The Indian Journal for Research in Law and Management

Open Access Law Journal – Copyright © 2024

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

DIGITAL PERSONAL DATA PROTECTION ACT (DPDPA)

A powerful tool for corporate transformation, if properly examined, is the vast amounts of digital data created by the ubiquitous use of information, communication, and technology (ICT). Market participants are working hard to get access to data and use it to find possibilities. IDC predicts that 175 trillion Zettabytes of data will be generated globally by 2025.Nearly 700 million people in India use the internet regularly, and 467 million of them use social media, which generates enormous amounts of digital data. India is now the second-largest internet market as a result. Digital data generation, ownership, sharing, data protection, and the upkeep of mutual trust among data transmitters have increased significance now that it has become a ubiquitous business enabler.

The spirit of the Organization for Economic Co-operation and Development (OECD) guideline, which states that data privacy should be recognized as the worldwide minimum norm for privacy and data protection, is also followed in articulating DPDPA since laws protecting data privacy are crucial. It provides a strong basis for establishing global standards for transferred data flows as well as efficient individual protection and trust. In order to expand the scope of advances and adapt data privacy guidelines in today's digital environment, the OECD regularly collaborates with nations and experts. The organization advocates for a comprehensive approach to privacy and data protection. The process of creating and updating data protection legislation is never-ending.

In a similar vein, the need of privacy and data protection is becoming more widely acknowledged, according to the United Nations Conference on Trade and Development (UNCTAD), since more and more social and commercial activities are being conducted online. It is not permissible to

gather, use, or share personal information with other parties without the knowledge or consent of the consumer, and data protection laws are required. In this regard, 137 of the 194 nations have laws in place to ensure data security and privacy, and India has joined the group.

In order to protect the interests of all parties involved, DPDPA offers complete data protection together with the necessary reinforcing checks and balances. Examining the DPDPA in detail will be fascinating to comprehend the obligations it places on various parties as well as the legal penalties it imposes in order to guarantee compliance.

Key stakeholders: Of the several parties involved in the act, a few are crucial to understanding its protective framework since they provide a well-insulated data protection environment.

(i) The data owner, or Data Principal (DP). DP may refer to people or organizations whose data needs to be secured. For the data to be generated and processed, the DP must provide explicit consent specifying the intended use of the data. DP has the right to limit its use or revoke consent at any time.

(ii) A company that gathers, stores, and shares data is known as a data fiduciary. In addition, a data fiduciary serves as a "Consent Manager," providing a DP with an easily accessible, transparent, and interoperable platform to grant, manage, evaluate, and revoke consent. When they prove to be systemically significant, the Central Government may designate any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciaries based on an evaluation of pertinent factor.

.

(iii) An organization handling data on behalf of a data fiduciary is known as a data processor. In some tiny businesses, the roles of data processor and data fiduciary may also be interchangeable. A Data Fiduciary may designate any person as a Data Protection Officer (DPO) in accordance with the terms of this Act.

(iv) The government's Data Protection Board of India (DPBI) is responsible for identifying and safeguarding any personal data that is in its custody or under its control by implementing appropriate security measures to avert data breaches. Any order made by

the DPBI may be appealed to the High Court. All appeals under this section must be filed within sixty days of the date of the order that is being appealed.

(v) Any infraction could be brought before the High Court Suo moto. Simultaneously, no injunction shall be given by any court or other authority with respect to any action taken under the terms of this Act, nor shall any civil court have the jurisdiction to accept any litigation or take any action in respect of any matter under the provisions of this Act.

(vi) Only in compliance with the provisions of this Act and the Rules issued thereunder, and for a legitimate purpose for which the DP has granted or is presumed to have granted consent, may an individual process the personal data of a DP.

(vii) Cross-border data storage: Since its enactment in 2018, the General Data Protection Regulation (GDPR) of the European Union (EU) has served as the model for a global upsurge in new data protection laws. In the hopes of receiving a positive adequacy finding from the European Commission that would permit unrestricted data flow between their nation and the European market, some politicians from around the world have pursued equivalence with GDPR.

Gartner projects that by 2023, 65 percent of the world's population will have their personal information protected by contemporary privacy laws. Under the DPDPA, which also takes into account international trade and mutual cooperation, the central government may, following an evaluation of relevant factors, notify foreign nations or territories to which a Data Fiduciary may transfer personal data, subject to the terms and conditions that may be specified. Data should be stored in India and may be transferred outside India for processing if explicitly consented to by the data principal for such transfer and subject to certain additional conditions.

Penalty for infringement: There may be monetary fines for any data protection violations or DPDPA noncompliance. Following an investigation that determines a person's noncompliance to be severe, the DPBI may, after affording the person a fair chance to be heard, impose a pecuniary

penalty of up to rupees five hundred crore (the highest limit) in each case. However, the pecuniary penalty might be as high as Rs. 250 crores for a data processor or fiduciary, or as little as Rs. 10,000 for a data principal (the owner of the data), depending on the severity of the act breach and the provisions violated However, the DPBI shall consider the following factors when determining the amount of a financial penalty to be imposed under sub-section (1) of DPDPA: (a) the nature, gravity, and duration of the non-compliance; (b) the type and nature of the personal data affected by the non-compliance; (c) the non-repeated nature of the non-compliance; (d) whether the person has realized a gain or avoided any loss as a result of the non-compliance; (e) whether the person took any action to mitigate the effects and consequences of the non-compliance, and the timeliness and effectiveness of that action; (f) whether the financial penalty to be imposed is proportionate and effective, having regard to achieving compliance and deterring non-compliance with the provisions of this Act; and (g) the probable effects on the individual of the financial penalty being imposed.

In conclusion the DPDPA's passage has the potential to fundamentally alter how digital personal data is managed and regulated, safeguarding its sanctity and privacy. It will open the door to the mindful gathering, storing, and safeguarding of digital data, keeping the data subject at the heart of decisions about how to utilize it.