SmartSuite

Framework / Privacy / Global Privacy Regulations

Digital Personal Data Protection Act, 2023 (DPDPA 2023)

India's Digital Personal Data Protection Act (DPDPA) regulates collection, processing, storage, and cross-border transfer of individuals' digital personal data.

DPDPA

What it is

The India Digital Personal Data Protection Act (DPDPA) 2023 is a national data protection regulation that helps organizations safeguard personal data, ensure individuals' privacy rights, and strengthen data governance in accordance with Indian law. Its primary goal is to establish standards for the collection, processing, storage, and transfer of digital personal data.

The DPDPA is published by the Government of India and applies to organizations, both public and private, that process digital personal data of individuals within India, including offshore entities handling Indian residents' data. The Act covers key areas such as privacy governance, data protection obligations, consent management, cross-border data transfers, and rights of data principals, aligning with global trends in data privacy regulation.

At a glance

PUBLISHER Ministry of Electronics and Information Technology (MeitY), Government of India	TYPE Framework	VERSION DPDPA 2023
EFFECTIVE August 11, 2023	DOMAIN Privacy	FAMILY Global Privacy Regulations
REGION India	ADOPTION MODEL Regulatory Compliance	IMPLEMENTATION COMPLEXITY High

Source: https://www.meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

Why it matters

- **Strengthen privacy governance** Promote robust accountability, oversight, and transparency around personal data processing to foster stakeholder and regulatory trust.
- **Enhance regulatory compliance** Align organizational data practices with Indian legal requirements to mitigate enforcement risks and regulatory penalties.
- **Support data subject rights** Enable streamlined processes to honor individual rights related to access, correction, and consent for their personal data.
- **Increase operational resilience** Improve organization-wide preparedness for data breaches and incidents through mandated policies and structured response procedures.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How SmartSuite supports DPDP Act 2023

Processing Inventory and Purpose Controls

Document data categories, purposes, sharing, retention, and safeguards.

Notice and Consent Governance

Track notice content, consent capture, withdrawal handling, and policy reviews.

Rights and Grievance Workflows

Manage requests and grievances with deadlines, responses, and audit trail.

Vendor and Processor Oversight

Track processor contracts, safeguards, and monitoring evidence.

Security Safeguards and Incident Alignment

Centralize safeguards and incident response documentation tied to personal data risk.

Compliance Reporting

Report request performance, open actions, and accountability evidence.

Common framework mappings

APEC PF | CCPA/CPRA | GDPR | HIPAA | ISO 27701 | NIST Privacy Framework v1.0 | OECD Privacy Guidelines | UK GDPR

Official resources

India Digital Personal Data Protection Act (DPDPA) 2023

Provides comprehensive regulations for personal data protection and privacy in India.

meity.gov.in/static/uploads/2024/06/2bf1f0e9f04e6fb4f8fef35e82c42aa5.pdf

DPDPA Implementation Guide

Outlines key steps and measures for implementing compliance with DPDPA requirements.

meity.gov.in/dpdpa-implementation

DPDPA Ecosystem Overview

Describes the broader framework and components related to personal data protection in India.

meity.gov.in/dpdpa-ecosystem-overview

DPDPA Compliance Framework

Defines the legal and operational guidelines for achieving compliance under the DPDPA.

meity.gov.in/dpdpa-compliance-framework

Frequently asked questions

What is the India Digital Personal Data Protection Act (DPDPA) 2023 used for?

The DPDPA is used to establish legal requirements for handling digital personal data within India, focusing on protecting individuals' privacy rights and enforcing data protection standards. It provides a framework for data collection, processing, storage, and transfer, ensuring organizations adopt appropriate safeguards to prevent unauthorized access or misuse of personal data.

Is compliance with DPDPA mandatory for organizations in India?

Yes, compliance with the DPDPA is mandatory for all organizations, including private and public sector entities, that process digital personal data of individuals in India. It also applies to foreign companies and offshore processors if they handle data concerning Indian residents.

What is the scope of the DPDPA and who does it apply to?

The scope of the DPDPA covers any organization (data fiduciary) that collects, stores, or processes digital personal data within India, as well as entities located outside India if they process such data for offering goods or services to individuals in India. It also includes data processors and third-party vendors managing Indian data.

What are the key concepts and required documentation under the DPDPA?

Key concepts in the DPDPA include data fiduciaries (organizations controlling data), data principals (individuals), consent management, purpose limitation, breach notification, and cross-border data transfers. Required documentation typically includes privacy policies, records of processing activities, impact assessments, and breach response plans.

Updated Sep 26, 2026 · © 2026 SmartSuite Inc. All rights reserved.

How should organizations implement DPDPA compliance?

Organizations should implement DPDPA compliance by developing robust privacy policies, appointing a data protection officer, mapping data flows, conducting data protection impact assessments, instituting technical and organizational security controls, and ensuring transparent consent mechanisms for data processing.

How does the DPDPA relate to other data protection frameworks?

The DPDPA aligns with global data privacy principles seen in frameworks like the EU's GDPR, emphasizing user rights, accountability, and strong data governance. However, the DPDPA is tailored to the Indian legal and social context, with specific regulatory requirements and enforcement mechanisms under a dedicated Data Protection Board.

What ongoing requirements must organizations meet under DPDPA?

Ongoing compliance involves regular risk assessments, continuous monitoring of data processing activities, periodic staff training, documentation and review of privacy practices, timely breach notifications, and maintaining up-to-date records to demonstrate adherence to DPDPA obligations.

How would SmartSuite support India Digital Personal Data Protection Act (DPDPA) 2023 compliance?

SmartSuite streamlines DPDPA compliance by enabling organizations to track risks, manage and map regulatory controls, document evidence of data protection practices, and support audit readiness. It facilitates centralized management of compliance workflows, automates breach reporting, and delivers executive dashboards for real-time reporting and ongoing monitoring of key controls.

License included / downloadable: Yes The Digital Personal Data Protection Act is national legislation and is publicly available through official government sources.

Full framework page and mappings: smartsuite.com/frameworks/india-digital-personal-data-protection-act-dpdpa-2023