De Jure

December 3, 2024

Rajani Associates
simple solutions

INTRODUCTION

In the pre-digital era, the sharing of personal information was largely entrusted to individuals, institutions, or the state by handing over physical copies of documents/ information. The entities receiving such information operated in the absence of a comprehensive legal framework, which resulted in limited accountability and governance.

THE DIGITAL SHIFT: EVOLUTION AND CHALLENGES

With the evolving digital age, communication evolved from handwritten letters to electronic mail, which facilitated seamless sharing of personal information. The rise of chat platforms such as WhatsApp and Telegram further accelerated this transformation making it effortless for individuals to exchange thoughts, opinions and documents to one another. With the convenience of google forms, people have been collecting personal information by sharing links without being accountable for the manner and purpose for which the data can be stored or used. The convenience extended to the processing of personal data, with automated systems enabling faster transactions by linking personal information seamlessly.

However, this era of digital ease has also brought forth unprecedented challenges. Data breaches, unauthorized access, and misuse of personal information have become rampant, exposing glaring vulnerabilities in the legal frameworks governing data protection.

The broken and archaic nature of existing regulations posed a dual challenge:

1. **Data owners**: The struggle to protect their privacy amidst escalating threats.
2. **Data receivers**: Navigating the complexities of compliance under outdated and inconsistent laws.

Although certain legislation provides for provisions for protection of personal data a unified, robust framework to address use, misuse, fraud, and breaches of trust of personal data in digital form has become imperative. Some of the legislations which provided for provisions for the protection of personal data are as follows:

Legislations	Personal Data protected under the legislation
The Aadhaar (Targeted Delivery of Financial and Other Subsidies, Benefits and Services) Act, 2016	• Aadhar number • Photograph • Finger print • Iris scan • Other biological attributes of an individual • Name • Nate of birth • Address • Other relevant information of an individual
Information Technology Act, 2000 & SPDI Rules	• Electronic signature • Electronic signature certificate • Digital signature • Fingerprints • Eye retinas and irises • Voice patterns • Facial patterns • Hand measurements

Legislations	Personal Data protected under the legislation
	• 'DNA' for authentication • Password • Financial information such as Bank account or credit card or debit card or other payment instrument details • Physical, physiological and mental health condition • Sexual orientation • Medical records and history • Biometric information
Legislations in relation to Medical Sector	Medical records not only cover a hospital case sheet but can also include: • Outpatient department slips • Prescription notes • Inpatient department records • Laboratory test results • Radiological films • Histopathological slides and tissue blocks • Operative reports • Wound certificates • Autopsy findings • Sickness and fitness certificates • Clinical trial documentation • Clinical research data **Note:** above are instances of few documents that may be considered as medical records

ORIGINS OF THE DIGITAL PERSONAL DATA PROTECTION ACT

The Digital Personal Data Protection Act, 2023 (the "***DPDP Act***") is a result of legislative and judicial efforts that arise from the recognition of privacy as a fundamental right. In the landmark judgment of Justice K.S. Puttaswamy (Retd.) v. Union of India (2017), the Hon'ble Supreme Court unequivocally declared the Right to Privacy as an intrinsic facet of the Right to Life and Personal Liberty under Article 21 of the Indian Constitution.

Subsequent to the aforesaid judgement, the Government of India initiated efforts to establish a digital data protection regime. The DPDP Act represents a significant milestone, aligning India's legal framework with global standards such as the EU General Data Protection Regulation (GDPR) while addressing certain unique domestic challenges.

The enactment of the DPDP Act has redefined the persons receiving data as Data Fiduciaries, placing upon them the onus of determining the purpose and means of processing personal data. This legislation heralds a paradigm shift in how data is handled, protected and processed in the world's most populous democracy.

OVERVIEW OF THE DPDP ACT

The DPDP Act outlines key aspects in relation to the processing of the **digital** personal data (DPD), including how, which, where, what, and the manner in which DPD is to be processed with the intent to (a) protect the **rights of the**

individuals disclosing the personal data in the digital format, and (b) the **need to process** the DPD for a **lawful purposes** and for matters connected or incidental thereto.

The DPDP Act not only protects the data provided by the person in the digital format, but also protects the data that the data receiver later digitises as part of the lawful purposes.

Before we do a deep dive into the subject matter, as part of this article, let us familiarise with few key terms, which we will elaborate in the next Article.

*"**data**" means a representation of **information**, **facts**, **concepts**, **opinions** or **instructions** in a manner suitable for **communication**, **interpretation** or **processing** by human beings or by automated means;*

*"**Digital personal data**" means **personal data** in **digital form**;*

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

*"**processing**" in relation to **personal data**, means a wholly or partly automated operation or set of operations performed on **digital personal data**, and includes operations such as **collection**, **recording**, **organisation**, **structuring**, **storage**, **adaptation**, **retrieval**, **use**, **alignment** or **combination**, **indexing**, **sharing**, **disclosure** by transmission, **dissemination** or otherwise **making available**, **restriction**, **erasure** or **destruction.***

On a plain reading of the aforesaid terms, the DPDP Act looks straight forward, but to understand the applicability of the DPDP Act and the persons who must comply with the provisions of this DPDP Act, one will need to undertake a careful analysis of the aforesaid terms for each cases involving data of individuals which may be considered as personal data.

Some of the scenarios that may attract the provisions of DPDP Act are:

1. opinion provided by the former employer as part of employee background checks undertaken by the new employer;
2. digitalised medical prescription uploaded online to online pharmacies and digitalisation of medicines purchased by patients at local pharmacies;
3. feedback received from customers in relation to employees of a legal entity;
4. customer profiling by marketing companies.

CONTRIBUTED BY:

Ankur Singhania, Partner: ankur@rajaniassociates.net

Rishi Rajani: rishi@rajaniassociates.net

AREAS OF PRACTICE

| Capital Markets | Private Equity | Mergers and Acquisitions | Corporate Litigation & Arbitration | Projects & Project Finance | Real Estate & Trust | Corporate & Commercial | Banking & Finance | Structuring | TMT | IPR | Employment

DISCLAIMER

Contact US

Rajani Associates
simple solutions

Address:	Krishna Chambers 59 New Marine Lines Churchgate Mumbai 400020 Maharashtra, India
Telephone:	(+91-22) 40961000
Facsimile:	(+91-22) 40961010
Email:	dejure@rajaniassociates.net
Website:	www.rajaniassociates.net