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

INTRODUCTION

As technology spins its ever-widening web, our personal data hangs ever more exposed. Enter the Digital Personal Data Protection Act of 2023 (DPDP) – a formidable shield erected to safeguard this digital lifeblood. This landmark act casts its protective gaze not just on data born in the digital realm, but also on any offline whispers later digitized.

With cybercrime and data breaches swirling like digital cyclones, public anxieties surrounding our online footprints have reached a fever pitch. The DPDP emerges as a balm, meticulously outlining the responsible handling of personal information. From its cradle of collection to its vault of storage, every step in the data dance must now adhere to rigorous security measures. And most importantly, at the heart of this data tango lies informed consent – the individual's explicit nod of approval before their information takes flight. This act is more than just lines of legalese; it's a fundamental right enshrined in digital ink. It's a bulwark against the erosion of privacy, a safeguard against the potentially devastating consequences of data breaches for individuals and businesses alike. It's a promise whispered to every citizen: your digital self deserves a fortress, and the DPDP is the key that unlocks its gates. So, as you navigate the ever-evolving digital landscape, remember – the DPDP stands watch, a vigilant sentinel guarding your right to privacy in the age of information.

JURISDICTION AND SCOPE

Stretching its protective arms beyond Indian borders, the DPDP Act safeguards not only personal data processed within the country, but also any such data pertaining to Indian residents, even if handled abroad. No organization, foreign or domestic, escapes its purview when it comes to

collecting and processing this vital information. Furthermore, the Central Government holds the power to tighten the reins, potentially restricting the outward flow of data for outside processing. In essence, the DPDP Act casts a wide net, encompassing government agencies, businesses, and non-profit organizations – no entity that handles personal data stands exempt from its watchful gaze.

LEGITIMATE PURPOSE FOR PROCESSING OF PERSONAL DATA

Under the DPDP Act, there are circumstances where the processing of personal data can proceed without requiring explicit consent from the data principal. These legitimate purposes include

Voluntary Submission: Data principals willingly providing their information for a clearly defined purpose.

State Functions and Legal Obligations:Data processing necessary for the state to fulfill its functions or meet legal obligations.

Court Orders: Compliance with judicial decisions, decrees, or orders.

Medical Emergencies :Life-or-health-threatening situations involving the data principal.

Disasters and Public Order Breakdowns: Data processing essential during crises or disruptions to public order.

Employment Purposes and Employer Protection:Data usage for employment-related activities and safeguards against employer losses or liabilities.

Medical Services During Public Health Threats:Data processing for the provision of medical services during epidemics, disease outbreaks, or other public health risks.

A SHIELD FOR YOUNG MINDS: DPDP ACT'S PROTECTIONS For CHILDREN

Recognizing children's heightened vulnerability in the digital age, the DPDP Act stands as a vigilant guardian, weaving a protective web around their personal data. At its core, the Act requires data fiduciaries – anyone handling a child's information – to seek the unambiguous consent of the child's parent or legal guardian before embarking on any data processing journey.

But the Act's shield extends beyond mere consent. It recognizes that not all data is equal, especially when it comes to children. Sensitive information that could negatively impact a child's well-being is deemed off-limits for processing. This encompasses everything from harmful stereotypes and profiling to data that could exploit or endanger them. Imagine the potential repercussions of a child's medical history falling into the wrong hands, or personalized ads bombarding them with age-inappropriate content. The Act acts as a firewall against such scenarios, prioritizing the child's right to a safe and healthy online environment.

The DPDP Act, therefore, becomes not just a legal framework, but a social pledge. It is a recognition that protecting children online requires a collective effort, where data fiduciaries, parents, and society at large must work together to build a safer, more responsible digital ecosystem for young minds to thrive. And with its comprehensive measures, the Act takes a significant step towards fulfilling this vital promise.

GRIEVANCES REDRESSAL

Armed with the DPDP Act, the central government can establish a data-guiding sentinel: the Data Protection Board of India. This independent entity, wielding its own corporate identity and legal stature, will stand as a stalwart protector of personal information. The Board's leadership, handpicked by the central government, will draw upon expertise in data governance, conflict resolution, and consumer protection – fields vital to navigating the intricate landscape of data rights. Each member will carry the torch of responsibility for a two-year term, ensuring a dynamic flow of fresh perspectives within the Board.

CASE STUDY: K.S. PUTTASWAMY V/S UNION OF INDIA

A lone challenge echoed through the halls of the Supreme Court in 2015. Justice K.S. Puttaswamy, retired from the Karnataka High Court, questioned the Aadhaar card scheme and its potential to shatter the edifice of individual privacy. In a resounding response, a nine-judge bench in 2017 unanimously ruled that privacy, nestled within Article 21 of the Constitution, was a fundamental right, deserving of fierce protection.

Recognizing the urgent need for legislative armor, the Supreme Court forged the Srikrishna Committee, led by Justice B.N. Srikrishna, in 2017. This dedicated team drafted the Personal

Data Protection Bill, 2018, a blueprint later revised in 2019. After meticulous polishing by the Joint Parliamentary Committee, the bill re-emerged in 2021, bearing a new name: the Digital Personal Data Protection Bill. A swift passage through both houses of Parliament in August 2023, followed by the President's nod, transformed the bill into a powerful law.

But this wasn't a blank canvas. Digital data had previously danced to the tune of the Sensitive Personal Data or Information (SPDI) Rules, established under the IT Act, 2011. However, the DPDP Act marked a turning point, notably severing ties with Section 43-A of the IT Act, which once offered compensation for negligence in upholding SPDI rules. It's a story of resilience, adaptation, and a collective commitment to protecting the fundamental right to privacy in the ever-evolving digital age.

CONCLUSION

A positive stride has been Started by the Indian Government through the Establishment of the Digital Personal Data Protection Act 2023. This legislation aims to safeguard the personal data of individuals online and ensure that businesses adequately protect their data.