



# The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2026

Editor-in-Chief – Dr. Muktai Deb Chavan; Publisher – Alden Vas; ISSN: 2583-9896

This is an Open Access article distributed under the terms of the Creative Commons Attribution-Non-Commercial-Share Alike 4.0 International (CC-BY-NC-SA 4.0) License, which permits unrestricted non-commercial use, distribution, and reproduction in any medium provided the original work is properly cited.

---

## Governing Data in Corporations: A Critical Study of DPDP Act 2023 and its Compliance Lacunas

*By: Chetna Parashar*

### Introduction

The Digital Personal Data Protection Act, 2023 (DPDP) is a recently enforced legislature with the purpose to ensure protection of personal data in the digital ecosystem while ensuring fair data processing by the State and private entities to ensure the fundamental right of privacy as declared by the 9-judge bench in the landmark judgement of *K.S Puttaswamy v. Union of India*<sup>1</sup> and to prevent any kind of misuse or exploitation of personal data.

For enabling such accountability and protection of data at digital platforms DPDP Act provides procedures which govern the collection, storage, sharing of such data in a lawful manner. This also imposes a legal duty on entities like corporate and government bodies in regards to procession of data and a fiduciary responsibility that if breached can lead to penalties as per the provisions of the act.

Though the purpose of the act is entirely the protection of digital personal data and ensure accountability of organisations in case of such breach, still many lacunas persist within the procedural aspect of this act that can lead to its incompliance and further nullifying the purpose of the act. This blog focuses on such gaps that can appear in the application of this law which need to be filled for the better enforcement of this act.

---

<sup>1</sup> Justice K.S. Puttaswamy (Retd.) v. Union of India (2017) 10 SCC 1.

## Compliance provisions for Corporations

Certain compliance provisions that corporations need to adhere to under the DPDP Act are as follows:

1. **Purpose of Data Collection:** Under the DPDP Act, a corporate is specifically considered to be a data fiduciary<sup>2</sup> or data processor<sup>3</sup> which brings them under the direct regulatory framework. The DPDP uses governing mechanisms for the regulation of data collection done by corporate entities which examines the entry control of data where the primary focus is upon the fact whether the data is collected for lawful purposes or not<sup>4</sup>. Further clear nature of data collected also needs to be revealed by the corporations, this results in corporations no longer being able to engage in opaque data harvesting.
2. **Usage of Data:** According to the DPDP Act, the corporations can only use the personal data collected only for mentioned purposes and secondary exploitation without consent can be penalised<sup>5</sup>. Such provisions ensure the safety and privacy of individuals safeguarded without being compromised.
3. **Retention of Personal Data:** The companies cannot retain personal data after its purpose is fulfilled. Doing such act is considered lawful so long as it is considered to fall under necessity which will be decided on the fact whether such is necessary to adhere to compliance of some other law<sup>6</sup>.
4. **Security Safeguards:** According to this 2023 act the companies are legally required to implement reasonable security safeguards in order to protect the data from any kind of unlawful breach and in case of breach the corporate entity is required to notify the Data Protection Board of India<sup>7</sup>. This provision ensures that protection of collected personal data is the legal duty of the corporations and any breach due to negligence will lead to breach of their legal responsibility under the act.

---

<sup>2</sup> Digital Personal Data Protection Act, § 2(i), 22, Act of Parliament, 2023 (India).

<sup>3</sup> Digital Personal Data Protection Act, § 2(k), 22, Act of Parliament, 2023 (India).

<sup>4</sup> Digital Personal Data Protection Act, § 4, 22, Act of Parliament, 2023 (India).

<sup>5</sup> Digital Personal Data Protection Act, § 6, 22 of 2023, Act of Parliament, 2023 (India).

<sup>6</sup> Digital Personal Data Protection Act, § 8(7), 22 of 2023, Act of Parliament, 2023 (India).

<sup>7</sup> Digital Personal Data Protection Act, § 8(5) & (6), 22 of 2023, Act of Parliament, 2023 (India).

5. **Significant Data Fiduciaries:** According to the DPDP Act, for the governance of data collected by the corporations which are at higher risk of harm to data principles laid down under the Act will be notified by the central government as under the 'SDF.' Such corporations listed as SDFs must institutionalise data protection into their organisational structure along with mandatory appointment of a Data Protection Officer also known as DPO for ensuring further protection of Personal DATA which stored in such high-risk corporations<sup>8</sup>.

## Compliance Risks for the Corporations

Despite the above-mentioned regulatory provisions enforced under good faith and better governance of digital data to curb misutilisation and breach of privacy, still the compliance risks for corporations in regards to these provisions prevail which are discussed below:

1. **Determination of Unlawful Purpose:** As discussed above, it was identified that under the DPDP Act the corporations must collect data only for lawful purposes, however the term 'lawful' is not exhaustively defined under the act which leaves a wide gap in its interpretation which may be only resolved post facto after tests or conditions are laid down by courts.
2. **Strict Purpose Limitation:** The purpose limitation under the DPDP Act, according to which the data can be used for the purpose for which it has been consensually collected from the individually and secondary usage is strictly prohibited, unless explicit consent is acquired results in a hefty limitation for the corporations as most companies further make coordination based on such data collected between businesses, market and compliance teams.
3. **Significant Data Fiduciaries:** The companies notified by Central government under the category of SDF will have certain exclusive provisions that they need to comply to, such as appointment of a DPO, however, despite the appointment of such officer being done to implement an internal data regulatory mechanism, this office still lacks

---

<sup>8</sup> Digital Personal Data Protection Act, § 10, 22 of 2023, Act of Parliament, 2023 (India).

independence and if the DPO is subordinated to business interest, the statutory intent of preventive governance is defeated, further creating a compliance risk for the corporation instead.

## **Conclusion**

The Digital Personal Data Protection Act, 2023 marks a significant shift in India's approach to governing personal data in corporations by introducing multiple regulatory frameworks. By classifying corporations as data fiduciaries and, in high-risk cases, as Significant Data Fiduciaries, the Act embeds data protection within corporate governance and compliance mechanisms. However, despite its progressive intent, several compliance lacunas persist. The Act leaves key concepts such as "lawful purpose," criteria for SDF designation, and standards for "reasonable security safeguards" largely undefined, creating interpretational uncertainty for corporations. Thus, leading to a necessity of further tests and conditions being established for better and specific application of law. These gaps and lacunas need to be filled for better implementation, establishing clear protocols that will further ensure uniform governance without which the purpose of the act remains unfulfilled.