Chandrawat & Partners

# The Digital Personal Data Protecttion Act 2023

A Comprehensive Guide

enquiries@chandrawatpartners.com | www.chandrawatpartners.co

# TABLE OF CONTENTS

# Introduction

The necessity to protect people's privacy and personal data has become an urgent concern at a time when information is rapidly becoming digital and online platforms are everywhere. India made a significant advancement by introducing the Digital Personal Data Protection Act, 2023 (the “Act”) in response to this urgent necessity.

The Act, which is India's first data protection law, is a determined effort to create a thorough framework regulating the processing of personal data inside the boundaries of the country. A determined attempt to safeguard individual rights and ensure their control over the usage and dissemination of the digital personal data is enshrined in its rules.

The Act was passed by both houses of the Parliament and the President of India's approval before it was signed into law on August 11, 2023, represents a turning point in the nation's legal system. The Act is significant as a cornerstone in the preservation of digital privacy since it is based on the understanding that people have a basic right to protect the personal data. Its scope encompasses personal data processed both online and offline, demonstrating the digital age's all-encompassing nature.

The Act includes a variety of consequences for violations, including fines and jail for specific offences, in a comprehensive move towards a more secure digital world. These sanctions serve as a symbol of the determination to uphold the Act's principles and determine any violations of data protection standards.

The Act, which India is pioneering as its first data protection law, is a sign of the country's dedication to protecting its citizens' digital rights and privacy. This historic piece of legislation ushers in an era of responsible data governance and marks a significant advancement in the worldwide conversation about digital privacy and the protection of personal data.

# Overview

A ground-breaking legislative framework created to supervise and control the processing of digital personal data inside the boundaries of India is introduced by the Act.

This important legislative achievement's core purpose is to regulate the processing of digital personal data while upholding peoples' inalienable right to protect their data privacy. The Act encompasses a range of crucial elements in the service of this overriding goal, which together highlight its importance and influence.

The protection of individual rights and privacy in the area of personal data is fundamental to the spirit of the Act. The Act guarantees the preservation of people's rights and their autonomy over their sensitive information by extending extensive regulations to control the handling of digital personal data. The Act's structure explicitly recognizes the right to protect personal data, marking a significant turn in favor of giving people more authority in the digital era.

The legislation carefully spells out rules that stress privacy and individual rights, laying a solid framework for the appropriate processing of personal data. Its requirements cover a range of aspects of data handling, including data collection, storage, use, and disclosure.

The crucial idea of informed and unambiguous permission is a pillar of the Act. The Act establishes a high bar for organizations by requiring that clear, transparent and informed consent be sought prior to the collection and processing of personal data, recognizing the importance of people's agency in how their data is used.

This encapsulates the Act's main objective, which is to make it easier to process data while upholding the rights and preferences of persons.

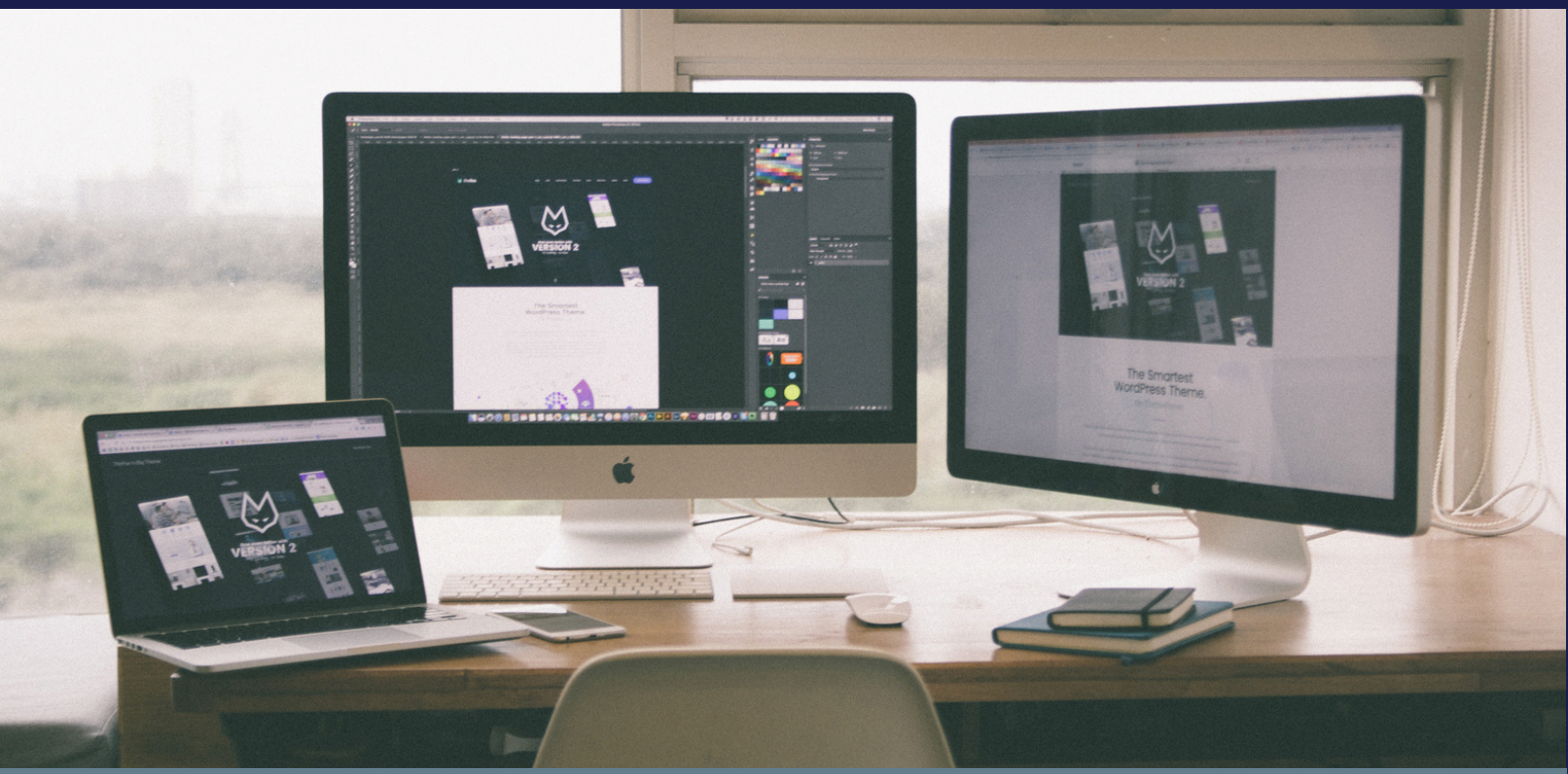
# Key provisions of the Digital Data Protection Act 2023

The Act, which is intended to control the processing of digital personal data within the borders of the country, marks an important legislative turning point for India. Its main components combine to create a solid framework that upholds data protection standards and gives people unprecedented control over their personal information.

**Key Provisions**

**Data Protection Authority:** The Act's central component is the creation of the Data Protection Authority of India (“DPAI”), a powerful organization tasked with monitoring and enforcing the Act's requirements. As a defender of data protection, the DPAI ensures compliance and upholds individual rights.

**Data Protection Officer:** In accordance with the Act's requirements, certain entities are required to designate a Data Protection Officer (“DPO”). This authorized officer takes on the responsibility of ensuring adherence to the Act's requirements and fostering a climate of responsible data handling.



# Scope and applicability of the Act

The Act, which was passed into law in India in 2023, is poised to change how digital personal data is processed while striking a careful balance between people's privacy and legal data use. At its core is the critical understanding of the right of individuals to protect their personal information, balanced with the unavoidable requirement for data to be used for legal purposes. The sole subject of this legislation is digital personal data, which includes both data that was first gathered digitally and offline data that was later converted to digital formats.

It is significant that the legislation adopts a principles-based methodology and draws comparisons to the guiding principles of the General Data Protection Regulation (“GDPR”). This attitude guides its goal of building a strong barrier of protection for people while also cultivating an atmosphere that is favorable for lawful data-driven operations. The Act marks a key step towards establishing peoples' trust in data processing by adopting these core principles and lays the road for global coherence in data protection measures.

A major accomplishment has been made in securing the processing of digital personal data inside the borders of India with the introduction of the Act. This regulation adopts a thorough approach to its applicability in order to ensure the proper management of personal data.

**Applicability Breakdown**

**Territorial applicability:** The Act only covers processing of digital personal data that takes place inside of India. This requires that every organization or person involved in the processing of such data within the nation must abide by its requirements, demonstrating the law's commitment to domestic data protection standards.

**Personal data inclusion:** The Act's embracing of a broad range of personal data is a nuanced aspect. This includes data that has been collected digitally as well as offline data that has been converted to digital format. The Act's extensive range of data types—including names, addresses identification numbers, financial information, medical records and even biometric data underscores its all-encompassing perspective.

**Data controllers and processors:** Both data controllers and data processors are covered under the legislation. The Act's rules apply to organizations that hold the position of data controllers, who are responsible for choosing the objectives and processing techniques for personal data. The requirements of the Act also apply to data processors or organizations that process data on behalf of controllers.

**Exemptions and state processing:** The Act offers exemptions for data processing carried out by the State in recognition of the complex world of national security. Although these exemptions are meant to protect important interests, caution is required to avoid the possibility of data acquisition, processing and retention that goes beyond what is technically necessary.

# Role of data protection officer

The key Responsibilities of the Data Protection Officer (“DPO”) are as follows:

**Monitoring Compliance:** The DPO's primary responsibility is to diligently monitor an organization's compliance with the requirements outlined in the Act. This includes monitoring the organization's data processing procedures to make sure they comply with legal requirements.

**Handling Complaints:** The DPO is in charge of dealing with and resolving complaints from individuals relating to the processing of their personal data, acting as a vital point of contact between them and the entity. To resolve issues and promote transparency, this function becomes crucial.

**Cooperating with data protection authority:** Collaboration with the Data Protection Authority is an essential component of the DPO's duties. This requires close collaboration with the Data Protection Authority as it performs its obligations, ensuring that regulatory goals are harmoniously aligned.

**Giving expert advice:** The DPO is required to give the entity and its workers crucial direction regarding their obligations as defined in the Act, armed with knowledge of data protection laws and regulations. The culture of informed compliance is advanced by this instruction.

**Training Mandate:** The DPO is tasked with the crucial responsibility of ensuring that staff members who process personal data obtain the necessary training on the relevant data protection laws and regulations. This training develops a workforce that is knowledgeable about ethical data practices.

**Independence and Conflict Resolution:** As a core principle, the Act calls for the independence of the DPO and forbids conflicts of interest. This aspect makes sure that the DPO's attention is constantly on protecting people's data privacy and adhering to the Act's rules.

# Appointment of data protection officer

The hiring of a DPO has a strategic significance under the Act, especially for Significant Data Fiduciaries (“SDFs”). The Act's directives provide that SDFs are directly responsible for appointing DPOs, making them the primary organizations charged with preserving data protection rules. The Act requires every data fiduciary, regardless of scale, to appoint a "grievance officer," recognizing the critical role of enabling individuals' concerns and complaints. This defined position acts as a direct point of contact for people, giving them a way to voice questions, complaints, or concerns about how their personal data is processed.

The Act's requirements are unambiguous when it comes to the DPO's residency, stating that the DPO must be located in India. This localization requirement guarantees effective communication between the data principal and the SDF and is in line with the Act's emphasis on data security inside the boundaries of the country. Beyond the residency requirement, however, the Act refrains from outlining explicit requirements for DPO appointment, giving organizations the flexibility to choose eligible personnel based on their particular settings.

In brief, the Act balances the responsibilities of the grievance officer and DPO in order to establish a responsive channel for people to communicate with data fiduciaries. In addition to highlighting the importance of data security, this combination of a dedicated DPO and a grievance officer creates a forum for people to have their voices heard within the data landscape, ultimately establishing a culture of openness, responsibility and trust.

# Responsibility and powers of Data Protection Officer

**The responsibilities of a Data Protection Officer ("DPO") include:**

**Ensuring compliance**: The DPO is in charge of making sure that the organization processes personal data in accordance with the relevant data protection laws. This includes keeping an eye on whether data protection laws and rules—like the European union EU General Data Protection Regulation (GDPR)—are being followed.

**Informing and advising:** The DPO is responsible for informing and advising the company about its legal obligations with regard to data protection. They educate people on data protection rights, obligations and responsibilities and offer guidance on how to interpret and apply data protection laws.

Monitoring and auditing: The DPO keeps an eye on how well the company complies with the rules and laws governing data protection. This entails carrying out audits, engaging in awareness-raising initiatives and training those who work in processing operations.

**Data protection impact assessments ("DPIAs"):** The DPO oversees the performance of a DPIA and offers advice and direction when one is conducted. DPIAs are carried out to evaluate and reduce risks related to processing personal data.

**Responding to requests from data subjects:** The DPO serves as a point of contact for those who have questions or requests about how their personal data is processed or how to exercise their data protection rights. They make sure that requests from data subjects to access or delete their personal information are honored or addressed.

**Cooperating with authorities**: The DPO works with data protection authorities ("DPAs") and serves as a point of contact for DPAs on matters relating to data processing. They support any enquiries or investigations made by DPAs.

# Duties of an independent Data Auditor

Significant Data Fiduciaries (“SDFs”) are required by the Digital Personal Data Protection Act of India to hire an independent data auditor, which is a crucial need. This tactical approach highlights the law's dedication to strengthen data governance and compliance, ensuring that SDFs abide by the Act's rules for protecting personal data.

**Key Duties of an Independent Data Auditor.**

**Data Integrity and Transparency:** Monitoring SDFs' adherence to data integrity and transparency is one of the independent data auditor's key responsibilities. This means guarding against impersonation or the omission of important facts while supplying information for any purpose. This alertness prevents against dishonest tactics and supports the principle of open data processing.

**Assessing privacy impact assessments and compliance**: Auditing SDFs' adherence to the Act is a key aspect of the independent data auditor's duties. Examining procedures, techniques, and data management plans is necessary to make sure they comply with regulations. Additionally, the auditor undertakes the responsibility of carrying out privacy impact analyses, a procedure crucial in understanding and minimizing potential privacy hazards.

**Monitoring compliance with the Act:** The independent data auditor's critical responsibility is to keep an eye on the SDF's continuous compliance with the Act. The proactive inspection reinforces the dedication to responsible data management by acting as a safeguard against any departures from data protection rules.

# Penalties and non-compliance

A strong system of sanctions intended to secure data privacy and compel compliance underlines the Act's objectives. By defining maximum fines for particular infractions and comprehensively addressing non-compliance by data fiduciaries and Data Principals, the Act adopts a strong attitude toward responsibility.

**Key Aspects of Penalties:**

**Non-Compliance by Data Fiduciaries:** The Act stipulates severe penalties for non-compliance by data fiduciaries. Such infractions may result in fines of up to INR 250 crore in the financial sense. This hefty fine emphasizes how seriously the Act takes the duty of data fiduciaries to enforce data protection rules.

**Obligations of data principals:** The Act imposes compliance obligations on data principals or the people whose personal data is being processed. If data principals are shown to be in breach of their obligations, fines of up to INR 10,000 (about GBP 100) may be applied. The importance of individual compliance with data privacy laws is emphasized by this clause.

**Uniform penalties for breaches:** The Act imposes uniform sanctions for violations, regardless of the organization's annual revenue. This eliminates financial inequalities and guarantees that all infractions are subject to the same maximum punishment.

**Financial consequences of breaches:** The Act's ability to enforce data privacy through monetary penalties is a key feature. These monetary penalties may be triggered by any violation of data protection policies or failure to comply with the Act, acting as a concrete deterrent against data misuse and highlighting the value of prudent data management.

# Obligation of data fiduciary and data principle

The Act establishes a thorough set of requirements that data fiduciaries must diligently follow. These requirements highlight the legislation's goal of creating a moral and responsible data environment that prioritizes people's rights and privacy.

**Key Obligations of Data Fiduciaries:**

**Accuracy upkeep:** Upkeep of the accuracy of the personal data that is processed by data fiduciaries is a requirement of responsible data management. This dedication to data accuracy strengthens people's confidence in data custodians and acts as a precaution against false information.

**Data security**: Within the Act, data fiduciaries are required to maintain the security of any personal data that falls within their control. This means putting in place suitable and effective safeguards to defend against unauthorized access, breaches or abuse of data, ultimately protecting the sensitive data of individuals.

**Lawful data processing:** Data fiduciaries are required to only process personal information for legitimate purposes. Either the data principal's consent is required for this processing, or it must be judged necessary for the precise purposes listed in the Act. This clause prevents improper or illegal data processing.

A symbiotic relationship between people and data fiduciaries is reflected in the Act which imposes certain requirements on data principals. These commitments are focused on encouraging an informed and empowered data landscape, protecting the integrity of personal data, and participating in data in an ethical manner.

**Data Deletion:** A fundamental principle of data protection requires data fiduciaries to destroy personal data after its intended use has been satisfied. This clause makes sure that data is not kept around longer than is necessary, encouraging ethical and appropriate data management.

**Key obligations on data principals:**

**Data accuracy:** It is the responsibility of data principals to provide accurate personal information to data fiduciaries. This dedication to correctness strengthens data processing's dependability by guaranteeing that the information supporting decisions and actions is founded on reliable data.

**Consent provision:** With some limitations outlined in the Act, data principals are required to give their consent for the processing of their personal data, which is a crucial aspect of individual agency. By ensuring that persons participate in the processing of their own data in an informed manner, this clause protects their rights and privacy.

**Exercise of rights:** The Act gives data principals a range of rights aimed at giving them control over their personal data. These rights include the ability to ascertain the type of processed data, ask for its deletion, fix errors, keep information current, and exercise control by restricting or objecting to data processing.

**Breach reporting:** Data principals are encouraged to report breaches of their personal data to the appropriate authorities in order to promote a sense of collective data accountability. This cooperative strategy supports data protection initiatives by bringing together individuals, data fiduciaries, and regulatory organizations.

**Contextual variability:** It is important to recognize that the obligations of data principals may change depending on the particular context of processing personal data. The complexity of data processing highlights how adaptable the Act is in adjusting requirements to fit certain situations.

# Future of data privacy regulation

A variety of dynamic elements that interact to form a comprehensive framework are positioned to have an impact on how data privacy policy develops in India.

**Enactment of the Digital Personal Data Protection Act:** The recent adoption of the Act by the Indian Parliament represents a significant advancement in the modernization of the data protection environment in that nation. Upon announcement from the government, the Act's upcoming adoption could bring India's data protection framework up to pace with international standards, demonstrating the country's commitment to protecting personal data.

**Growing data privacy concerns:** As society moves toward a more digital future, there are more people who are concerned than ever about data privacy and the security of personal information. There is a growing desire for strict data protection laws as people become more aware of their data rights, which reflects a social push for better privacy protections.

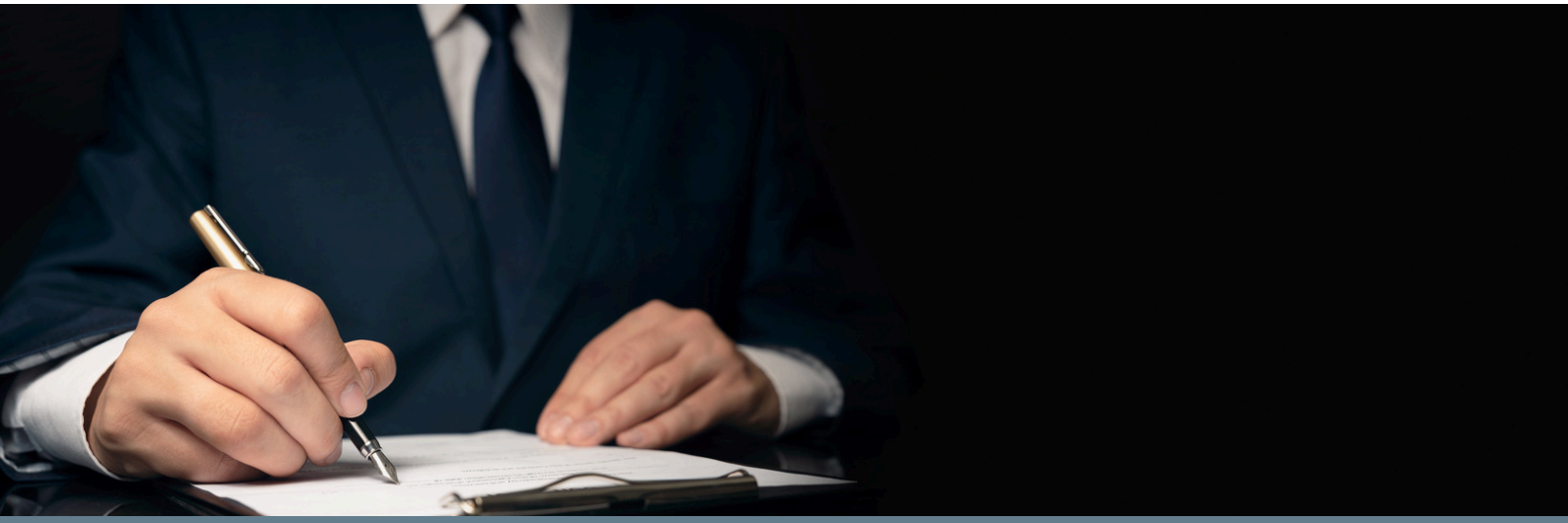
**Digital transformation and cyber security:** The rapid digitization sweeping across India has augmented the urgency for robust information and cyber security measures. Organizations are recognizing the necessity of investing in comprehensive data protection technologies and strategies to mitigate cyber threats in this evolving digital landscape.

**Adoption of emerging technologies:** The incorporation of cutting-edge technologies like block chain, the Internet of Things, and artificial intelligence creates new complexity in the protection of data privacy. Keeping up with these breakthroughs and developing strategies to ensure that personal data is protected in the face of technological advancements is a problem for regulators.

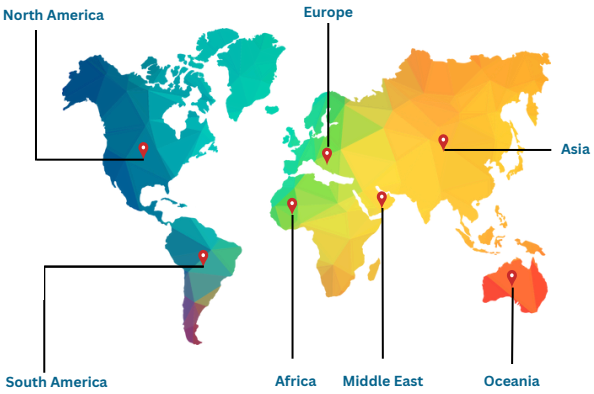
# How we can help?

By offering the following services, our team can help organizations comply with the Act:

- Our team would assist our clients to provide data protection officer to comply with the provisions of the Act and protect the digital privacy and data of our clients.
- Our team can assist by undertaking a comprehensive analysis of the organization's data privacy standards. This evaluation will assist in identifying the areas where the organisation needs to make improvements in order to adhere to the rules.
- Our team of professionals can assist in creating a thorough privacy policy that complies with the Act's standards. This policy will ensure accountability and openness.
- Our team can assist in setting up solid consent management systems which includes putting in place procedures that allow people to quickly withdraw their consent if they so want.
- Our professionals can assist in developing a data breach response plan. This plan will detail the actions to be done to lessen the effects of a breach, notify those who might be impacted and adhere to legal requirements.



## SERVING CLIENTS WORLDWIDE






# Key Contact

**Surendra Singh Chandrawat**

Managing Partner

surendra@chandrawatpartners.com

*Connect Surendra on*

LinkedIn WhatsApp

Chandrawat & Partners is a leading and rapidly growing full-service firm providing high quality professional and corporate services to foreign and local clients, representing companies and individuals in a wide range of sectors through separate entities established in various countries worldwide.



Follow us on: LinkedIn twitter facebook Instagram