January 28

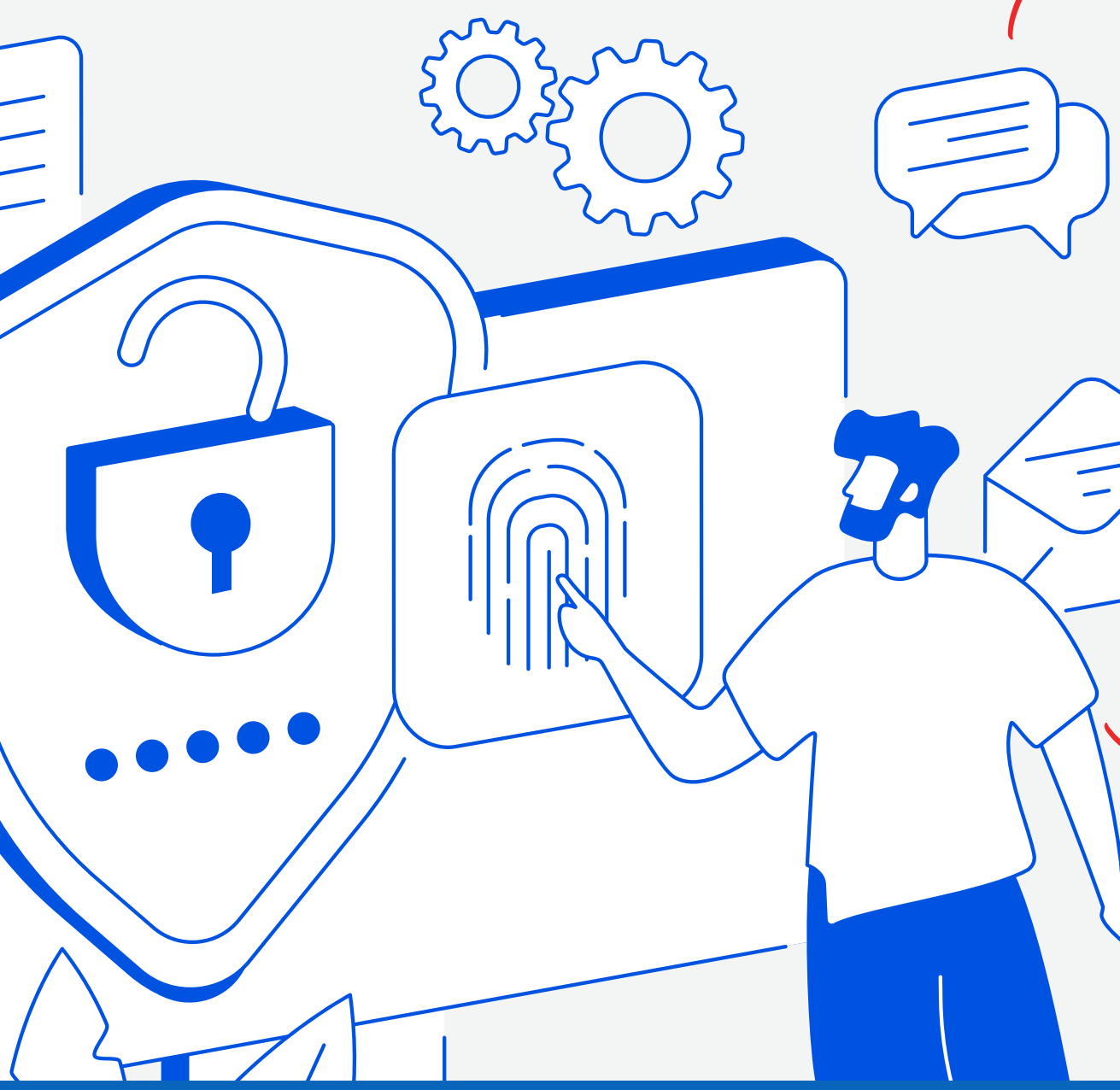
Data Protection Day

India's DPDP Regime at a Glance

Every year on January 28th, the world observes **Data Protection Day**, a day dedicated to raising awareness about the importance of data privacy and the protection of personal information in an increasingly digital world. In line with this global observance, India has taken significant strides toward safeguarding personal data with the enactment of the **Digital Personal Data Protection Act, 2023 (DPDP Act)**.

The Digital Personal Data Protection Act, 2023 (DPDP Act) and **the Digital Personal Data Protection Rules, 2025 (DPDP Rules)** released in phases with rules being released on **November 13, 2025,** provide crucial clarification to India's regulatory framework. With this official activation, India's new privacy framework is formally introduced and a mandated compliance roadmap for Data Fiduciaries is established.

This post explains: -



- What the DPDP Act and Rules are
- How it applies to companies
- Its compliance scope
- Key obligations in a simplified and business –friendly manner

Brief Overview of the DPDP Act, 2023

The DPDP Act, 2023 and the DPDP rules 2025 governs the **processing of digital personal data** in India and applies to: - Personal data collected in digital form, or Non-digital data that is later digitised.

The law is principle-based and focuses on:

Consent-driven data processing

Accountability of data fiduciaries

Protection of individual rights

Strong penalties for non-compliance

Who Does the Act Apply To?

The DPDP Act applies to:

Entity	Applicability
Companies	Applicable
LLPs	Applicable
Startups	Applicable
E-commerce platforms	Applicable
Fintech, Health-tech, Ed-tech	Applicable
Employers handling employee data	Applicable
Foreign entities offering goods/services in India	Applicable

Even a small website collecting email IDs or phone numbers is covered.

Key Concepts Under the DPDP Act

Term	Meaning
Data Principal	Individual whose personal data is processed
Data Fiduciary	Entity determining purpose & means of processing
Data Processor	Entity processing data on behalf of fiduciary
Consent Manager	Platform enabling consent management
Significant Data Fiduciary (SDF)	Entity notified by Government due to scale/sensitivity

Commencement Timeline – DPDP Act and DPDP Rules, 2025

Commencement of Act

- Section 1(2), section 2, sections 18 to 26 sections 35, 38, 39, 40, 41, 42, 43, and Section 44(1) & (3) : **effective from 13-11- 2025**

- Section 6(9) and Section 27(1)(d): effective from **13-11-2026 (1 year/12 months from the date of notification).**

- sections 3 to 5,Section 8(1) and Section 6(10),sections 7 to 10, sections 11 to 17, section 27 (a) to (c) and (e), sections 28 to 34, 36, 37 and 44(2): **effective from 13-5-2027 (18 months from the date of notification)**

Commencement of Rules

- Rules 1, 2, and 17 - 21: **effective from 13-11- 2025**
- Rule 4: effective from**13-11-2026 (1 year/12 months from the date of notification).**
- Rules 3, 5 - 16, 22 - 23: **effective from 13-5-2027 (18 months from the date of notification)**

Core Obligations of Companies under DPDP Act& Rules

1. Lawful Purpose Limitation

Personal data must be collected for a **lawful purpose** and Used **only for the purpose communicated.** No excessive or unnecessary data collection is permitted.

2. Consent-Based Processing

Companies must provide **consent notices in simple language**explaining: - What data is collected - Why it is collected - How long it will be retained - How consent can be withdrawn

3. Notice Requirement

Before collecting data, companies must issue a **Data Protection Notice** containing: - Description of personal data - Purpose of processing - Rights of data principal - Grievance redressal mechanism

4. Data Principal Rights

Individuals have the right to:

Right	Description
Right to Access	Obtain summary of personal data
Right to Correction	Update inaccurate data
Right to Erasure	Delete data once purpose is met
Right to Grievance Redressal	Raise complaints
Right to Nominate	Nominate another person

Companies must create internal mechanisms to respond to these requests.

5. Reasonable Security Safeguards

Companies must: - Implement technical & organisational safeguards - Prevent data breaches - Ensure confidentiality and integrity of personal data

6. Data Breach Reporting

In case of personal data breach: - Immediate intimation to the Data Protection Board - Communication to affected individuals***within 72 hours*** of becoming aware on a description of the breach, including its nature, extent, timing and location ofoccurrence and the likely impact

Failure to report may lead to heavy penalties.

7. Data Retention & Deletion

Personal data must be: - Retained only till the purpose is fulfilled - Deleted once no longer required

Data Fiduciary shall at ***least forty-eight hours before completion of the time period for erasure of personal datainform*** the Data Principal that such personal data shall be erased uponcompletion of such period

“Store forever” practices are no longer legally acceptable. “

8. Obligations of Data Processors

Where companies outsource: - Payroll - Cloud storage - CRM - IT support

They must ensure processors: -

1. Act only on instructions
2. Maintain security safeguards
3. Do not use data independently.
4. Strong **Data Processing Agreements (DPAs)** become mandatory.

Significant Data Fiduciaries (SDF)

Entities may be notified as SDFs based on: - Volume of data processed - Sensitivity of personal data - Risk to data principals

Additional obligations include: - Appointment of Data Protection Officer (DPO) - Independent data audits - DPIA (Data Protection Impact Assessment)

Penalties Under DPDP Act

Non-Compliance	Penalty
Data breach under Section 8 (5)	Up to ₹250 Crores
Failure to safeguard data under Section 8(6)	Up to ₹250 Crores
Violation of consent under section 9	Up to ₹200 Crores
Non-fulfilment of obligations	Significant monetary fines

Penalties are adjudicated by the **Data Protection Board of India**.

The DPDP Act's punishment mechanism is intended to encourage behavioral change, advance privacy-first governance, and guarantee that businesses incorporate data protection into their regular operations in addition to punishing. To emphasize the significance of data privacy and Act compliance, the punishment under this Act is severe.

Wider Scope & Business Impact

The DPDP Act impacts: - Corporate governance - IT infrastructure - Vendor contracts - HR data management - Marketing & customer analytics - Compliance frameworks

It pushes companies towards:

- Privacy-by-design
- Strong documentation
- Internal accountability

Key Takeaway for Companies

- DPDP compliance is **not optional**
- Applies irrespective of company size
- Documentation is as important as technology
- Non-compliance has reputational + financial risks

📢Conclusion

The Digital Personal Data Protection Act, 2023 marks a **paradigm shift in how Indian businesses handle personal data**. Companies must move from informal data practices to structured compliance frameworks.

Those who adapt early will not only avoid penalties but also build **consumer trust, transparency and long-term sustainability**.