

NEWSFLASH

Digital Personal Data Protection Rules, 2025 Notified

Background

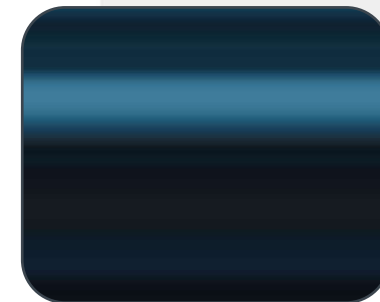
The Digital Personal Data Protection Rules, 2025, notified on 13 November 2025, turn the 2023 Act into clear, actionable obligations for anyone handling digital personal data. This framework is India's key legal standard for governing how such data is collected, used and protected. It applies to any organization acting as a Data Fiduciary when processing the personal data of individuals or Data Principals while offering goods or services in India.

The Rules spell out what organizations must put in place, how those measures should work in practice and the level of accountability expected. Controls like encryption, masking, backups and strict access governance are no longer optional—they are legal requirements.

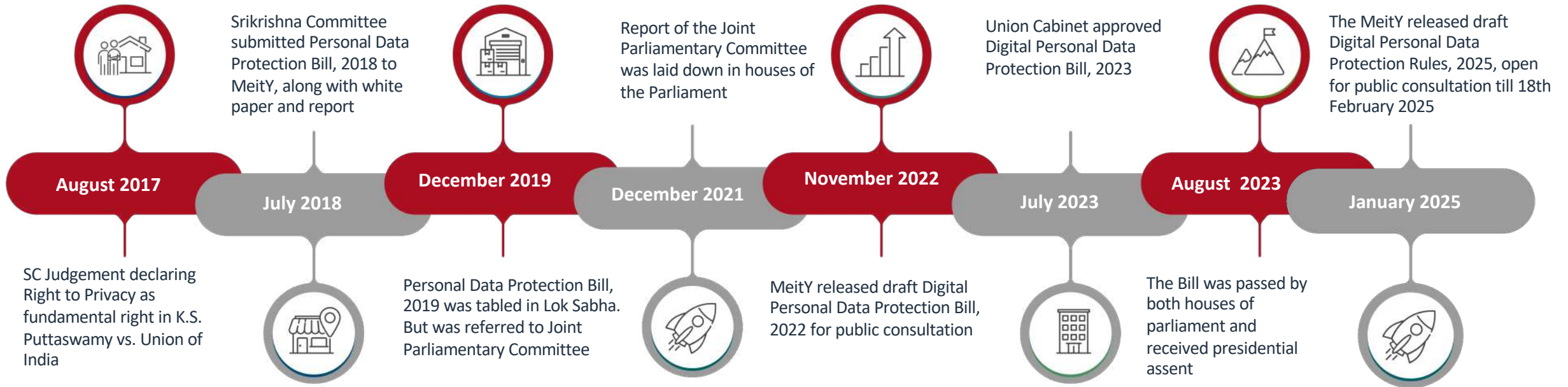
The transition is structured in phases so organizations can move steadily from basic alignment to complete operational readiness. The target is full compliance within 18 months, with all mandated safeguards, processes and accountability mechanisms functioning as required.

Why this matters

This law reshapes how digital operations must run in India. Compliance is essential for two reasons. First, it is a legal obligation, backed by substantial penalties for failing to meet requirements around consent, security and data handling. Second, it strengthens trust. Clear privacy notices and rights such as access and erasure give Data Principals more control, helping organizations build credibility and transparency in a competitive digital market.



Evolution



DPDP Implementation Timeline

Phase	Timeline	Strategic Focus & Outcomes
Phase 1: Immediate	Effective November 2025	Governance & Foundation: Establishing core administrative functions, definitions, and initiating the operating procedures for the regulatory Board.
Phase 2: One Year Milestone	Effective November 2026	Consent Management Ecosystem: Preparing for API-based integration, aligning workflows with the regulatory standards for Consent Managers, and enabling centralized consent management for Data Principals.
Phase 3: Full Operational Control	Effective May 2027 (18 Months)	Operational Control: Mandatory activation of all core data fiduciary obligations: notices, verifiable consent, security safeguards, breach notifications, data retention, and SDF duties.

Phase 1 - Immediate Mandatory Action (Effective from Nov 2025)

Rule	Requirement Summary	Action Plan
DPBI Establishment (Rules 17-21)	The Data Protection Board of India (DPBI) is established as the digital-first regulator, overseeing compliance and imposing penalties.	Establish internal Governance Roles (Grievance Officer, etc.) and ensure internal reporting lines are prepared for digital communication with the Board.
Designated Contact (Act Sec 13)	Duty to publish contact details of the Grievance Officer or equivalent person.	Publish clear contact details on your website and privacy policy immediately.
Definitions (Rule 2)	Establishes core definitions like Verifiable Consent and User Account.	Conduct initial readiness groundwork and update internal legal documentation with the new DPDP terminology.

Phase 2: One Year Milestone (By November 2026)

Area	Requirement Summary	Action Plan
Consent Manager (CM) (Rule 4)	Establishes the registration, technical, and operational standards for CMs -entities that manage user consent on behalf of the Data Principal.	API Integration: Plan, develop, and test APIs to enable seamless, real-time integration with registered CMs to facilitate user consent giving, management, and withdrawal.
Record Retention (Rule 4)	Consent Managers must maintain a record of all consent interactions for a period of seven years.	Conduct an operational impact analysis to align your systems for accepting and logging consent status from the new CM infrastructure.

Phase 3: 18 Months Milestone (By May 2027)

Area	Requirement Summary	Action Plan
Notice & Consent (Rule 3)	Privacy Notices must be clear, standalone, purpose-specific, include rights, withdrawal mechanisms, and grievance contact.	Rewrite Notices: Redesign privacy notices across all touchpoints (website, apps, forms) to be understandable, multi-lingual, and explicit about the purpose of data collection.
Security Safeguards (Rule 6)	Mandates the implementation of Reasonable Security Safeguards (T&O measures), including encryption, masking, access controls, IAM, and comprehensive logging.	Conduct a comprehensive Security Gap Assessment and implement required technical controls to ensure data security is provable, not optional.
Breach Notification (Rule 7, 8)	Notification of the DPBI and affected Data Principals "without delay." A detailed report is required to the Board within 72 hours.	Establish and test a robust breach response process, including pre-approved communication templates and a detailed stakeholder matrix for rapid deployment.
Data Principal Rights (Rule 9-14)	Full activation of rights: Access, Correction, Erasure, Grievance Redressal (with 90-day response timeline), and Right to Nominate.	Implement processes and technology to honor all Data Principal rights requests efficiently and within the statutory 90-day timeline.
Children's Data (Rule 12)	Requires Verifiable Parental Consent (VPC) before processing data of a minor. Targeted advertising is banned.	Implement robust age-gating and identity verification technical measures (e.g., using Digital Locker or virtual tokens) for VPC compliance.
Data Retention (Rule 10)	Personal data must be erased once the purpose of processing is fulfilled (purpose limitation).	Rethink and update retention policies and automate deletion workflows for all personal data once the specified purpose is complete.

Responsibility of Data Fiduciary

1.

A Significant Data Fiduciaries (SDF) must carry out due-diligence on any automated or algorithm-driven system used for processing personal data

2.

Conduct a DPIA and an annual audit each year, with the results formally submitted to the Board by the individual responsible for the assessment.

3.

Implement the mandated safeguards to process Central Government – identified personal and traffic data in line with specified restrictions, ensuring it is not moved outside India.

A. The Burden of Proof (Act Sec 6(10))

The DPDP Act places the burden of proof squarely on the Data Fiduciary.

Principle: When consent is the legal basis for processing, the Data Fiduciary must prove that the Notice was given and valid, compliant consent was obtained.

Action: Implement an Audit Trail and Logging System to record the exact time, method, notice version, and scope of every consent received. This evidence must be auditable and maintained for regulatory review.

B. Significant Data Fiduciaries (SDF) (Rule 11)

Organizations notified as SDFs due to the volume, sensitivity, or risk of their processing face extra duties.

Additional Duties: SDFs must appoint a Data Protection Officer (DPO) and conduct mandatory Annual Data Protection Impact Assessments (DPIAs) and Annual Audits.

Action: If you meet the criteria (or are likely to be designated), immediately initiate DPIA and audit preparation and allocate budget for a dedicated DPO role.

Key Highlights

Obligations	Rule reference	Timeline in hours
Breach Reporting	Rule 7(1) and 7(2)	E-commerce, social media and gaming platforms must erase personal data after a fixed retention period of three years. They also need to notify users 48 hours before the deletion happens.
Personal Data Erasure	Rule 8(2), Third Schedule	E-commerce, social media and gaming platforms must erase personal data after a fixed retention period of three years. They also need to notify users 48 hours before the deletion happens.
DPIA and Data Audit Frequency	Rule 12(1)	These assessments must be carried out every year starting from 13 November 2025. The date on which DPDP Rules was notified or the date an organization is classified as a Significant Data Fiduciary.
Consent Record Retention	First Schedule, Part B, 4(c)	Consent managers must maintain consent logs for seven years.
Grievance Redressal	Rule 14(3)	Responses to Data Principal grievances must be provided within 90 days.

Penalties for Non-Compliance

The DPDP Act includes provisions for significant financial penalties, designed to enforce compliance. Penalties can range up to ₹250 crore for non-compliance with requirements like failing to implement reasonable security safeguards, violating data principal rights or failing to report a breach.

Breach Intimation Requirements:

- Primary Intimation to the DPB - Must be sent *without delay* once the Data Fiduciary becomes aware of the breach (What happened — nature, extent, likely impact with details of when and where it occurred).
- Secondary Intimation to the DPB - Must be filed *within 72 hours* (or within an extended period approved by the DPB) - Updated details from the first report (Root cause analysis report with all the details)
- Intimation to Data Principals - Must also be issued *without delay* once the breach is known. Combine details from first two points and impact on data principals.

Exceptions: Children Personal Data

Scenario	Details
Processing children's personal data	<ul style="list-style-type: none">• Healthcare facilities and professionals involved in medical or therapeutic care• Allied health services such as diagnostics or clinical support• Schools, colleges and institutions that manage student information• Caregivers and operators of daycare facilities• Service providers responsible for transporting school or day-care children
Scenario were children's data may be processed without consent	<ul style="list-style-type: none">• Carrying out legal duties intended to safeguard or support a child• Delivering government-backed services, benefits, permits or certifications that rely on personal data• Creating communication accounts (such as email IDs) for authorized use• Determining a child's live location when needed for safety or tracing• Restricting or blocking material that could harm a child's wellbeing

Cross-Border Data Transfer under DPDP (Rule 15)

What Organizations Must Do by May 2027

Any organization transferring Indian personal data outside the country needs to ensure its systems, contracts and safeguards meet DPDP expectations. Key tasks include:

Requirements	Responsibility
Map global data flows	Create a complete inventory showing where Indian personal data is stored, processed and transferred, including cloud setups and vendor networks.(Rule 15)
Strengthen contractual protections	Update all cross-border DPAs to ensure overseas processors follow DPDP requirements, especially the security controls listed in Rule 6.(Rule 6, Rule 15)
Match security standards overseas	The foreign recipient must apply the same level of protection required in India—encryption, role-based access, breach reporting and other Reasonable Security Safeguards.(Rule 6)
Track government notifications	Put a monitoring process in place to catch any update from the government announcing restricted countries.(Rule 15)
Document accountability	Keep clear records of the legal basis for every transfer, whether consent or legitimate use. The Data Fiduciary must be able to prove compliance even when data moves outside India

Our Locations

NOIDA

(Delhi NCR - Corporate Office) A-109,
Sector - 136, Noida - 201304, India
T: +91 120 2598000

CHENNAI

Prestige Palladium Bayan,
Level 5, 129-140, Greams Road,
Thousand Lights, Chennai - 600006
T: +91 44 46549201

HYDERABAD

25, 4th Floor, Veer Chambers,
Door No: 1/10/63/1/1, Opposite Shoppers
Stop, Old Patigadda, Chikoti Gardens,
Begumpet, Hyderabad, Telangana - 500016

DELHI

(Registered Office) B-27, Soami Nagar,
New Delhi - 110017, India
T: +91 120 2598000

BENGALURU

Prestige Obelisk, Level 4, No 3 Kasturba
Road, Bengaluru - 560 001,
Karnataka, India
T: +91 80 2248 4555

GURUGRAM

001-005, Emaar Digital Greens Tower-
A 10th Floor, Golf Course Extension
Road, Sector 61, Gurugram - 122102
T: +91 0124 430 1551

PUNE

3rd Floor, IndiQube Park Plaza, CTS
1085, Ganeshkhind Road, Next to
Reliance Centro Mall, Shivajinagar,
Pune - 411005, India

MUMBAI

4th Floor, Iconic Tower, URMI Estate,
Ganpat Rao Kadam Marg, Lower Parel,
Mumbai - 400013, India
T : +91 22 4474 3400

DEHRADUN

1st Floor, "IDA" 46 E.C. Road, Dehradun -
248001, Uttarakhand, India
T: +91 135 271 6300

www.nangia.com | query@nangia.com