INDIALAW

DATA PRIVACY

Detailed Analysis of the Digital Personal Data Protection Rules, 2025 (hereafter “Rules 2025”), which are the subordinate rules under the Digital Personal Data Protection Act, 2023 (“DPDP Act”) in India

AUTHOR Abha Shah

PUBLISHED 14 November 2025

The Rules 2025 represent a significant step forward in India's data-protection regime. They build out the high-level DPDP Act in a way that draws on international good practices (consent, breach-notification, minimisation, erasure).

Purpose / Key Objectives:

The Rules-2025 are meant to operationalise the DPDP Act that aim to:

1. *Establish* detailed compliance requirements and duties for data fiduciaries – especially on transparency, consent, security, and breach management.
2. *Facilitate* the exercise of individual data rights – i.e. operationalizing user rights of access, correction, and deletion.
3. *Strengthen* safeguards for vulnerable groups – i.e. children and persons with disabilities.
4. *Regulate* and govern cross-border data flows/ data transfers, retention, and supervisory mechanisms.
5. *Align* and support privacy protection with business and governance priorities; keeping innovation-friendly digital ecosystem.

Evaluating the Rules: Merits and Concerns

Merits of the Rules:

- These Rules bring clarity supplying more detailed obligations which will help organisations plan compliance.
- They align with global best practices through focus on children's data, retention/erasure norms, and breach notifications
- The explicit requirement of "reasonableness" of safeguards promotes risk-based approach rather than rigid checklists.
- The transparency/notice obligations bolster individual rights and enable accountability.

Areas of Concerns / Gaps

- Significant government discretion and exemptions may impact oversight and independence.
- Operationalising obligations like verifiable consent for children or retention/erasure requirements can be challenging, especially for smaller or legacy systems.
- Ambiguity in definitions, e.g., "significant data fiduciary" and thresholds for stricter obligations.
- Potential compliance burden and operational costs for data-heavy or cross-border businesses, which may affect innovation.
- Limited transparency in stakeholder consultations; draft summaries may not reflect full input.

Implications of Key Provisions

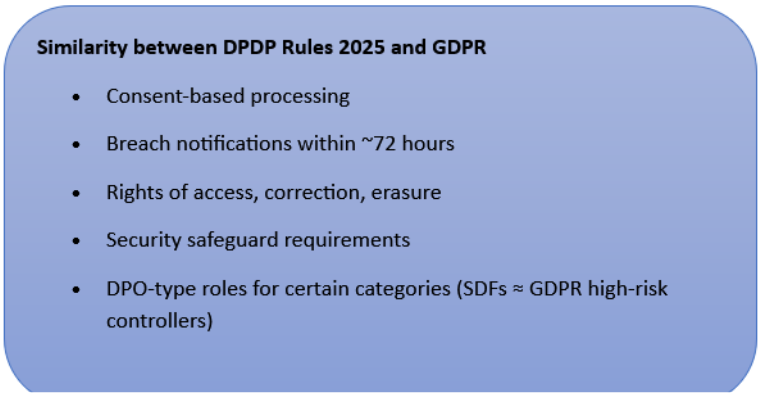
S.No	Rule	Description	Implications
1	Rule 5 – Reasonable Security Safeguards	This Rule mentions data fiduciaries to implement measures such as encryption, obfuscation, masking or the use of virtual tokens, access controls (logs, monitoring), data backups, detection of unauthorized access, contractual and security safeguards.	Businesses will need to audit/upgrade their data-security infrastructure. Smaller firms may struggle with costs or sophistication.
2	Rules 7 – Data Breach Notification	This Rule mentions data fiduciaries to intimate the Data Protection Board "without delay" on becoming aware of a personal data breach specifying the nature, extent, timing, location of breach; circumstances and reasons leading to the breach, consequences, mitigation and remedial measures.	Strong operational/incident-response requirements. Data-fiduciaries must have policies, detection capabilities.
3	Rule 8 – Limitation on Retention / Erasure Obligation	This Rule mentions data fiduciaries like e-commerce, social media intermediaries and online gaming portals with large user-base; must erase personal data after 3 years of data collection.	Firms need strong data-lifecycle/record-management mechanisms. May impose challenges for business models reliant on long-term data retention for analytics, profiling, etc.

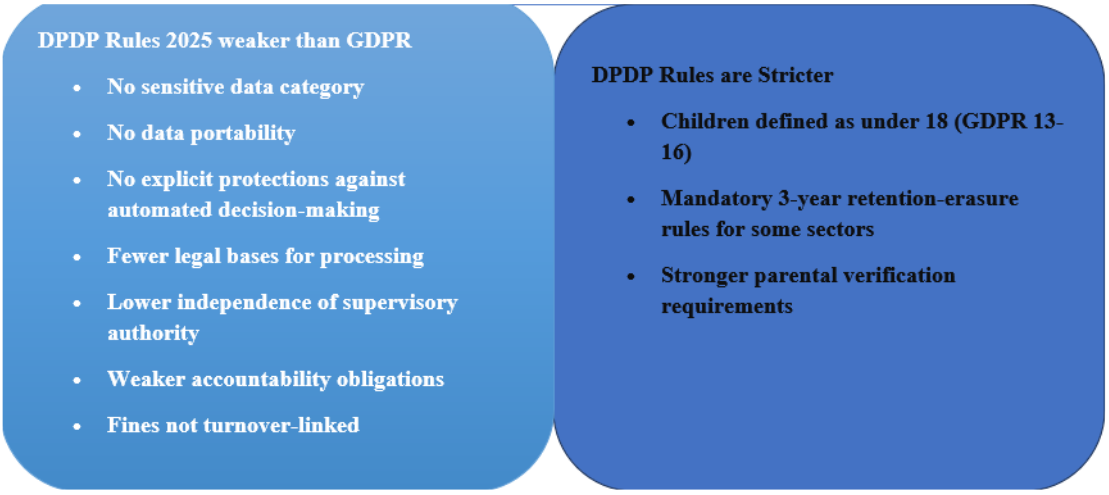
4	Rules 10 / 11- Consent & Children / Persons with Disabilities	This Rule mentions processing of personal data of vulnerable groups i.e. children and persons with disability – This requires “verifiable consent” of parent/guardian.	Platforms (especially social media, apps aimed at minors) must redesign flows for age-verification, parental/guardian consent. May introduce friction or exclusion risk for minors/guardians.
5	Rule 13 – Additional Obligations of Significant Data Fiduciary	This Rules mentions about annual independent audits, Mandatory Data Protection Impact Assessments, stronger governance and stricter record-keeping:	SDFs face **higher accountability and oversight** compared to ordinary data fiduciaries.Compliance cost for audits and impact assessments.; which require significant investment in governance, technology, and specialised staff.
6	Rule 15 – Transfer of personal data outside the territory of India	This Rule mentions that cross-border transfers will be allowed subject to prescribed restrictions.	Multinational businesses will need to monitor regulatory developments on which countries are permitted, what safeguards needed, possibility of localisation obligations.

Practical Impact on Various Stakeholder Segments

- Individuals / Data Principals: Better rights (access/erasure), clearer notices, mandatory breach notifications. But they must be aware of rights and vigilant.
- Private Sector / Businesses: Need to map data-flows, inventory personal data, ensure retention/erasure policies, implement security safeguards, update notices and consent flows, prepare for breach-notification mechanisms, audit cross-border flows.
- Start-ups / SMEs: Greater compliance burden may hit smaller players harder. They may need to budget for compliance (legal, tech, operations).
- Multinationals / SaaS / Platforms: Must watch thresholds/classifications (e.g., if you become a “significant data fiduciary”), address localisation/cross-border transfer risk, align global flows with Indian obligations.
- Government / Regulators: Need to strengthen oversight infrastructure (e.g., the Data Protection Board), ensure clarity, transparency in rule-making, handle exemptions carefully to avoid undermining trust.

Comparative Angliss between the Digital Personal Data Protection Rules, 2025 (India) and the EU General Data Protection Regulation (GDPR).





Conclusion:

While the Rules 2025 aims for the DPDP Act to be at par with international good practices consent, breach-notification, minimisation, erasure) ***however,*** its success will depend heavily on clarity in definitions, realistic operationalisation timelines, the strength of oversight institutions, and how well business practicality is balanced with rights-protection.

If implemented well, they could elevate India's data-protection landscape in the digital economy era. If not, there's a risk of regulatory burden, ambiguity, and erosion of trust.

Related Practice Areas

Data Protection and Privacy