India's new data protection law

A guide for contract managers

Zoho Contracts

ZOHO

Table of Contents

Disclaimer: This e-book does not provide legal advice on the DPDPA. Its objective is to support organizations in developing contract management systems that facilitate compliance. If you have any queries concerning the law, we strongly recommend consulting with your legal counsel and data privacy expert.

Introduction

India's Digital Personal Data Protection Act (DPDPA) came into effect on the 11th of August, 2023. This Act sets guidelines for handling digital personal data, balancing individuals' rights to protect their data with organizations' legitimate reasons for processing it.

Scope

The Act defines personal data as, "any data about an individual who is identifiable by or in relation to such data."

The Act is applicable for the processing of both digital and digitized personal data within the territory of India as well as outside it. Additionally, any activity related to offering goods and services to data principals within India falls under the purview of this Act.

However, the Act does not apply to the processing of data for domestic or personal purposes by individuals. Furthermore, it does not cover personal data that has been made publicly available.

Key stakeholders

(The definitions included here are as mentioned in the Act.)

Data Principal

A Data Principal is the individual to whom the personal data relates and where such individual is—

a. a child, including the parents or lawful guardian of the child.

b. a person with disability, including their lawful guardian, acting on their behalf.

Board

A regulatory body, or Board, refers to the Data Protection Board of India established by the Central Government under section 18 of this Act.

Consent Manager

A Consent Manager is a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review, and withdraw their consent through an accessible, transparent, and interoperable platform.

Data Fiduciary

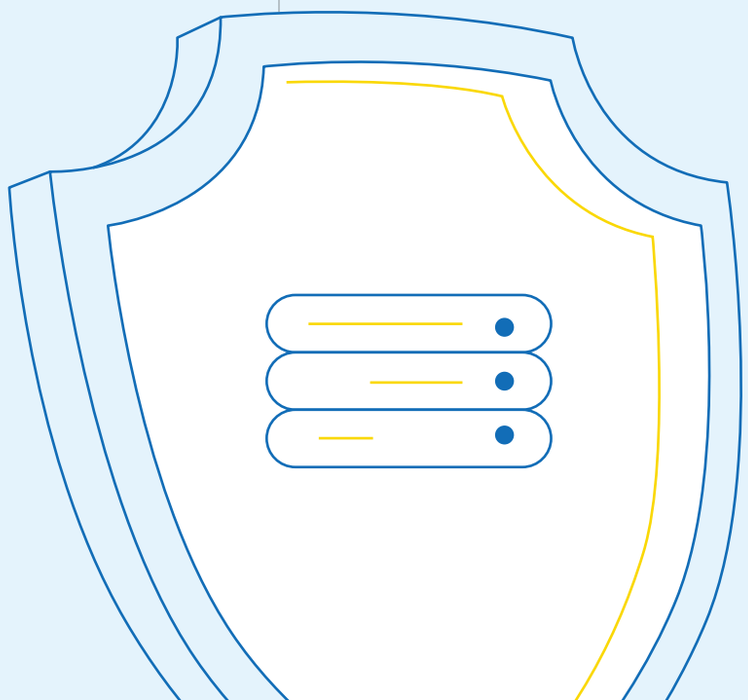
A Data Fiduciary is any person who, alone or in conjunction with other persons, determines the purpose and means of processing of personal data.

Data Processor

A Data Processor is any person who processes personal data on behalf of a Data Fiduciary.

Significant Data Fiduciary

A Significant Data Fiduciary refers to any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government under section 10 of this Act.



Data Protection Officer

A Data Protection Officer is an individual appointed by the Significant Data Fiduciary under clause (a.) of sub-section (2.) of section 10 of this Act.

Rights and duties of a Data Principal

1. Right to access information about personal data.

Data Principals can ask for:

a.) A summary of the personal data being processed.

b.) The identities of other entities with whom the data has been shared.

c.) Any other related information about their personal data and its processing.

Exemptions are made when data is shared with other entities for detecting or investigating offenses.

2. Right to correction and erasure of personal data

Data Principals have the right for corrections, completion, updates, or erasure of their data for which they have previously given consent.

Upon receiving a request, it is the responsibility of the Data Fiduciary to correct the data if it is inaccurate, complete it if it is incomplete, update it if it is outdated, and erase it unless the data is required for a specific purpose or legal compliance.

3. Right of grievance redressal

Data Principals can raise grievances regarding data management with the respective Data Fiduciary or Consent Manager.

These entities must respond to grievances within a specified period. If the requirements are not met, the Data Principals can approach the central board.

4. Right to nominate

Data Principals can nominate another individual to exercise their data rights in case they're incapacitated (due to mental unsoundness or bodily infirmity) or deceased.

5. Duties of Data Principals

Data Principals must:

a.) Comply with all other relevant laws.

b.) Avoid impersonation.

c.) Not suppress vital information when providing data for official documents or proofs.

d.) Avoid lodging false grievances or complaints.

e.) Provide authentic information when asking for corrections or erasure.

Obligations of the Data Fiduciary

The key obligations of the Data Fiduciary are as follows:

- Data Fiduciaries must comply with the provisions of this Act under all circumstances and be responsible for the data processing by themselves or by the Data Processor.
- Data Fiduciaries can use data processors to process personal data on its behalf only under a valid contract.
- Data Fiduciaries must employ suitable technical and organizational measures to follow the Act's provisions.
- Data Fiduciaries must safeguard personal data against breaches, including when processed by data processors.

- If there is a data breach, Data Fiduciaries should notify the board and impacted Data Principals.
- Data should be erased when the Data Principal withdraws consent or when its purpose is no longer served. If a law requires retention, it can be kept.
- The purpose of retaining data is considered invalid if the Data Principal does not approach the data fiduciary or exercise any related rights for a set period.
- Data Fiduciaries must publicly share contact details of their Data Protection Officer or a representative who can address queries about personal data processing.
- Data Fiduciaries must have a system to address grievances of Data Principals.
- A Data Principal is deemed not to have approached a Data Fiduciary if they have not initiated contact in any form during a specified period.

Obligations of the Significant Data Fiduciary

The significant data fiduciary must fulfill the following obligations:

- Appoint a Data Protection Officer who will represent them under this Act, be based in India, be answerable to the organization's primary governing entity such as the Board of Directors, and act as the primary point of contact for grievance redressal.
- Select an independent auditor for compliance assessment.
- Carry out regular Data Protection Impact Assessments that highlight the rights of Data Principals, the purposes of data processing, and the associated risks.
- Undertake periodic audits and align with other prescribed measures consistent with this Act.

Monitoring children's personal data

Before handling the personal data of children or individuals with disabilities under guardianship, Data Fiduciaries are obligated to secure verifiable consent from either the child's parent or the guardian. They must ensure that the data processing won't negatively impact a child's welfare and are strictly barred from tracking, behaviorally monitoring, or directing targeted ads at children.

Transfer of personal data outside India

The Central Government has the authority to set rules that may restrict a Data Fiduciary from transferring personal data for processing to specific foreign countries or regions. However, any current Indian law that provides more stringent protection or tighter restrictions on the export of personal data will continue to be in effect and take precedence.

Exemptions

Provisions of this Act don't apply in cases where:

a.) Data processing is necessary for legal rights or claims.

b.) Data processing is done by courts, tribunals, or any other body which is entrusted by law in India.

c.) Data is processed for preventing, detecting, or investigating any offense.

d.) Data of individuals outside India is processed based on a contract with someone outside India.

e.) Data processing is necessary for corporate restructurings like mergers or demergers approved by the authority.

f.) Processing is to determine the financial standing of a loan defaulter.

(For more details on exemptions, please refer to Chapter IV of this law.)

Penalties

- Breach of provisions of the Act or rules: **Up to ₹250 crore.**
- Failure of the Data Fiduciary to prevent a personal data breach: **Up to ₹200 crore.**
- Failure to notify the Board or the affected individual about a data breach: **Up to ₹200 crore.**
- Breach regarding children's data obligations: **Up to ₹150 crore.**
- Breach in observance of duties by the Data Principal: **Up to ₹10,000.**
- Violation of voluntary undertaking accepted by the Board: **Penalty applicable for the original breach under section 28.**
- Breach of any other provision of the Act or its rules: **Up to ₹50 crore.**

The impact of the DPDPA on contract management

Whenever a new law or regulation emerges in the industry that you operate in, it invariably impacts your business and its contracts. Specifically, two broad alterations emerge:

1. Changes in the language of your contracts to reflect the new provisions in the law/regulation.

2. Introduction of new procedures and controls in your contract management process to ensure compliance.

The DPDPA is no exception to this phenomenon. It necessitates the following transformation in the contract management process of an organization.

Changes in contractual languages

Enhanced rights of Data Principals

The DPDPA provides enhanced rights to the Data Principals, including the right to be informed, the right to correction, erasure, and more. Contracts must now reflect and accommodate these expanded rights, specifying the roles and responsibilities of each party.

Liabilities and indemnities

Given the DPDPA's rigorous penalties for data breaches and non-compliance, contracts must carefully address liabilities and indemnities. Thus, organizations would now be required to refine indemnity clauses to manage potential risks and liabilities.

Data breach notification

Contracts need to clearly lay out the processes, responsibilities, and timelines for data breach notifications. The DPDPA necessitates that affected Data Principals and the Board are duly informed.

Data transfers

In light of the DPDPA's strict guidelines on international data transfers, contracts need to integrate provisions like standard contractual clauses to ensure data that is transferred outside of India remains protected.

Record keeping

The DPDPA mandates that certain entities, like the Data Fiduciaries, maintain a comprehensive log of their data processing activities. This means contracts must now have clauses concerning record maintenance, accessibility, and auditing.

Changes to the contract management processes

Vendor management

The DPDPA emphasizes that organizations should be answerable not just for their own adherence to the law, but also for their vendors' and subcontractors' compliance. This translates to a need for a rigorous procedure to gauge and oversee the DPDPA compliance of third-party entities.

Review and update

Given the stricter data protection mandates of DPDPA, organizations need to periodically revisit and update their existing contracts to ensure they're in line with the latest requirements.

Data processing agreements (DPAs)

If an organization engages a Data Processor (as a third party) to process personal data on its behalf, DPDPA requires that a valid contract (i.e., DPA) is in place between the Data Fiduciary and the Data Processor. Contract managers must be adept at incorporating and understanding these agreements.

Training and awareness

The complex requirements of the DPDPA make it imperative for contract management professionals to have a thorough understanding of its provisions. Regular training, combined with internal audits and activity tracking, is vital to ensure consistent compliance and to address any potential oversights promptly.

Staying DPDPA-compliant with CLM Software

Centralized contract repository

A centralized digital repository for storing all contracts is essential in ensuring their easy accessibility, searchability, and manageability. For compliance with the DPDPA, such a system is invaluable. For instance, with a centralized repository coupled with advanced analytics, organizations can swiftly identify and isolate contracts containing specific DPDPA clauses that may require modification to remain compliant.

Template standardization

Contract management solutions often provide standardized templates. Organizations can create DPDPA-compliant templates to ensure every new contract meets the necessary requirements, reducing the risk of non-compliance.

Version control

As contracts undergo revisions, it is essential to maintain a clear record of changes, especially concerning data protection clauses. Contract management software typically offers version control features to track versions.

Obligations management

Obligations related to the DPDPA can be complex and time-sensitive. Contract management software aids in capturing and tracking these obligations. Whether it is periodic audits or specific data handling commitments, automated alerts ensure that organizations never miss a deadline, thereby ensuring compliance and fostering trust with stakeholders.

Access controls

The DPDPA emphasizes the principle of data minimization and restricted access—and business contracts comprise a lot of critical data. Contract management software allows organizations to set granular user permissions, ensuring only authorized individuals can access specific contracts or data.

Audit trails

In compliance with the DPDPA's mandates, it is vital for organizations to ensure transparency and accountability in their data handling processes. Contract management systems can provide comprehensive audit trails detailing who accessed a contract, when, and what changes they made.

Data management

The DPDPA mandates that organizations should not retain personal data beyond its necessary duration. Contract management software aids in this aspect by evaluating metadata within the CLM system and examining contract content. This ensures timely deletion or anonymization of data in compliance with DPDPA guidelines.

Encryption and security

To protect personal data, contract management software that align with DPDPA compliance offer robust encryption protocols, both for data in transit and at rest. This reduces the risk of unauthorized data breaches.

About Zoho Contracts

With over 25 years of history, Zoho is trusted by more than a hundred million users worldwide. Zoho Contracts is our contract management solution. It provides an all-in-one CLM solution, allowing businesses to streamline the contract lifecycle on a singular platform. This eliminates the need for multiple apps, reducing contract cycle times and operational costs. Our platform features advanced analytics for strategic insights, detailed activity monitoring, and targeted obligation management to boost compliance, mitigate risks, and improve productivity. Below are some key features of Zoho Contracts.

Avoid using multiple software

Eliminate the need for a separate word processor, email application, e-signature software, spreadsheet system, document management software, and calendar. Zoho Contracts encompasses all of these software to manage your contracts.

Accelerate your contract authoring

Leverage the power of our native authoring capabilities, which are built on a full-blown word processor that has been refined over 15 years of R&D. Write contracts instantly with the help of our predefined templates, the exhaustive clause library, and intuitive collaboration features. Import your contracts in the draft, signed, or even expired states, and manage them all in Zoho Contracts.

Automate approvals

Create your own approval workflows, both sequential and parallel. Approvers can add contextual comments before approving or rejecting a contract.

Negotiate online with password-protected links

Provide secure access to contracts for counterparty contacts through password-protected links. They can engage in synchronous collaboration, propose modifications, annotate with contextual comments, set comment visibility, track negotiation history, and compare changes.

Never miss out on a renewal opportunity

Choose to auto-renew your contracts. Stay updated on renewal opportunities with in-app and email alerts.

Secure legally binding signatures digitally

Our eSignature capability, powered by Zoho Sign, allows you to establish a signing order for signatories, including representatives from your organization, counterparty organization, and additional representatives, and secure legally binding signatures.

Zoho Sign

Effortlessly manage post-execution stages

Our automatically generated amendment letters capture the entire contract history as well as the changes that were made in the current amendment. The letter templates are available for renewals, extensions, and terminations as well.

Translate contract data into business insights

Get insights from 30+ standard reports across different aspects of contract management. Get a high-level overview of your contracts at a glance with a personalized dashboard.

Stay on top of all activities

Track activities at the individual contract, user, and stage levels. Audit, access, and download logs ensure improved auditability. The data protection settings allow you to delete and anonymize counterparty data on demand.

Track and manage contractual obligations

Contextually track and manage obligations from within the contract. Allocate tasks to appropriate business stakeholders and schedule reminders. Keep abreast of the ongoing fulfillment of tasks using reports centered on obligations.

Close more deals faster with the Zoho CRM integration

Sales reps can initiate a contract and track its status from Zoho CRM. They can also initiate negotiation, signing, renewal, and amendment requests.

ZOHO

For more information on product features,
pricing, and resources, please visit our website at

zoho.com/contracts