Grant Thornton | 90 in Bharat and beyond

#GTBharat
SHAPING VIBRANT INDIA

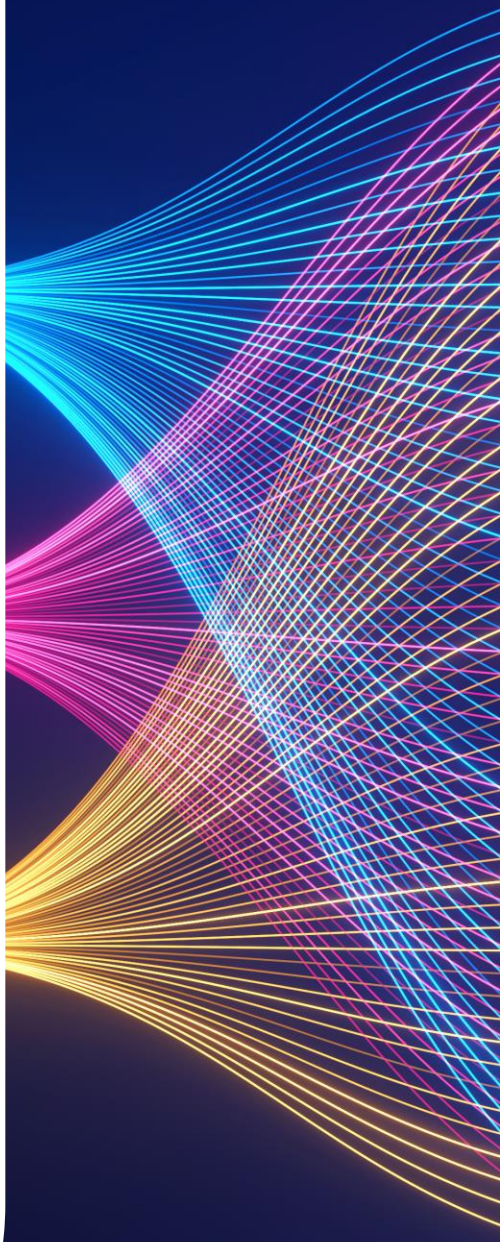
Privacy Compliance Guide 2025

Executive summary

The Digital Personal Data Protection (DPDP) Rules, 2025, published on 13 November 2025, establish India's complete regulatory framework for data protection compliance. These Rules operationalise the Digital Personal Data Protection Act (DPDPA), 2023 through a carefully structured three-phase implementation timeline spanning 18 months. They introduce three distinct compliance periods, allowing organisations to achieve readiness across governance establishment, intermediary registration, and full operational compliance.

The DPDP Rules introduce a mandatory 90-day limit for responding to data principal grievances, a major change from the earlier undefined timelines. This creates immediate compliance urgency for all data fiduciaries, regardless of size or sector. The Rules also clarify that sector-specific laws override DPDPA's data erasure requirements, ensuring organisations meet legal retention obligations before deleting data. This alignment helps avoid conflicts with regulatory mandates across industries. The Rules also provide that personal data may be transferred outside India only if the data fiduciary (DF) complies with conditions specified by the Central Government. The final rules adopt a 'blacklist' approach transfers are permitted except to countries or territories notified as restricted. Internal consent management solutions within data fiduciary ecosystems remain critical, while external consent managers act as neutral intermediaries between data fiduciaries and data principals. Additionally, significant data fiduciaries must additionally conduct annual data protection impact assessments (DPIA), independent audits, algorithmic fairness checks for AI systems, and appoint a data protection officer (DPO). Rule 7 mandates that any personal data breach must be reported to the Data Protection Board (DPB) and affected individuals within 72 hours of becoming aware.

The DPDP Rules 2025 set up the Data Protection Board of India (DPBI) as the country's first dedicated data protection authority, operating as a fully digital office. It has powers to investigate breaches, issue compliance directions, and impose penalties. Appeals against its decisions will go to the Telecom Disputes Settlement and Appellate Tribunal (under TRAI). The Board is sector-agnostic but will coordinate with regulators like IRDAI, RBI, SEBI and others to ensure consistent enforcement. This marks a significant transformation in India's data protection landscape, requiring organisations to prepare comprehensively across technology, processes, policies, and governance.



Phased implementation timeline

The Rules structure compliance obligations across three distinct phases with precise activation dates, enabling organisations to develop phased readiness plans with regulatory certainty. Call to action for organisations to follow timelines.

Phase	Rules covered	Effective date	Key implications
Phase 1: Immediate implementation	1, 2, 17-21	Effective from 13 November 2025	It provides foundational governance and definitional provisions. Rule 1 provides clear phased timelines, eliminating uncertainty. Rule 2 introduces critical definitions like 'techno-legal measures' and 'verifiable consent'. Rules 17-21 operationalise the DPB, enabling complaint handling and enforcement. This phase focuses on governance setup rather than business operational compliance.
Phase 2: Consent manager registration	Rule 4	Effective from 13 November 2026	Introduces mandatory registration for consent managers, who facilitate consent management for data principals. Eligibility requires Indian incorporation, financial soundness, technical capacity, and conflict-of-interest safeguards. Consent managers must maintain 7-year consent records, implement security measures, and publish transparency disclosures.
Phase 3: Full operational compliance	Rules 3, 5-16, 22-23	Effective from 13 May 2027	Substantive compliance obligations affecting daily operations become effective from this phase. It includes privacy notices, security safeguards, breach notifications, and data erasure rules. Rule 7 mandates 72-hour breach reporting; Rule 8 adds legal compliance exceptions for erasure. Organisations must implement robust security, consent withdrawal mechanisms, and grievance redressal within 90 days.

Critical changes: Draft vs final rules

Comparison between January 2025 draft and November 2025 final rules reveals substantive modifications affecting compliance frameworks.

Rule number	Topic	Implication of new rule
Rule 1	Commencement and notification	The final Rules eliminate ambiguity by setting clear timelines for compliance. This allows organisations to plan resources effectively, with immediate governance obligations and extended deadlines for operational requirements such as consent and security.
Rule 2	Definitions	Introducing new definitions such as 'techno-legal measures' and 'verifiable consent' provides clarity for implementation. This ensures consistent interpretation across compliance processes and operationalises child protection and breach notification obligations.
Rule 3	Notice given by data fiduciary to data principal	The requirement for privacy notices to be presented independently, not embedded within lengthy terms and conditions. Notices must clearly list granular purposes for data processing with specific descriptions, categories of personal data collected, rights available to individuals, and contact details of the DPO or grievance officer. They must also be easily accessible and provided in English, with translations into any of the 22 Indian languages upon request to ensure inclusivity and transparency.
Rule 8	Time period for specified purpose to be deemed as no longer being served	This introduces an exception to data erasure, ensuring that organisations do not delete personal data when retention is required under other applicable laws. This prevents conflicts between DPDP obligations and sectoral regulations, such as those governing financial records, employment documentation, or telecom requirements. Organisations must now assess overlapping retention mandates before erasing data, balancing purpose-based retention, statutory requirements, and erasure rights. This change signals a shift toward multi-framework compliance, requiring organisations to update retention schedules and governance processes while preparing for lawful government information requests under Schedule 7. Businesses must align DPDP obligations with sectoral laws and implement mechanisms for confidentiality and traceability.
Rule 13	Additional obligations for significant data fiduciary	Significant data fiduciaries are required to conduct annual DPIA and audits to ensure compliance with this Act and its rules. They must submit key findings to the Board, exercise due diligence to verify that technical measures and algorithmic software do not pose risks to data principals' rights and implement restrictions to prevent specified personal and traffic data from being transferred outside India.
Rule 14	**Rights of data principals**	**Introducing a mandatory 90-day grievance resolution timeline creates operational urgency. Organisations must establish robust redressal mechanisms and update processes to meet this strict SLA.**

Rule number	Topic	Implication of new rule
Rule 15	Transfer of personal data outside territory of India	This broadens the cross-border transfer provisions but clarifies that data fiduciaries can transfer personal data globally unless the destination country is blacklisted by the Central Government. Additional restrictions, including data localisation and enhanced compliance measures, apply only to significant data fiduciaries for certain sensitive data categories. Organisations must monitor government notifications and review global data flows to remain compliant.
Rule 23	Calling for information from data fiduciary or intermediaries	The Central Government may, for purposes listed in the Seventh Schedule, direct any data fiduciary or intermediary to provide specified information within a given timeframe through the authorised person named in the said Schedule. Where such disclosure could harm India's sovereignty, integrity, or security, the Government may prohibit informing the affected data principal or any other party, unless prior written approval is obtained from the authorised person.

Call to action as per DPDPA 2023 read with DPDPA Rules 2025

Privacy notice requirements (Rule 3)

DFs must provide notices independently presented in plain language describing personal data collection, processing purposes and services, rights withdrawal and exercise mechanisms, DPB grievance procedures, and DF representative contact information. Notices must shift from itemised to specific description, allow multiple purposes, and be prominently displayed rather than embedded in lengthy policy documents.

Security safeguards (Rule 6)

Security safeguards have become prescriptive, mandating specific minimum measures for all data fiduciaries regardless of size or data volume. These include encryption, masking or tokenisation, strict access controls, one-year audit log retention, backup mechanisms, contractual obligations for data processors, and robust organisational and procedural controls. Compliance is no longer optional; every DF must implement these safeguards.

Breach notification (Rule 7)

Within 72 hours of **on becoming aware** of any personal data breach, DFs must notify affected data principals describing breach nature, extent, timing, location, consequences, mitigation measures, safety measures, and contact information. Simultaneously, DFs must notify DPB initially without delay, then provide comprehensive 72-hour report including updated facts, measures taken, remedial actions, contact information, erasure instructions, and affected user account particulars.

Data erasure (Rule 8)

DFs must erase personal data upon “Third Schedule” period completion if data principals have not approached fiduciaries or exercised rights, except where retention is necessary for legal compliance. However, deletion of personal data such as, associated traffic data and logs of processing cannot occur within the first year due to mandatory log retention requirements, and any erasure request during this period will not be possible. Additionally, data must be retained where required for legal compliance, meaning organisations must reconcile DPDP obligations with sectoral laws before erasure. 48 hours prior to deletion, fiduciaries must notify data principals, who can prevent erasure by reactivating their account or contacting the fiduciary.

Child data compliance (Rule 10)

Child data processing requires verifiable parental consent for individuals under 18 years. The Rules clarify that verifying the parent-child relationship is not required—only the parent's identity and age must be confirmed. Verification can be done through reliable details already available with the fiduciary (such as KYC records or government ID) or voluntarily provided credentials, including virtual tokens from authorised entities like digital locker. This simplifies consent flows while ensuring compliance.

Persons with disabilities safeguards (Rule 11)

Processing personal data of persons with disability requires verifiable consent from a lawful guardian for individuals with disabilities. The guardian must be appointed by a court, a designated authority under the Rights of Persons with Disabilities Act, 2016, or a local committee under applicable guardianship law. Organisations must conduct due diligence to confirm the guardian's status, which includes verifying official documentation such as a disability certificate issued under the Person with Disabilities Act, 2016.

Significant data fiduciary obligations (Rule 13)

Organisations designated as SDFs must conduct annual DPIA assessing processing risks with independent assessment and Board reporting; annual independent audits ensuring compliance with Board reporting; algorithmic fairness verification of technical systems; and implementation of measures preventing Central Government-specified personal data and traffic data transfer outside India.

Grievance redressal (Rule 14)

DFs and consent managers must prominently publish grievance redressal procedures with maximum 90-day response time and implement measures ensuring compliance. This new firm deadline creates immediate operational requirement affecting all organisations. The identifier definition expanded to include email address and mobile number.

Cross-border data transfers (Rule 15)

All personal data processing under the Act may transfer outside India only if data fiduciaries meet Central Government-specified requirements (pending notification). Anticipated mechanisms include adequacy determinations, standard contractual clauses, binding corporate rules, data subject consent with safeguards, sectoral restrictions, and critical personal data localisation.

Regulatory governance & enforcement

Data Protection Board of India

The DPBI will be established following the appointment of its chairperson and members through search-cum-selection committees. Once operational, it will function as a fully digital office and serve as the adjudicating authority for privacy compliance. The chairperson is recommended by committee comprising cabinet secretary (Chair), legal affairs secretary, MeitY secretary, and two experts. Members are recommended by separate committee with MeitY secretary (Chair), legal affairs secretary, and two experts. Central Government appoints based on recommendations. Board chairperson and members receive compensation per Fifth Schedule specifications. The Board functions as digital office with authority to adopt techno-legal measures enabling remote proceedings without physical presence.

Schedules overview

Schedule	Key provisions	Impact/implication	Cross-reference
First Schedule	Consent manager registration conditions (INR 2 crore net worth, certification, integrity standards). Obligations include consent enablement, record maintenance, security safeguards, transparency, and audits.	Organisations planning to act as consent managers must meet stringent financial and technical criteria. Internal consent management solutions should align for interoperability.	Rule 4; Section 6(7)-(9) DPDPA 2023
Second Schedule	Standards for state processing (Rule 5) and research/statistical processing (Rule 16): proportionality, purpose limitation, minimisation, security, accuracy, retention, accountability.	Public sector and research entities must adopt strict governance and security measures.	Rule 5 & 16; Section 7, 17(2)(b) DPDPA 2023
Third Schedule	Retention periods: 3 years for user account access, 3 years for virtual token transactions, delivery + support period for services, and periods specified by law.	Retention schedules must incorporate DPDP timelines and legal exceptions. No deletion within first year due to mandatory log retention; erasure requests during this period cannot be honoured.	Rule 8; Section 8(7)-(8) DPDPA 2023
Fourth Schedule	Exemptions for child data processing: specified fiduciaries and purposes exempt from verifiable consent, subject to child protection safeguards.	Simplifies compliance for certain fiduciaries but requires robust child safety measures.	Rule 10; Section 9 DPDPA 2023
Fifth Schedule	Board chairperson and member compensation: salary, allowances, tenure, removal provisions, retirement benefits.	Reinforces governance and independence of the Data Protection Board.	Sections 19-21 DPDPA 2023
Sixth Schedule	Board officers and employees' appointment terms: recruitment, qualifications, pay scales, service rules, promotion, disciplinary procedures, retirement.	Ensures professional and transparent staffing for Board operations.	Section 24 DPDPA 2023
Seventh Schedule	Purposes for Central Government information requests and authorised persons (to be notified by Central Government).	Organisations must prepare for lawful government requests and implement confidentiality safeguards.	Rule 23; Sections 36-37 DPDPA 2023

Conclusion

The DPDP Act makes privacy compliance a core business priority and strengthens customer trust. The 2025 Rules set clear obligations: improve data security, update notices and consent, and ensure timely breach notifications. Organisations must keep logs for at least a year, review data mapping, and provide grievance redressal within 90 days. Significant DFs will need annual impact assessments, audits, and algorithm risk checks once notified. Privacy notices should be accessible and multilingual where required. Continuous compliance, planning, and monitoring will be critical through 2027–2028.

For more details on what the DPDPA means for your business. Please contact:

Dinesh Anand
Partner and ESG & Risk Consulting Leader
Grant Thornton Bharat
E: dinesh.anand@in.gt.com

Akshay Garkel
Partner and Cyber Monitoring & Response Leader
Grant Thornton Bharat
E: akshay.garkel@in.gt.com

Vivek Iyer
Partner and Financial Services Risk Advisory Leader
Grant Thornton Bharat
E: vivek.iyer@in.gt.com

Jaspreet Singh
Partner and Cyber Assurance & Governance Leader
Grant Thornton Bharat
E: jaspreet.singh2@in.gt.com

Rohit Das
Partner, Cyber Assurance & Governance
Grant Thornton Bharat
E: rohit.das@in.gt.com

Kush Wadhwa
Partner, Cyber Monitoring & Response
Grant Thornton Bharat
E: kush.wadhwa@in.gt.com

Kartikeya Raman
Associate Partner
Grant Thornton Bharat
E: kartikeya.raman@in.gt.com

We are
Shaping Vibrant Bharat

A member of Grant Thornton International Ltd., Grant Thornton Bharat is at the forefront of helping reshape the values in the profession. We are helping shape various industry ecosystems through our work across Assurance, Tax, Risk, Transactions, Technology and Consulting, and are going beyond to shape a more **#VibrantBharat.**

Our offices in India

● Ahmedabad ● Bengaluru ● Chandigarh ● Chennai ● Dehradun
● Gandhinagar ● Goa ● Gurugram ● Hyderabad ● Indore ● Kochi
● Kolkata ● Mumbai ● New Delhi ● Noida ● Pune

Scan QR code to see our office addresses

www.grantthornton.in

Connect with us on

@Grant-Thornton-Bharat-LLP
@GrantThorntonBharat
@GrantThornton_Bharat
@GrantThorntonIN
@GrantThorntonBharatLLP
GTBharat@in.gt.com