PrivacyPillar

Indian DPDPA Compliance Playbook: Starter Guide

November 2025

The Digital Personal Data Protection Act 2023 (DPDPA)

The DPDPA 2023 marks the beginning of India's data protection era. It underscores the responsibility of organisations to safeguard digital personal data while preserving individuals' right to privacy and freedom.

Journey Until Now

- **2017 -** Supreme Court recognizes privacy as a fundamental right
- **2018 -** Justice B.N. Srikrishna Committee report and draft bill
- **2019 -** First official Personal Data Protection Bill introduced and later withdrawn
- **2022 -** Digital Personal Data Protection Bill, 2022 released for public consultation
- **2023 -** Bill passed by Parliament and received Presidential assent; becomes DPDPA Act
- **2024 -** DPDPA enforcement delayed, rules pending
- **2025 -** Final Digital Personal Data Protection Rules prepared for notification

Establishes the roles of Data Principal, Data Fiduciary, Significant Data Fiduciary and Consent Manager.

Data Principal
Individual whose personal data is processed.

Data Fiduciary
Entity controlling data processing purpose and means.

Significant Data Fiduciary
High-risk fiduciary with extra obligations.

Consent Manager
Registered intermediary managing user data consent.

Rights of Data Principals

Right to access personal data
Know data processed and shared

Right to withdraw consent
Revoke data processing permission anytime

Right to grievance redressal
File complaints for violations or issues

Right to erasure
Delete data when consent withdrawn

Right to correction
Fix inaccurate or incomplete data

Right to nominate
Appoint representative for data principal rights

Financial penalties up to

INR 250 crore

per instance

1. What is consent under the DPDP Act?

Consent must be free, specific, informed, unconditional and unambiguous with a clear affirmative action.

2. What are the obligations of data fiduciaries?

Secure data processing and, consent, data principal rights, breach & retention management.

3. What is the role of Consent Managers?

Registered entities facilitating transparent consent management between data principals and fiduciaries.

4. How are children's data protected?

Verifiable parental/guardian consent is mandatory for processing children's personal data.

5. What categories of personal data are protected?

The Act does not explicitly categorize personal data further, based on criticality, sensitivity, or nature of the data.

6. What is the definition of a data fiduciary?

Any person or entity deciding the purpose and means of personal data processing.

Certain Legitimate Uses to Process Data

No distinct consent is needed for specific "legitimate uses" permitted under the Act. These cover situations where data is either voluntarily shared or collected to meet a legal requirement. A privacy notice is also not required for such legitimate uses.

Scenarios covered under Legitimate Uses

- *Data processed **voluntarily** by Data Principal without objection.*
- *Data processed by **State** to provide government benefits.*
- *Processing for **national security** and public order.*
- *Processing required to comply with **legal obligations.***
- ***Medical emergencies** allow processing without prior consent.*
- ***Disaster situations** permit data use for safety.*
- *For purpose related to **employment** to protect employer interests.*

Table of Contents

1 - Introduction

1.1 - Why This Playbook?

India's **Digital Personal Data Protection Act, 2023 ('DPDPA')** represents shift in India's digital governance. For years, personal data protection was governed by fragmented rules under Information Technology Act, 2000 and scattered sectoral laws. The DPDPA consolidates these under a single statue, establishes a dedicated regulatory authority, defines rights for data principals and introduces accountability and compliance obligations that organisations must incorporate.

This playbook has been developed to bridge law and practice. While the Act outlines broad legal duties, its practical implementation requires organisations to interpret obligations in the context of business workflows, IT systems, and customer interactions. By blending statutory references with detailed operational strategies and industry-specific use cases, the playbook equips organisations with real and actionable insights.

Above all, this playbook emphasises that compliance should not be seen as a mere legal checkbox. If done right, DPDPA compliance could become a strategic differentiator and a trust advantage in a highly competitive Indian market.

1.2 - Who Should Use This Playbook?

This playbook is **designed for the following audience:**

MNCs & Large Enterprises

Adapt the existing global privacy framework to the specific DPDPA compliance requirements.

Senior Leadership

Approach DPDPA compliance strategically, establish governance mechanism, ensure cross-functional coordination.

SMEs & Startups

Initiate their DPDPA compliance journey by embedding privacy-by-design early and adopting proportionate controls to manage regulatory risks with scaling business.

Legal & Compliance Verticals

Interpret DPDPA obligations, develop policies and procedures, strengthen third-party contracts.

By offering practical guidance, the playbook enables organizations to understand their roles and approach the DPDPA compliance journey with practical steps and strategies.

1.3 - Scope Of This Playbook

This playbook is designed to serve as both a reference guide and a practical handbook, however, it could not be deemed as legal advice and, is purely documented to assist the audience in interpreting the compliance requirements and its subsequent considerations under the Act. The Case Studies highlighted under the respective sections of this playbook are illustrative in nature and not based on any real scenario.

Each section blends statutory references with explanatory detail, checklists, and use cases. The aim is not only to inform you what the law requires but also how to implement it effectively within business through technical workflows.

2 - Mapping Roles and Responsibilities

2.1 - Understanding Key Actors

The DPDPA's compliance framework begins with clear role definitions. Without clarity on whether an organisation is a Fiduciary, Processor or Significant Data Fiduciary (SDF), it is tedious and impractical to assign accountability or implement appropriate safeguards.

Data Fiduciary

means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data [Section 2(i)].

Data Processor

means any person who processes personal data on behalf of a Data Fiduciary [Section 2(k)].

Data Principal

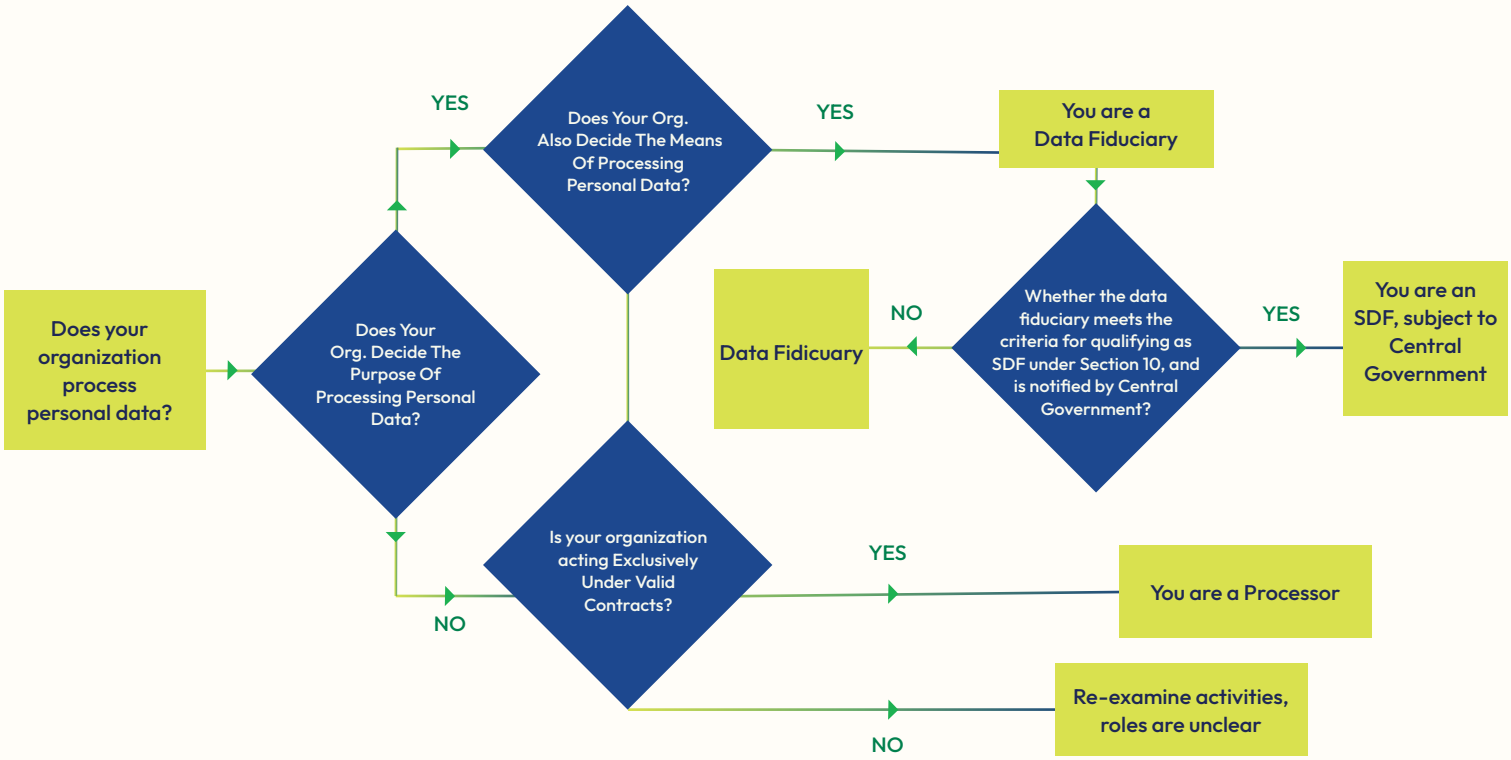
means the individual to whom the personal data relates and includes the parent or lawful guardian of a child or person with disability acting on their behalf [Section 2(j)].

Significant Data Fiduciary (SDF)

means any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10 [Section 2(z)].

2.2 - Determining Your Role

Accuracy of determination of your role under the DPDPA, is foundational as it defines the compliance obligations specific to such role. To assess your role, begin with these guiding questions:

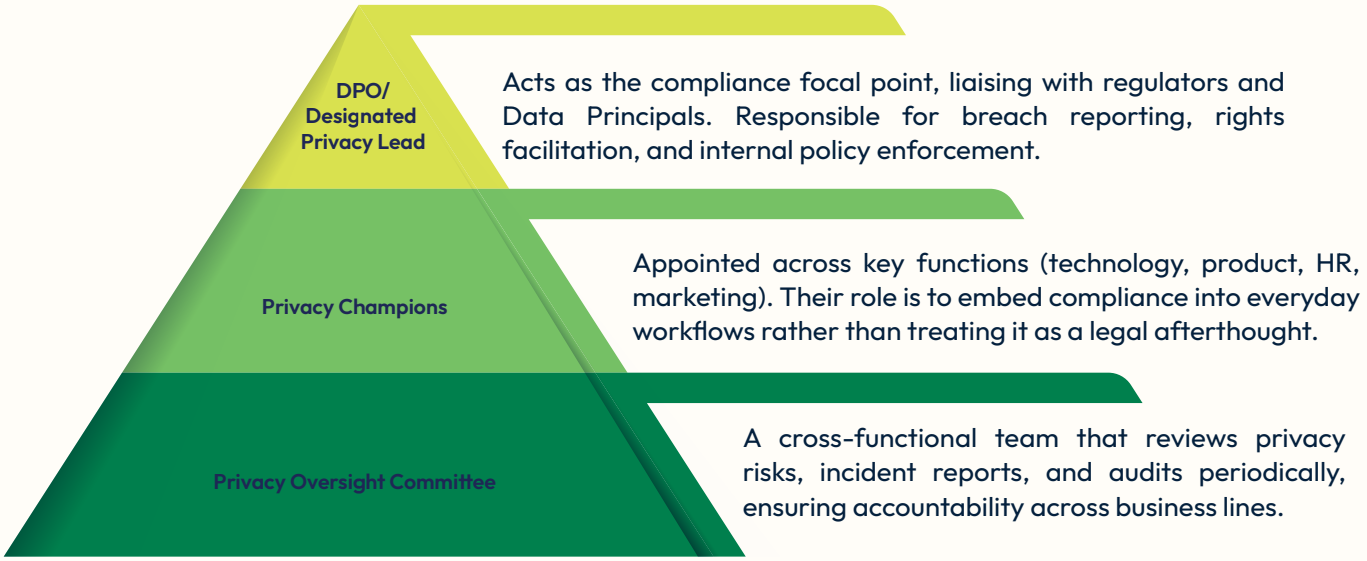


2.3 - Governance Structures and Accountability

The DPDPA recognises that compliance is not a one-time exercise but an ongoing governance challenge.

In addition to the obligations applicable to all data fiduciaries, Significant Data Fiduciaries (SDFs) are required to implement enhanced safeguards such as appointing a Data Protection Officer (DPO) and an independent auditor, conducting annual Data Protection Impact Assessments (DPIAs) and audits from the date they are notified as SDFs. While these obligations are mandatory for SDFs, they represent best practices for all categories of data fiduciaries.

A strong governance structure includes:



By decentralising responsibility (Privacy Champions) while maintaining central accountability (DPO), organisations create a culture of proactive compliance. This not only reduces the likelihood of regulatory action but also reassures customers that their personal data is handled responsibly.

3 - Personal Data Lifecycle Management

3.1.1 - Collection - Privacy Notice

The foundation of lawful data processing under the DPDPA is transparency. DPDPA mandates that Data Fiduciaries must provide an independent privacy notice, separate from any other documentation to Data Principals either before or at the time of data collection.
A compliant privacy notice must describe the following details:

- Categories of personal data collected;
- Purpose of processing and description of goods or services to be provided on the basis of such processing ;
- Retention practices;
- Rights vested with Data Principals and the appropriate channel for exercising rights
- Manner in which complaints could be filed with the Data Protection Board of India
- Identity/contact details of the Data Protection Officer or Grievance Officer.

Case Study: Banking App Notice

An Indian bank redesigns its mobile app to include a layered privacy notice. On the login page, users see a one-paragraph summary: "We collect your KYC details to comply with RBI norms and to provide banking services. We also request your consent for marketing updates." A "Read More" link expands into a full notice explaining retention periods, grievance redressal contacts, and cross-border data sharing rules. This approach balances legal compliance with user experience, without resulting in user-fatigue.

The Privacy Notice should be clear, concise, and accessible in multiple languages (22 official languages outlined within the Eighth Schedule of the Indian Constitution). Global experience (for instance, EU-GDPR enforcement actions) shows that regulators increasingly evaluate not just whether a notice exists but also whether it is easily comprehendible by the end-users. In India, this expectation is particularly relevant because the DPDPA emphasises accessibility, aligning with the government's goal of enabling digital literacy.

3.1.2 - Collection - Consent

Consent is a primary lawful basis for processing under the DPDPA. Section 6 requires that consent must be "free, specific, informed, and unambiguous," given through a clear affirmative action. Importantly, the Act prohibits bundled or coercive consent. Operationalising consent requires designing systems that support its entire lifecycle: collection, validation, renewal, and withdrawal. Each action must generate a Consent Artifact, an audit trail showing when, why, and how consent was given, updated, or revoked.
This ensures accountability in case of audits or disputes and honouring the Data Principal's autonomy over the usage of their personal data. Furthermore, consent interfaces must be designed for ease of use. If withdrawing consent is harder than granting it, fiduciaries could risk penalties.

Case Study: Retailer's Loyalty Program

A retailer launches a loyalty program requiring customers to provide personal details. The consent form clearly distinguishes between mandatory processing (billing and loyalty points management) and optional processing (marketing updates, data analytics for offers). Each purpose has a separate toggle, allowing granular consent. Later, a customer withdraws consent for marketing emails through a one-click dashboard. The system records the withdrawal on a real-time basis and ensures no further marketing messages are sent, while continuing loyalty points services.

3.1.3 - Collection - Processing Personal Data Corresponding to Vulnerable Data Subjects

3.1.3.1 Children's Data

Children's data receives special protection under the DPDPA. The Law requires that processing of personal data relating to children (defined as under the age of 18 years) must be backed by verifiable parental consent. Moreover, fiduciaries are prohibited from processing children's data in ways that could cause harm, such as targeted advertising, behavioural tracking, or profiling.

The operational challenge lies in verifying parental consent without over-collecting data. Methods may include Aadhaar/DigiLocker authentication or tokenised verification flows, by adopting privacy-preserving verification methods that minimise additional personal data collection.

The Act further reinforces that businesses must design child-centric digital experiences that prioritize safety and privacy from the outset. Implementing age-appropriate design, age-gating mechanisms, limited data collection, and transparent communication with verifiable parent or, lawful guardian could significantly strengthen compliance while fostering trust.

Case Study: EdTech Platform Verification

An EdTech platform enrolling students under the age of 18 years integrates a DigiLocker-based parental consent system. During sign-up, parents are prompted to authenticate their identity before approving their child's participation. The platform then stores a Consent Artifact linking the child's account to verified parental consent. The system also ensures that no targeted advertising or behavioural tracking is enabled for underage accounts, in compliance with DPDPA.

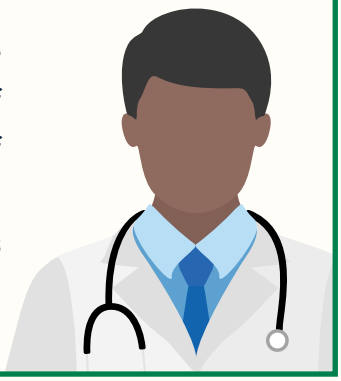
3.1.3.2 Personal Data of Persons with Disabilities

The DPDPA extends additional safeguards to persons with disabilities, recognising that their personal data may be processed through their lawful guardians. Where an individual is unable to take legally binding decisions due to long-term physical, mental, intellectual, or sensory impairment, or suffers from conditions such as autism, cerebral palsy, mental retardation, or multiple disabilities, the lawful guardian assumes responsibility on their behalf.

Fiduciaries must obtain verifiable consent from such lawful guardians before processing the personal data of persons with disabilities. The Draft DPDP Rules further require that guardianship be verified against appointments made by a court of law, a designated authority under the Rights of Persons with Disabilities Act, 2016, or a local level committee under the National Trust Act, 1999.

Case Study: Healthcare Portal Consent

A healthcare portal providing digital therapy sessions for individuals with cerebral palsy requires consent for storing patient progress data. During registration, the system prompts the lawful guardian to upload a digitally signed or certified copy of the guardianship certificate. Once verified, the guardian provides consent on behalf of the individual. The portal also provides a preference center, allowing the guardian to review, modify, or withdraw consent at any time. All changes are recorded as auditable Consent Artifact and restricts data usage solely to therapy-related services.



3.1.4 - Collection - Consent Managers

The DPDPA introduces the unique concept of Consent Mangers, setting it apart from other global privacy laws by empowering Data Principals with control over their personal data. Defined under Section 2(g) of the DPDPA, a Consent Manager is a registered entity with the Data Protection Board that acts as an intermediary, providing a transparent, accessible and interoperable platform where individuals can give, manage, review and withdraw their consent for data processing.

Under Rule 4 Part A of First Schedule of the Draft DPDP Rules, strict requirements govern the registration and functioning of Consent Managers. The company's leadership must have a reputation for fairness and integrity, with governance structures preventing conflicts of interest with Data Fiduciaries. Consent Managers must maintain transparency by publishing key leadership and ownership details, obtain independent certification for compliance with technical and organisational standards and uphold a fiduciary duty towards protecting Data Principals' rights.

3.1.5 - Collection - Cookies & Tracking Technologies

While the DPDPA does not explicitly mention cookies, its broad definition of personal data means cookies and device identifiers fall under its scope if they can identify individuals. Consent for non-essential tracking therefore falls under DPDPA's ambit.

Organisations must implement cookie banners and preference centres that allow granular consent for analytics, advertising, and functional cookies. Default opt-in (pre-checked boxes) is not compliant. Instead, default opt-out with explicit opt-in is the safer approach.

Beyond consent banners, organizations must conduct regular audits and maintain detailed inventories/logs to ensure ongoing compliance. Clear documentation of the cookies deployed, mapped with the specific purpose improves transparency, supports audit readiness, and demonstrates organizational accountability under the DPDPA and emerging global privacy frameworks.

Case Study: News Website Cookie Banner

A digital news publisher introduces a cookie banner with three categories: "Strictly Necessary," "Analytics," and "Advertising." Cookies are not actively deployed on the website until the user provides explicit consent. Users are also given the option to modify their preferences at any time. If they reject analytics cookies, the site continues to function but does not track reading habits. Consent choices are logged in a Consent Artifact for future audits. This not only complies with DPDPA but also enhances user trust.

3.2 - Personal Data Processing and Usage

3.2.1 - Lawful Grounds

The DPDPA establishes that personal data must only be processed for lawful purposes. While consent is the primary basis, DPDPA outlines legitimate uses where processing may occur without consent. These include:

- Employment purposes
- Compliance with law or court orders
- Emergencies or disasters
- Functions of the State in public interest
- Voluntary provision of personal data

Organisations must map every processing activity to one of these grounds and maintain documentary justification.

3.2.1.1 - Employment Purposes

Processing of employee data for purposes such as onboarding, payroll, benefits, and workplace safety is exempt from consent requirement. Additionally, fiduciaries are required to communicate the nature and purpose of such processing transparently to employees. This can be done through an easily understandable employee privacy notice, either incorporated into the employment contract or provided during the onboarding.

Case Study – HR Payroll System

A multinational company processes employees' bank account details to disburse salaries. Encryption and role-based access controls are in place to safeguard the data of its employees. Employees are provided with the mechanism to request correction of outdated account information. The company also ensures transparent communication regarding this processing though an employee privacy notice, made available via its payroll platform and incorporate within the employment contract.

3.2.1.2 - Compliance with law or Court Orders

Personal data may be processed without consent when required to comply with applicable laws, regulations, or judicial directives. Fiduciaries must ensure that only the data specifically mandated is disclosed and that such processing remains proportionate to the legal obligation.

Case Study: Court-Mandated Disclosure

A cloud storage provider receives a court directive to disclose user records in connection with an ongoing intellectual property infringement case. The provider furnishes only the information explicitly required under the order, ensures that the data is encrypted during transfer to the court and maintains an internal log of the disclosure for audit purposes. If allowed, the provider also notifies its users about the disclosure.

3.2.1.3 - Emergency and Disaster Scenarios

Emergencies often require processing without consent. For example, a hospital may access the medical history of an unconscious patient to provide life-saving treatment, or government authorities may share geolocation data during natural disasters to coordinate rescue operations.

Case Study: Disaster Relief Coordination

During a cyclone, telecom providers share anonymised location data with state authorities to coordinate evacuation efforts. While consent is bypassed, providers must ensure that data is retained only for the duration of the crisis and later deleted.

3.2.1.4 - State Functions

The State may process data without consent for functions such as law enforcement or regulatory compliance. However, fiduciaries must still ensure proportionality and safeguards.

Case Study: Tax Compliance

A fintech app shares user transaction data with the Income Tax Department under statutory obligations. While consent is not needed, the app informs users through its privacy notice and ensures only legally mandated data is shared.

3.2.1.5 - Voluntary Provision of Personal Data

Personal data may be processed without consent when the data principal voluntarily provides it, and it is reasonably expected to be used for that purpose.

Case Study: Retail Checkout

A customer provides their phone number at checkout to receive an e-bill. The retailer can process the number to send the invoice but cannot automatically add the customer to promotional SMS campaigns without explicit consent.

3.3 - Sharing and Transfer

3.3.1 - Internal Sharing

Internal sharing of personal data must be safeguarded through appropriate technical and organisational measures. This includes encryption, access controls, audit trails, and segregation of duties to ensure that only authorized personnel have access to the data required for their role.

3.3.2 - External Sharing

When personal data is shared externally with vendors, partners, or other third parties, fiduciaries must establish contractual safeguards. A valid Data Processing Agreement (DPA) or equivalent contract must clearly define roles, responsibilities, and limitations on use, along with compliance requirements under the DPDPA. Fiduciaries must also inform Data Principals about the recipients of their data and ensure that contractual provisions with the Processor enables the efficient management of the data principal requests raised to exercise their rights.

Case Study: Healthcare Provider

A hospital internally shares patient medical records between its oncology and radiology departments through a secured electronic health records system with strict access controls. For external sharing, the hospital engages a diagnostic lab for specialized testing under a contractual agreement that restricts data use solely to diagnostic purposes and requires compliance with DPDPA safeguards, including secure transfer protocols and timely deletion after use.

3.4 - Storage and Deletion

3.4.1 - Security Safeguards

Fiduciaries must adopt "reasonable security safeguards" to prevent data breaches. Measures that must be undertaken must include at minimum, encryption, pseudonymisation, access controls, and disaster recovery plans.

3.4.2 - Retention and Deletion

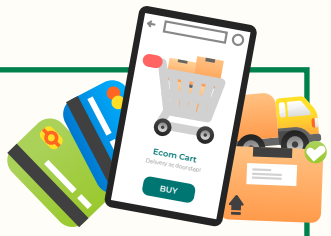
Personal data must be erased when the purpose of processing is fulfilled, unless law requires retention. Retention schedules should be documented in consonance with the DPDPA, its subsequent Rules and any other sector-specific statutory obligations. Under Rule 8 of the DPDP Draft Rules, Fiduciaries must also notify Data Principals at least 48 hours before deletion, giving them the opportunity to act if desired.

Case Study: E-commerce Platform

An e-commerce platform retains user order data until delivery is complete.

Personal data provided for marketing purposes is deleted upon withdrawal of consent.

However, invoice data may be retained for statutory GST filing obligations. This demonstrates alignment with both DPDPA and relevant sector- specific financial regulations.



3.4.3 - Organisational Best Practices

- Maintain a data inventory linked to retention periods.
- Automate deletion triggers based on expiry or consent withdrawal.
- Conduct periodic data minimisation audits.

4 - Rights of Data Principal

Right to Access

Data Principals can demand a summary of personal data processed, details of processing activities, and disclosure of third-party sharing.

Right to Correction & Erasure

Data Principals may correct inaccurate or misleading data, complete incomplete data, and erase data no longer required. However, fiduciaries may retain data where law mandates.

Right to Grievance Redressal

Fiduciaries must maintain accessible grievance systems. If unresolved, complaints may be escalated to the Data Protection Board of India.

Right to Nominate

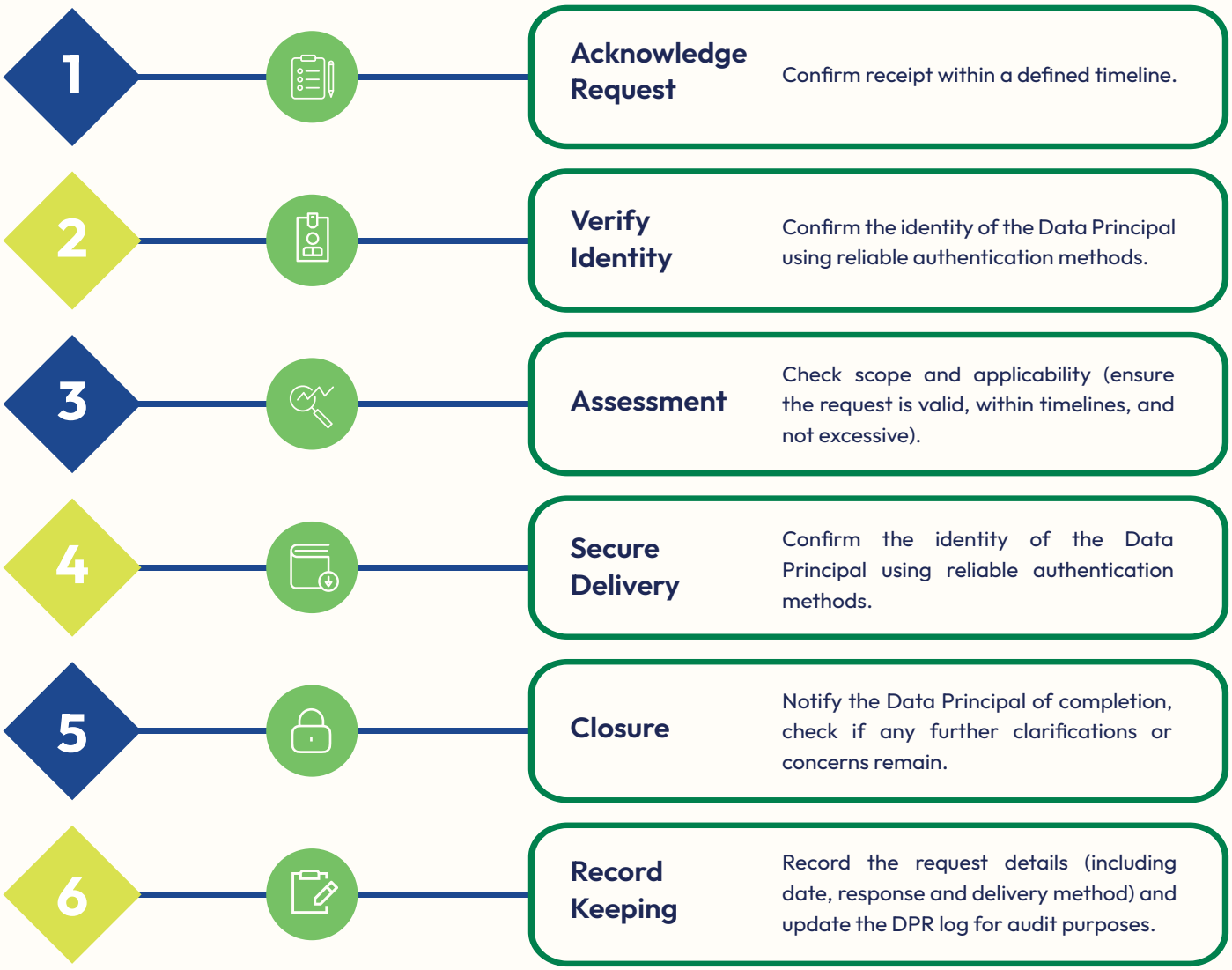
This uniquely Indian right allows a Data Principal to nominate another individual to exercise rights upon death or incapacity.

Withdrawal of Consent

Data Principals may withdraw consent as easily as giving it. Fiduciaries must cease processing immediately unless further retention is legally required.

4.6 - Sample Data Principal Request (DPR) Management Workflow

Problem Statement: A Data Principal Access Request is received by an organization processing the pertinent personal data corresponding to the Data Principal:



5 - Breach Reporting

5.1 - Notification Obligations

Data Fiduciaries must notify both the Data Protection Board and affected individuals in case of a breach. Notification should specify the nature of the breach, extent, timing and location of the breach along a detailed report within 72 hours to the Board.

5.2 - Timelines

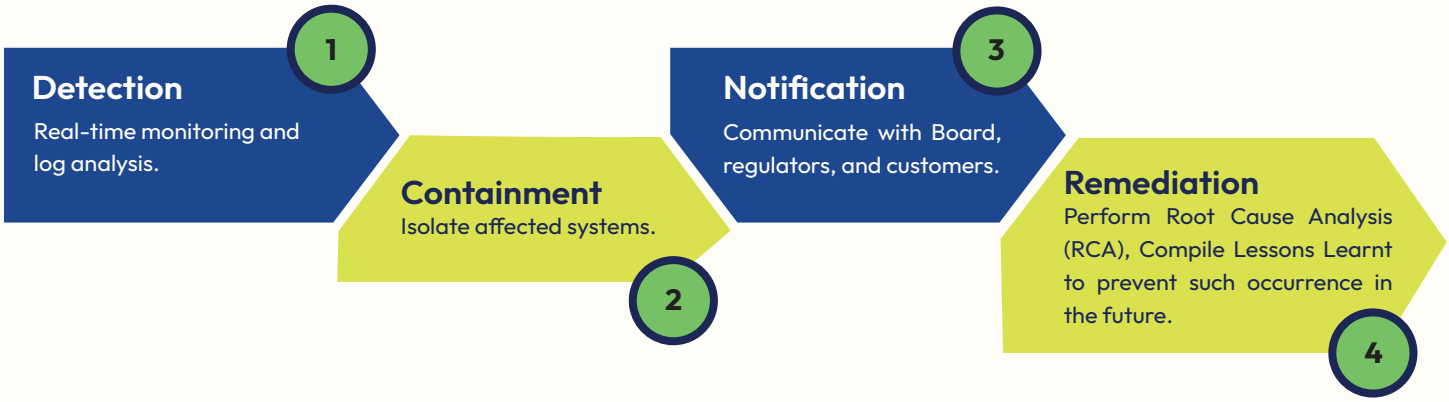
Rule 7 of the Draft DPDP Rules requires a personal data breach must be notified:

- To Data Principals: They must be informed in clear language of the breach (nature, extent, timing, location), likely consequences, mitigation steps by the Data Fiduciary, safety measures they can take, and contact details for queries.

- To the Data Protection Board: The Data Fiduciary must immediately provide details of the breach (nature, extent, timing, location and likely impact), followed by a detailed report within 72 hours, covering updated facts, causes, mitigation and remedial steps, identity of the person and confirmation of notices to the affected Data Principals.

5.3 - Data Breach Management Workflow

The standard industry best practice for management of security incidents, could be leveraged as a workflow to manage data breaches as well. The workflow could encompass the following stages -



6 - DPDPA Compliance Journey

Ensuring compliance with India's Digital Personal Data Protection Act (DPDPA), 2023 requires a structured and methodical approach. This step-by-step journey guides organisations through essential activities - from conducting an initial gap assessment and data discovery to implementing privacy controls, developing policies, and embedding privacy by design. It also emphasises continuous risk assessments, third-party management, employee training, and ongoing monitoring to maintain accountability and adapt to evolving compliance requirements. By following these stages, organisations can build a robust data protection framework that safeguards personal data, meets legal obligations, and fosters trust with customers and stakeholders.

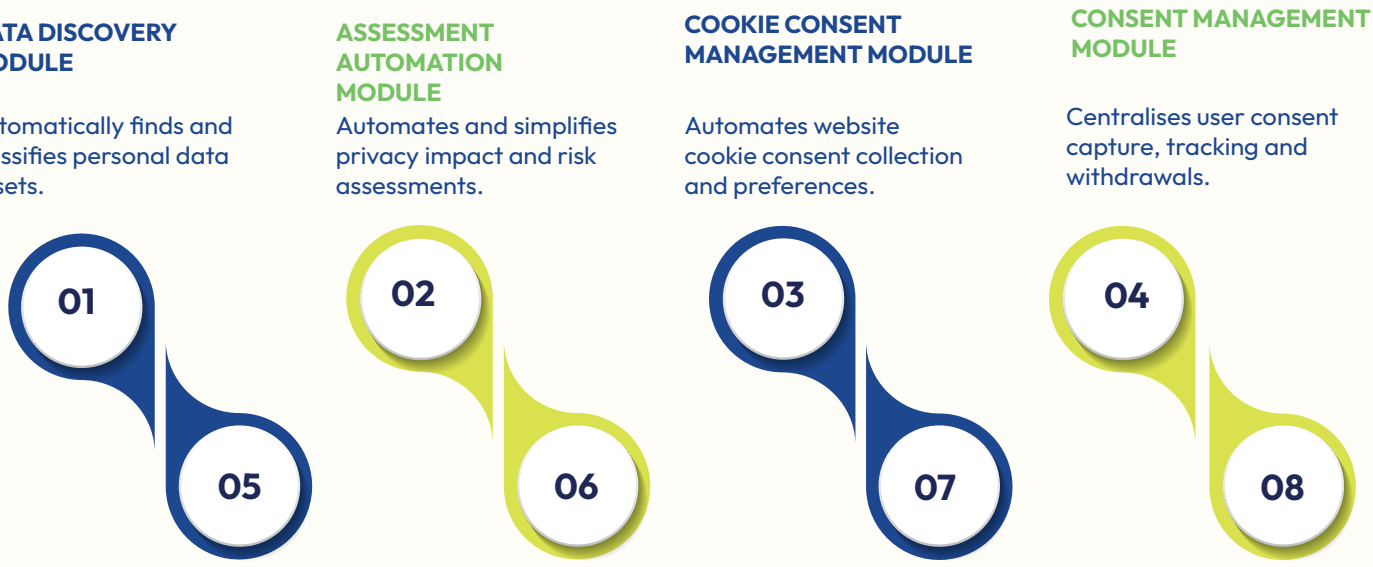
7 - About Us & How We Can Help

Founded in 2018, Privacy Pillar is a data privacy solutions provider committed to empowering consumers and enabling businesses to thrive in an increasingly regulated digital landscape. Our purpose is to deliver robust, affordable, and user-friendly solutions that help organizations meet evolving privacy, information security, and regulatory compliance requirements.

As a rapidly growing company, Privacy Pillar is focused on becoming a trusted leader in data privacy and compliance. Through our solutions, we help businesses harness the Power of Permission, placing trust and transparency at the core of customer engagement. This not only enhances user experience but also mitigates legal and regulatory risks.

7.1 - Key Automation Capabilities

Privacy Pillar offers a robust suite of automation capabilities designed to streamline and strengthen DPDPA compliance. These modules help organisations efficiently discover, map, and manage personal data, automate user consent and requests, monitor risks, and provide integrated oversight across all privacy functions. This comprehensive automation ensures accuracy, agility, and regulatory alignment for businesses in a dynamic data protection landscape.



Each of the above capabilities aims to simplify and operationalize compliance with DPDPA by embedding automation into everyday privacy operations. These capabilities are completely interoperable and can be seamlessly integrated with existing enterprise systems to ensure seamless implementation of workflows & connectivity. They are completely customizable to align with specific business and regulatory requirements across industries. Designed for swift deployment, the capabilities enable organizations to accelerate DPDPA compliance readiness, strengthen governance, and maintain continuous oversight of privacy obligations through real-time monitoring and automated reporting.

7.2 - Our Functional Services

Our functional services provide expert guidance and hands-on support across the entire spectrum of data privacy management. From establishing frameworks to offering assessments and audits, we help organizations build a strong foundation for regulatory compliance and privacy best practices.

Contributors

MR. AKHILESH MS

Director - Strategy & Growth

MS. KRITHI SHETTY

Associate Director - Data Privacy

MR. PAWAN KALYAN

Data Privacy Consultant

MS. SRISHTI BORKAR

Data Privacy Trainee

Get In Touch With Our Privacy Team

MR. DHARMESH PATEL - Founder & CEO	dharmesh@privacypillar.com
Mr. KASHYAP VYAS - Co Founder & COO	kash@privacypillar.com
MR. AKHILESH MS - Director [Strategy & Growth]	akhilesh.ms@privacypillar.com | +91 88868 88465
MS. KRITHI SHETTY - Associate Director [Data Privacy]	krithi.shetty@privacypillar.com | +91 81051 19604