Privacy Regime Rejig: What Lies Ahead?

India's comprehensive framework for responsible use of personal data

Lex Fulcrum
Advocates and Solicitors

www.lexfulcrum.com

This guide highlights the key aspects of India's data privacy regulations and outlines core compliance actions businesses must undertake to ensure robust and timely implementation.

THE JOURNEY BEGINS

India's New Data Protection Era: Act & Rules

The **Digital Personal Data Protection Act, 2023** and **Digital Personal Data Protection Rules, 2025** establish India's comprehensive framework for the responsible use of personal data.

The legislation seeks to strike a **careful balance** between **safeguarding individual rights** and enabling **lawful, purpose-driven data processing by businesses** to foster **innovation** and accelerate **economic growth**.

The Act has already been set in motion and is being implemented in a phased manner over a period of **18 months (starting from 13 November 2025)**, while the Government is considering to shorten this timeline for big technology companies.

This staggered rollout is intended to facilitate the creation of the foundational institutional infrastructure and administrative machinery required for effective enforcement, while simultaneously allowing businesses adequate time to adjust their systems and adopt responsible data practices.

Once fully operational, the law will regulate the entire lifecycle of personal data, and change the way businesses process personal data.

While considerable discourse has emerged on its adoption, it is imperative to re-emphasise what lies ahead and how businesses must proactively prepare to navigate the evolving regulatory landscape, build future-ready systems, and ensure sustained compliance.

The compliance clock has already begun to run.

IMPLEMENTATION ROADMAP

Phased Implementation Timeline

13 November 2025

Provisions relating to establishment of Data Protection Board of India and procedural framework made effective

13 November 2026

Provisions relating to Consent Manager's registration and obligations will be effective

13 May 2027

Full Implementation - compliance of all provisions will be required

GOVERNMENT IS CONSIDERING TO SHORTEN THIS TIMELINE FOR BIG TECHNOLOGY COMPANIES (Potential Significant Data Fiduciaries)

FOUNDATIONAL CONCEPTS

Key Terms You Must Know

Personal Data

Any data about an individual who is identifiable by or in relation to such data

Collected in digital form (or non-digital form and digitised later)

Data Fiduciary

Any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data

Data Processor

Any person who processes personal data on behalf of a Data Fiduciary

Data Principal

The individual to whom the personal data relates

Significant Data Fiduciary

Data Fiduciary to be notified by Central Government which will have enhanced obligations and restrictions

Consent Manager

An entity that provides a single, transparent and interoperable platform through which a Data Principal may give, manage, review or withdraw consent

The Personal Data Lifecycle

Compliance obligations apply at every stage starting from collection to erasure

Notice

Clear disclosure in plain language

Consent

Free, specific, informed

(Verifiable consent of parent/lawful guardian in case of children & persons with disability)

Processing

Consent-driven, lawful purpose-limited use

Sharing/transfer

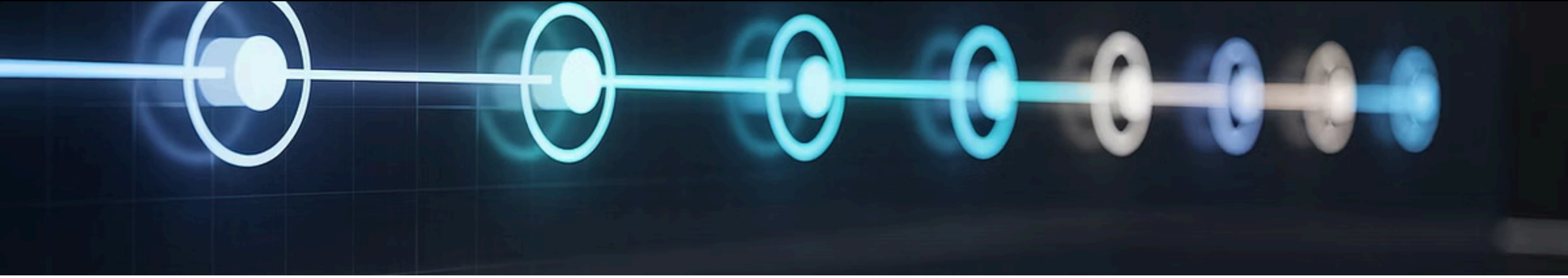
Based on consent and subject to compliance and restrictions

Storage

Secure, limited retention

Erasure

Timely deletion when no longer needed, consent is withdrawn or upon data principal's request



Core Compliance Principles

1

Data Minimisation

Collect only what's necessary for the stated purpose - no more, no less

2

Purpose Limitation

Use data strictly for stated lawful purpose and consented to by Data Principals

3

Consent driven processing & Transparency

Process data only with consent except for legitimate uses, and ensure transparency which is paramount.

OBLIGATIONS FRAMEWORK

Data Fiduciary Responsibilities

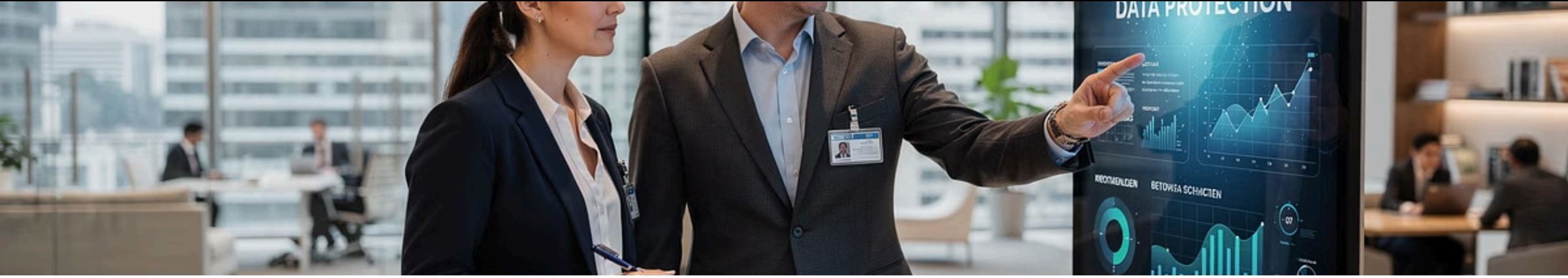
Standard Data Fiduciaries

- Provide clear notices and obtain consent
- Enable consent withdrawal
- consent driven processing
- Implement reasonable security safeguards
- Appoint designated officer as point of contact
- Establish grievance redressal mechanism
- Notify breaches promptly
- May engage registered Consent Manager

Significant Data Fiduciaries (SDFs)

Enhanced obligations include:

- Appoint Data Protection Officer under valid contract
- Conduct Data Protection Impact Assessments
- Periodic independent audits mandatory
- Due Diligence of technical measures
- Data localisation (as may be notified)



Empowering Data Principals

Right to Know

Understand what data has been collected and how it is being used

Right to Access

Access personal data held by Data Fiduciaries

Right to Correct

Update inaccurate or incomplete personal data

Right to Erasure

Request deletion when data no longer serves its purpose

For the first time, Data Principals also have **duties** - failure to comply may result in penalties

ENFORCEMENT & OVERSIGHT

Regulatory Architecture

Data Protection Board of India

Independent body overseeing compliance, investigating breaches, ensuring corrective action

Appellate Tribunal

Adjudicates appeals against Board's decisions

Supreme Court

Final appellate authority

The Cost of Non-Compliance

Financial penalties reflect the severity of violations - robust safeguards are non-negotiable

Security Safeguards Breach

Failure to implement reasonable security safeguards to protect personal data

Upto **₹250Cr**

Breach Notification/ Children's Data

Failure to notify Board and affected Data Principals of breaches/ Violations relating to processing of personal data of children

Upto **₹200Cr**

SDFs Violations

Non-compliance with Significant Data Fiduciary-specific enhanced obligations

upto **₹150Cr**

General Breaches

Failure to provide notice, obtain valid consent, honour Data Principal rights or other breaches

Upto **₹50Cr**

Data Principal Duty

Penalty for non-fulfilment of duties by Data Principals

Upto **₹10,000**

Key Actions for Full Implementation (13 May 2027)

As the full implementation date approaches, proactive measures are essential to ensure comprehensive compliance.

Clear Notice

Provide notices detailing data purpose, processing, rights, and grievance redressal.

Transparency is paramount.

Fresh Consent for Existing Data

Issue DPDP-compliant notices to re-obtain consent from Data Principals whose data was collected prior to the Act's commencement.

Processing may continue unless consent is withdrawn.

Multilingual Notice Option

Data Fiduciaries must offer Data Principals the option to access notices in English or any Scheduled regional language.

Valid Consent Protocol

Obtain free, specific, informed, unambiguous consent with opt-in by clear affirmative action by Data Principals.

Easy Consent Withdrawal

Ensure withdrawing consent by Data Principals is as straightforward and accessible as providing it.

Accessible Privacy Policy

Maintain a DPDP-compliant, easy-to-understand, and publicly accessible privacy policy.

Key Actions for Full Implementation (13 May 2027)

As the full implementation date approaches, proactive measures are essential to ensure comprehensive compliance.

Consent-Driven Processing

Strictly adhere to consent-driven data processing, ensuring no personal data is processed without valid consent (unless legally permitted).

Implement Robust Security

Deploy technical & organizational safeguards including encryption, control access, appropriate logs, monitoring and review for early detection of breach and remediation.

Data Processor Contracts

Formulate robust contracts with Data Processors, ensuring their compliance with DPDP obligations and detailing obligations and remedies.

Strengthen Grievance Redressal

Establish effective and timely mechanisms for Data Principal grievances, using feedback to improve systems.

Vendor/Third-Party Contracts

Update all existing and new agreements with vendors and third parties to fully reflect DPDP obligations.

HR Policy Alignment

Review and update internal employment policies and contracts to ensure complete alignment with DPDP requirements.

Key Actions for Full Implementation (13 May 2027)

As the full implementation date approaches, proactive measures are essential to ensure comprehensive compliance.

Appoint Designated Officer/ Point of Contact

Designate a clear point of contact for all Data Principal queries and concerns regarding personal data and her rights.

Appoint Data Protection Officer (SDFs)

Mandatory for Significant Data Fiduciaries, ensuring expert oversight under a valid contractual agreement.

Appoint Consent Manager

Data Fiduciaries may appoint a registered Consent Manager and must establish clear contractual terms for effective consent management.

Conduct DPIAs (SDFs)

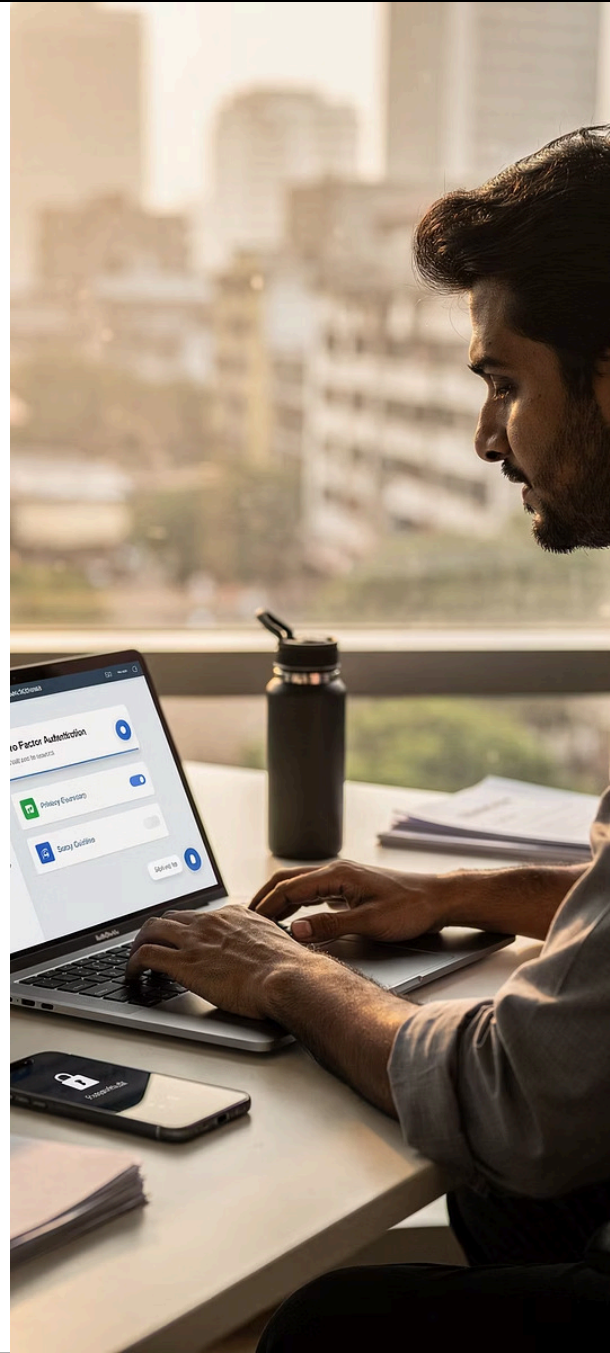
Significant Data Fiduciaries must perform annual Data Protection Impact Assessments and provide report to the Board.

Regular Audits (SDFs)

Significant Data Fiduciaries must ensure periodic audit by independent auditor and provide report to the Board.

Due Diligence (SDFs)

Significant Data Fiduciaries must conduct due diligence to ensure that their technical measures processing data do not pose risk to data principals' rights.



OPERATIONAL EXCELLENCE: GOING DEEPER

Further Operational Imperatives

Maintaining compliance requires a continuous commitment to these foundational principles and operational practices.

Purpose Limitation

Process data strictly for specific purpose consented to by Data Principal, ensuring alignment with expressed intent.

Data Minimisation

Collect and process only such personal data that is absolutely necessary and directly relevant to the stated purpose.

Data Updation & Access

Respond to Data Principal requests for access, correction, updating, or erasure of personal data.

Data Erasure

Erase data when consent is withdrawn, purpose is fulfilled or upon data principal's request unless required to be retained as per law.

Records Management

Maintain accurate records of all data processing activities in the prescribed manner and for the required duration.

Vulnerable Data Principals

Obtain verifiable consent when processing personal data of children and persons with disabilities, and implement stringent processing restrictions and security measures.

Breach Notification

Notify the Board and affected Data Principals without delay, explaining breach, impact and remediation steps.

Cross-Border Data Transfers

Adhere to government-notified restrictions for transfers of personal data outside India.

Data Localisation (SDFs)

Significant Data Fiduciaries must ensure that Government identified personal data is not transferred outside India.

Building a Culture of Compliance

Periodic Training & Awareness

Conduct regular awareness and training sessions on data handling, breach reporting, and other DPDP obligations for all employees

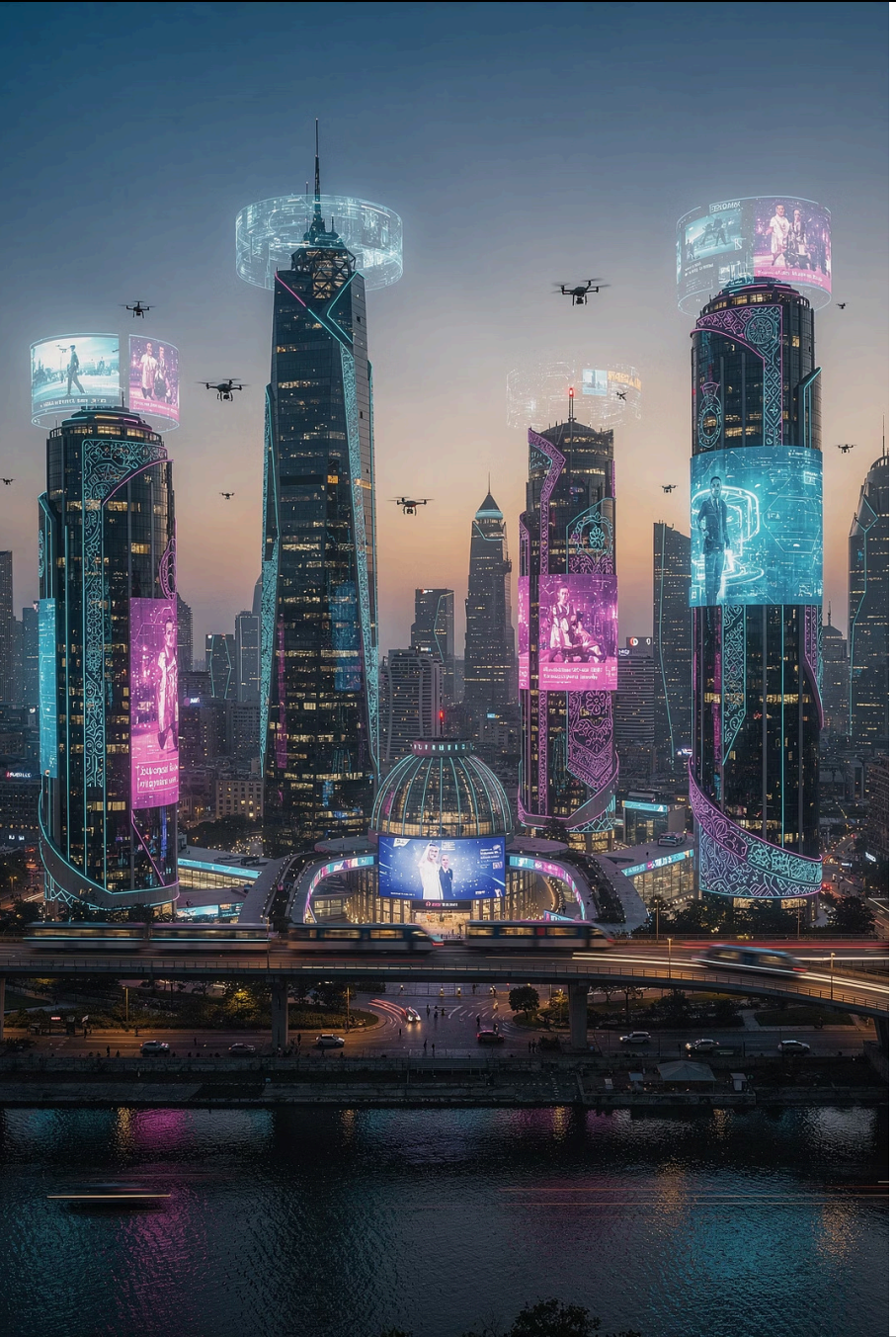
Global Alignment

Harmonise with GDPR and other international frameworks where applicable for smooth global operations

Sectoral Compliance

DPDP intersects with RBI, SEBI, IRDAI, TRAI, MeitY regulations - ensure multi-layered compliance

Compliance is not a one-time exercise - it's an ongoing commitment to responsible data processing



Ready to Navigate the New Regime?

The DPDP Act represents a transformative shift in how businesses collect, process, and protect personal data in India. With the compliance clock running, proactive preparation is essential to build future-ready systems, ensure sustained compliance, and maintain stakeholder trust.

> The journey toward responsible data practices begins now—strategic action today ensures regulatory readiness tomorrow.

For further assistance, please write to
vinita.sahitya@lexfulcrum.com