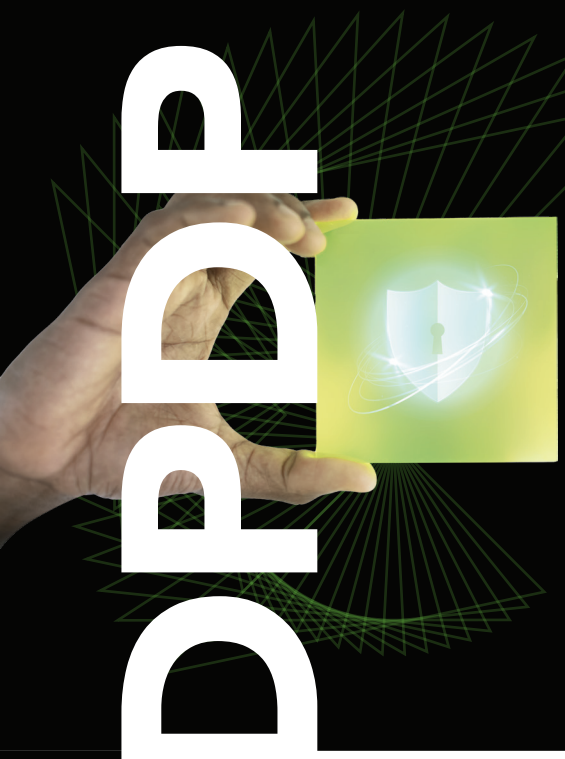

India's Digital Personal Data Protection Bill 2023:
A Comprehensive Overview

Recognizing the need to safeguard the privacy of its citizens, India has introduced the Digital Personal Data Protection (DPDP) Bill 2023.

The DPDP bill defines personal data as 'any data about an individual who is identifiable by or in relation to such data.

The critical elements of the DPDP Bill include:

01

Empowering Individuals: Rights and Duties

Bill empowers individuals (Data Principals) with rights like data access, updates, corrections, and erasure, while also outlining their duties to authenticate information, comply with laws, and avoid false grievances.

02

Regulating Data Processors: The Role of Data Fiduciaries

Data Fiduciaries must redress grievances, ensure data security, and report breaches; Up to INR 200 crore penalties for failing to notify breaches and up to INR 250 crore for inadequate security safeguards.

03

Special Provisions: Cross-border Data Transfers and Data Localization

'Black-list' approach, allowing cross-border transfers to all except specific countries or territories. No mandated local storage, enabling cost optimization and simplified compliance.

04

A Robust Governance Structure: The Data Protection Board of India

Data Protection Board of India enforces Act, directs remedies, investigates breaches, and oversees penalties.

05

Consent Mechanism: The Role of a Consent Manager

'Consent Managers', registered with the Data Protection Board, are the single point of contact for users, empowering complaints and streamlining consent process.

06

Appeals, Mediation, and Voluntary Undertakings

Clear pathways for appeals to the Appellate Tribunal. Concept of mediation and voluntary measures, offering alternate routes to address personal data concerns.

Data Discovery and Classification: The first step to DPDP compliance

SISA

Data Fiduciary

An entity or organization that determines the purposes and means of processing personal data alone or in conjunction with others.

- *Must have absolute visibility of the entire data they hold in their environment end-to-end*
- *Need to maintain the accuracy of data, keep data secure, and delete data once its purpose is met*
- *Adopt reasonable security precautions to avoid a personal data breach*

Data Processor

Organizations that collect, store, or perform any other operation on personal data directly or on behalf of a Data Fiduciary. Even if the primary obligation always rests with the data fiduciary, a Data Processor must:

- *Protect personal data in their custody*
- *Adopt reasonable security precautions to avoid a personal data breach,*

Begin your journey with Data Discovery

The DPDP framework prompts organizations to reassess privacy practices for consumer data. The journey toward improved data handling and compliant collection starts with 'Data Discovery and Classification.'

How SISA Radar can help!

An automated Data Discovery and Classification tool designed to assist organizations in understanding their sensitive information and answers crucial questions, such as

- Identifying what sensitive data the company possesses
- Locating where the data is stored
- Determining the nature of data if it is personal (Content-based classification)
- Determining the nature of data depending on the job role (Context-based classification)
- Understanding why the data was collected and determining how the data is being utilized

SISA Radar key features

- Locate, tag, and classify data both at rest and in motion
- Deployable in both agent and agentless modules using on-prem and cloud applications
- Process data stored in any cloud environment, Azure, AWS, GCP, etc
- Detect personal data stored in
  - Application logs, API Logs
  - Databases, database snapshots
  - Audio files, images, and images inside documents
  - PDFs, emails, and attachments,
- Built-in 60+ pre-defined and other user-defined PII types
- Helps meet multiple compliance regulations, including DPDP, GDPR, HIPPA, and more

> “95% of our customers are shocked to find the volume and location of sensitive data that our tool uncovers, revealing exposures that could have led to legal action by regulators.”
>
> **- Prabhu Narayan,** VP of Data Security and Governance, SISA.

Reach out to us at **sales@sisainfosec.com** or visit **www.sisainfosec.com**.
Get started on your DPDP Journey with SISA today!