IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Objects, Right And Obligations Of The Data Principal Under DPDP Act 2023

Alamelu

This article is written by Alamelu, Guest Faculty at Tamilnadu Dr. Ambedkar Law University, Chennai. It deals with the object and purpose of the Indian Digital Personal Data Protection Act 2023. It further explains the provisions of the Act such as definition of key terms, right and obligations of the Data Principal and Duties of Data Fiduciary as per the Act.

Introduction:

The Indian Digital Personal Data Protection Act 2023 (DPDP Act)1 represents a significant milestone in India's journey towards robust data protection and privacy regulations. It represents a landmark development in India's legislative landscape, aimed at fortifying the protection of personal data in an increasingly digital world. This legislation aims to safeguard the personal data of individuals while balancing the needs of businesses and the government. Here is a comprehensive overview of the key aspects of the DPDP Act and elucidating its key provisions, principles, and implications.

The DPDP Act was enacted in response to escalating concerns over data privacy and the absence of a robust legal framework to safeguard personal data in India. The DPDP Act is inspired by global standards, such as the European Union's General Data Protection Regulation (GDPR) and from China's Personal Information Protection Law (PIPL)2, yet it is tailored to address the unique socio-economic and technological landscape of India. The enactment of this legislation marks a significant stride towards aligning India with international data protection norms, thereby enhancing its global standing in the digital economy.

Object and Purpose of the DPDP Act

The primary object of the Digital Personal Data Protection Act is to provide a robust legal framework for the protection of personal data in the digital environment. This includes:

Safeguarding Personal Data: Ensuring that personal data is collected, processed, stored, and shared in a manner that protects the privacy and rights of individuals.

Regulating Data Processing: Establishing clear guidelines and standards for the lawful processing of personal data by data controllers and processors.

Empowering Individuals: Granting individuals greater control over their personal data, including rights to access, correct, and delete their data.

Promoting Transparency: Mandating transparency in data processing activities, ensuring that individuals are informed about how their data is being used.

Ensuring Accountability: Holding data controllers and processors accountable for their data processing activities, including compliance with the DPDP Act and any associated regulations.

Protecting Privacy: To protect the fundamental right to privacy of individuals by ensuring that their personal data is handled with care and respect.

Fostering Trust: To build and maintain trust in digital services and technologies by ensuring that personal data is processed in a secure and transparent manner.

Facilitating Innovation: To create a balanced regulatory environment that allows for innovation and growth in the digital economy while safeguarding personal data.

Harmonizing Standards: To align with international data protection standards and best practices, facilitating cross-border data flows and cooperation.

Enhancing Security: To enhance the security of personal data by implementing stringent data protection measures and protocols.

Providing Remedies: To provide individuals with effective remedies and recourse in the event of data breaches or violations of their data protection rights.

History of India Digital Personal Data Protection Act

Before 2022, India lacked a comprehensive privacy law. In 2017, the Supreme Court of India acknowledged the right to privacy as a constitutionally protected right in the "Puttaswamy judgement"3 also known as the Right to Privacy verdict. The court also highlighted India's absence of a comprehensive privacy law and the limitations of the existing Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, or SPDI Rules, which were implemented in 2011. Following the Right to Privacy verdict, the Indian government developed draft legislation aimed at protecting the privacy of Indians. Earlier versions of the Personal Data Protection Bill faced significant scrutiny and were ultimately unsuccessful, including the Data Protection Bill 2021, which bore some similarities to the European Union's General Data Protection Regulation (GDPR). This bill was withdrawn in August 2022. On November 18, 2022, the Ministry of Electronics and Information Technology proposed the Digital Personal Data Protection Bill 2022. This bill was intended to replace certain parts of existing law (Section 43A of the IT Act) and the SPDI Rules4 and was finalized as India's Digital Personal Data Protection Act (DPDP Act) when it received approval from both houses of Parliament and the assent of the President in August 2023. The law came into effect August 11, 2023 and covers personal data collected in digital format, or collected by other means and later digitized.

Key Definitions

Personal Data

"Personal data" means any data about an individual who is identifiable by or in relation to such data.5

Any information that relates to an identified or identifiable individual.

Data Principal

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

(i) a child, includes the parents or lawful guardian of such a child;

(ii) a person with disability, includes her lawful guardian, acting on her behalf.6

The term "Data Principal" refers to the individual to whom the personal data pertains. This definition encompasses specific considerations for certain groups of individuals. When the Data Principal is a child, the term extends to include the parents or lawful guardian of the child. This means that the parents or lawful

guardian are considered the Data Principal in relation to the child's personal data. When the Data Principal is a person with a disability, the term includes her lawful guardian who acts on her behalf. This ensures that the lawful guardian is recognized as the Data Principal in matters concerning the personal data of the person with a disability. The definition of "Data Principal" is inclusive, ensuring that children and persons with disabilities are represented by their lawful guardians in matters related to their personal data.

Data Fiduciary

"Data Fiduciary" means any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data.7

Any person, including the State, a company, any juristic entity, or any individual who alone or in conjunction with others determines the purpose and means of processing personal data. Essentially, a Data Fiduciary is responsible for the collection, storage, and processing of personal data and must ensure that these activities are conducted in compliance with the provisions of the DPDP Act. Few examples of Data Fiduciary:

Tax Authorities: Collect and process personal data for tax assessment and collection.

E-commerce Websites: Platforms like Amazon and Flipkart collect and process personal data for online shopping and transactions.

Banks: Collect and process personal data for account management, loans, and other financial services.

Hospitals and Clinics: Collect and process personal data for patient care and medical records, etc.

Data Processor

"Data Processor" means any person who processes personal data on behalf of a Data Fiduciary.8

A data processor is an entity or individual who processes personal data on behalf of a data fiduciary. The data processor does not own the data but handles it according to the instructions and purposes defined by the data fiduciary and within the legal framework of the DPDP Act.

Examples of Data Processors:

- Cloud service providers who store data on behalf of a company.
- Third-party analytics firms that analyse data for another organization.
- Payroll companies that manage employee data for other businesses.

Scope and Applicability

The DPDP Act applies to the processing of digital personal data within the territory of India where the personal data is collected in (i) digital form; or (ii) non-digital form and digitised subsequently. It applies to the processing of digital personal data within India, and to data fiduciaries and data processors outside India if they process personal data in connection with any business carried out in India, or if they offer goods or services to data principals within India. DPDP Act does not apply to an individual who processes such personal data for any personal or domestic purpose. This means that activities such as maintaining a personal address book, family photo albums, or personal correspondence are exempt from the regulations. DPDP Act does not apply to data made publicly available by the data principal themselves or by law.

Rights of Data Principal

The DPDP Act grants several rights to data principals, empowering individuals to have greater control over their personal data.

Right to access information about personal data: The Data Principal, who has previously given consent to a Data Fiduciary for the processing of their personal data, has the right to request certain information from that Data Fiduciary. Upon making a request in the prescribed manner, the Data Principal can obtain:

(a) a summary of the personal data being processed and the processing activities undertaken by the Data Fiduciary;

(b) the identities of all other Data Fiduciaries and Data Processors with whom the personal data has been shared, along with a description of the shared data; and

(c) any other prescribed information related to their personal data and its processing.

However, the requirements to provide information under clauses (b) and (c) do not apply if the personal data is shared with another Data Fiduciary authorised by law for purposes such as the prevention, detection, investigation, prosecution, or punishment of offences or cyber incidents, provided the request for such data sharing is made in writing.

Right to correction and erasure of personal data: A Data Principal has the right to request the correction, completion, updating, and erasure of her personal data, for which she has previously given consent, in accordance with applicable laws. Upon receiving such a request, a Data Fiduciary must correct the inaccurate or misleading data, complete the incomplete data, and update the personal data. For erasure requests, the Data Fiduciary must erase the data unless it is necessary to retain it for specified purposes or legal compliance.

Right of grievance redressal: the Data Principal is entitled to grievance redressal mechanisms provided by the Data Fiduciary or Consent Manager for any issues related to personal data handling. The Data Fiduciary or Consent Manager must respond to grievances within a prescribed period, and the Data Principal must exhaust these grievance mechanisms before approaching the Board.

Right to nominate: the Data Principal can nominate another individual to exercise her rights in the event of her death or incapacity, defined as the inability to exercise her rights due to unsoundness of mind or physical infirmity.

Duties of Data Principal

A Data Principal is required to adhere to several duties, including complying with all applicable laws while exercising their rights under the DPDP Act. They must not impersonate others when providing personal data for specified purposes and should avoid suppressing any material information when submitting personal data for documents or identifiers issued by the State. Additionally, they should refrain from registering false or frivolous grievances or complaints with a Data Fiduciary or the Board. Lastly, they must ensure that any information provided for correction or erasure is verifiably authentic.

Obligations of Data Fiduciary

Data Fiduciaries have several obligations under the DPDP Act to ensure the protection of personal data.

A person may process the personal data of a Data Principal only in accordance with the provisions of the DPDP Act and for a lawful purpose, which includes obtaining the Data Principal's consent or for certain legitimate uses. A lawful purpose is defined as any purpose not expressly forbidden by law.

Requests for consent must be accompanied or preceded by a notice from the Data Fiduciary, detailing the personal data to be processed, the purpose, the Data Principal's rights, and the complaint process. The consent given by the Data principal must be free, specific, informed, unconditional, and unambiguous with a clear affirmative action, and the Data Principal has the right to withdraw consent at any time. The Data Fiduciary must cease processing the data upon withdrawal of consent unless otherwise required by law. Consent can be managed through a Consent Manager, who must be registered and accountable to the Data Principal. Every Consent Manager shall be registered with the Board in such manner and subject to such technical, operational, financial and other conditions as may be prescribed. The Data Fiduciary must prove that proper notice was given by her to the Data Principal and consent were obtained from such Data Principal to the Data Fiduciary if questioned in a proceeding in this regard.

Data Fiduciary is accountable to the Data Principal and irrespective of any agreement to the contrary or failure of a Data Principal to carry out the duties provided under DPDP Act, she must implement appropriate measures to ensure compliance with the DPDP Act.

The Significant Data Fiduciary, any Data Fiduciary or class of Data Fiduciaries as may be notified by the Central Government, conduct assessments called "Data Protection Impact Assessments" for processing activities that pose a high risk to data principals rights and freedoms. Data Fiduciary must notify the Data Protection Authority and affected data principals in the event of a data breach. Data Fiduciary may appoint Data Processor to process personal data on its behalf for any activity related to offering of goods or services to Data Principals under a valid contract.

Data Protection Authority

The DPDP Act 2023 establishes that the Central Government may, by notification, appoint, for the purposes of this DPDP Act, a Board to be called the Data Protection Board of India (DPBI) responsible for overseeing the implementation and enforcement of the DPDP Act. The DPBI has the power to:

- Monitor and enforce compliance with the DPDP Act
- Investigate data breaches and complaints
- Impose penalties for non-compliance
- Issue guidelines and codes of practice

Penalties

Failure to adhere to the requirements of the DPDP Act, particularly the breach of essential information security measures necessary to reduce the risk of a personal data breach, may result in fines reaching 250 crore INR ($30 million). This penalty is less stringent than the 2022 legislation, which suggested fines of up to 500 crore INR (approximately $61 million).

Conclusion

The Indian Digital Personal Data Protection Act 2023 is a pivotal piece of legislation that aims to fortify data privacy and protection in India. By establishing clear guidelines and robust enforcement mechanisms, the DPDP Act seeks to build trust in the digital ecosystem and ensure that personal data is handled with the utmost care and responsibility. As businesses and individuals navigate the new regulatory landscape, the DPDP Act 2023 will play a crucial role in shaping the future of data protection in India.

References

1. https://www.meity.gov.in/writereaddata/files/Digital%20Personal%20Data%20Protection%20Act%202023.pdf
2. https://usercentrics.com/knowledge-hub/india-digital-personal-data-protection-act dpdpa/#:~:text=The%20DPDP%20Act%20is%20a,to%20control%20and%20protect%20it.
3. Puttaswamy V Union of India, SC, 2017 (10)
4. https://www.digitalguardian.com/blog/what-indias-digital-personal-data-protection-dpdp-act-rights-responsibilities-everything-you.
5. Section 2 (t) of the DPDP Act.
6. Section 2 (j) of the DPDP Act
7. Section 2 (i) of the DPDP Act
8. Section 2(k) of the DPDP Act