify that algorithmic software deployed by it is not likely to pose a risk to the rights of Data Principals." SDFs must also appoint an India-based Data Protection Officer (DPO) to act as the point of contact for grievance redressal and the DPB.

VII. THE DATA PROTECTION BOARD (DPB) OF INDIA

The DPB is established as a 'digital-first' adjudicatory body under Rule 20. It is vested with the powers of a civil Court and its proceedings will be conducted digitally. Furthermore, the Rules establish a strict timeline for adjudication. Rule 19(9) mandates that any inquiry by the Board must be completed within six months from the date of the complaint or intimation, though this period may be extended for reasons to be recorded in writing. Rule 22 clarifies that any person aggrieved by a DPB Order may appeal to the appellate tribunal.

VIII. CONSENT MANAGERS & CROSS-BORDER TRANSFER

1. CROSS-BORDER DATA TRANSFER–

Rule 15 permits the cross-border transfer of personal data by default. However, the Central Government retains the power to restrict transfers to specific foreign countries or entities through a general or special order.

2. CONSENT MANAGERS-

As per Rule 4, Consent Managers will function as intermediaries to enable Data Principals to manage their consent. The Rules mandate that these entities be companies incorporated in India with a minimum net worth of ₹2 crore. They are required to provide an interoperable platform for users to give, manage, and withdraw consent. Furthermore, they are legally obligated to act in a fiduciary capacity for the user, ensuring a strict avoidance of any conflict of interest with Data Fiduciaries.

IX.IMPACT

The DPDP Rules strengthen user rights by ensuring clearer consent, greater transparency, and faster grievance redressal. This, in turn, imposes strong and mandatory accountability on companies, which face an 18-month deadline to implement a complete compliance overhaul. Organisations will now be required to invest in security safeguards such as encryption, access controls, and detailed operational processes to meet the 72-hour breach-reporting mandate.

Furthermore, the Rules hold Significant Data Fiduciaries to a higher standard, requiring them to conduct enhanced oversight to ensure that their data-processing systems and algorithms do not pose risks to user rights. Overall, the Rules mark a major step toward building a safer and more trustworthy digital ecosystem.

X.CONCLUSION

while Rule 10 imposes strict verifiable parental consent obligations, Rule 12 provides certain exemptions. These exemptions apply to specific classes of data fiduciaries, such as educational institutions and healthcare professionals, provided the processing is necessary for the health protection or in the child's best interest.