Cyberjure Legal Consulting
Simplifying Cyber Laws

DIGITAL PERSONAL DATA PROTECTION ACT 2023

-Understanding the Law in a Nutshell

Advocate Puneet Bhasin
Cyber Law & Data Protection Expert

CONTACT US
Cyberjure Legal Consulting
www.cyberjure.com | www.puneetbhasin.in adv.puneet@cyberjure.com | contact@cyberjure.com

I. INTRODUCTION

The Digital Personal Data Protection Bill, 2023, has been introduced in the Indian Parliament after 5 years of deliberation involving the government, tech companies, and civil society. The Act outlines procedures for collecting and using personal data of Indian citizens by corporations and the government. This is the fifth and final version of India's attempts to establish a personal data protection law. Notable changes from the previous version include a negative-list approach for cross-border data transfers, removal of certain processing grounds, exemptions for publicly available data, and government authority to block access to a data fiduciary's platform. The bill's provisions are high-level, with implementation details to be specified in rules. On August 11, 2023, the Bill got the assent from President of India making it into law to regulate digital personal data processing, addressing the absence of a standalone data protection law in India, which currently relies on the Information Technology Act of 2000. The Act reflects India's ongoing efforts to create a comprehensive data privacy law governing the collection, processing, and storage of personal data.

II. HISTORY

Prior to the present Act's enactment, India lacked an independent law dedicated to data protection. The utilization of personal data was governed by the Information Technology (IT) Act of 2000. In 2017, the national government established a Committee of Experts on Data Protection, led by Justice B. N. Srikrishna, to investigate matters concerning data protection within the nation. The Committee concluded its findings in July 2018. Building upon these recommendations, the Personal Data Protection Bill of 2019 was presented in the Lok Sabha (House of the People) in December 2019. This Bill underwent examination by a Joint Parliamentary Committee, which issued its report in December 2021. Subsequently, in August 2022, the Bill was withdrawn from the Parliament. In November 2022, a preliminary Draft Bill was made accessible for public input. Finally, in August 2023, the Digital Personal Data Protection Bill of 2023 was introduced in the Parliament.

III. CONCEPT OF DATA

In Digital Personal Data Protection Act, the term "data" essentially refers to a way of representing information, facts, ideas, opinions, or even directions. This representation is designed in a manner that's convenient for sharing, understanding, and using by either people or automated systems. Think of it as a kind of language that both humans and machines can understand, helping us exchange thoughts and insights effectively. Personal data pertains to information connected with a recognized or identifiable person. Both businesses and governmental bodies handle personal data to provide products and services. The act of dealing with this personal data helps in comprehending individuals' preferences, which can be advantageous for tailoring experiences, pinpointed advertisements, and creating suggestions. Furthermore, processing personal data might also assist law enforcement efforts. In essence, personal data serves as a tool that organizations and authorities can use to better understand individuals, offer personalized experiences, and potentially aid in maintaining law and order. According to the Act, the personal data is gathered through two distinct methods:

(i) collected from the data principal via online channels; and
(ii) initially collected offline and then converted into digital format.

IV. MEANING OF DATA PRINCIPAL, DATA FIDUCIARY AND DATA PROCESSOR

(i) "**Data Fiduciary**" is described as any person who alone or in conjunction with other persons determines the purpose and means of processing of personal data. In simpler words the meaning of "Data Fiduciary" encompasses any person, organization, or entity that holds the responsibility, either individually or in cooperation with others, of defining both the objective and the mechanisms by which personal data is managed and processed.

(ii) "**Data Principal**" denotes an individual to whom specific personal data pertains.This involves a direct connection between the data and the person it concerns. In situations where this individual is categorized as a child, the definition broadens to encompass not only the child but also extends to include their parents or the legal guardian who is entrusted with their care and well-being. Similarly, if the Data Principal is an individual with a disability, the scope of the term incorporates not only the person with the disability but also encompasses their lawful guardian, who acts as a representative and advocate on their behalf.

(iii) "**Data Processor**" pertains to an individual or entity that engages in the processing of personal data, undertaking this responsibility in a representative capacity on behalf of a designated Data Fiduciary. The role of a Data Processor involves handling personal data in accordance with the directions, objectives, and methods established by the Data Fiduciary.

V. APPLICABILITY OF THE ACT

Scope of Applicability: The Act's coverage pertains to personal data acquired either in digital format or originally non-digital but subsequently transformed into digital form.

Geographical Scope: It applies to processing digital personal data within the territory of India. It also applies to processing of digital personal data outside India if such processing is in connection with any profiling or offering goods or services to data principals within India.

VI. EXCEPTIONS TO APPLICABILITY OF THE ACT

The Act does not encompass:

(i) non-digital data;
(ii) data managed for personal or household purposes; and
(iii) data made openly accessible by a data principal or any other entity due to legal obligations.

VII. CROSS BORDER DATA TRANSFER

The Act allows a data fiduciary to transfer personal data to any other country or region for processing, unless the Central Government limits such transfers to specific countries designated through notifications. In essence, the Act employs a "blacklisting" approach, which implies that the movement of personal data is generally unimpeded except when it's intended for a territory or country that has been "blacklisted" by the Central Government. However, if any Indian law, particularly laws specific to certain sectors, offers a greater level of safeguarding or imposes more stringent constraints on the transfer of personal data beyond India's borders, those laws will remain in effect and will take precedence over the Act.

VIII. CONCEPT OF NOTICE AND CONSENT

1. **NOTICE:** A data fiduciary is required to give an itemized notice to the data principal, either at the time of making or preceding a request for consent, (i) describing the personal data sought to be collected and the purpose for its processing; (ii) the manner in which the data principal may exercise his/her/their rights (including the right to correction, withdrawal of consent, etc.); and (iii) the manner in which the data principal may make a complaint to the Board. If the data principals have already provided his/her/their consent for processing their personal data prior to the commencement of the Act, the data fiduciary must provide him/her/ them with such notice ‘as soon as it is reasonably practicable’. The notice must be presented in clear and plain language, by way of a separate document or in an electronic form, or in a form ’as may be prescribed’. Further, the data fiduciary must give the data principal the option to access the contents of the notice in English or any of the 22 (twenty-two) languages specified in the Eighth Schedule to the Constitution of India.

2. **CONSENT:** Consent means an indication by the data principal signifying an agreement for their data to be processed for a specified purpose. Consent should be free, specific, informed, unconditional and unambiguous. And it should be through clear affirmative action. Data principals also have the right to withdraw their consent and utilize the services of consent managers. If a data principal withdraws their consent, the data fiduciary must get the data processor to stop processing that individual's personal data, unless it is otherwise authorized.

IX. LEGITIMATE USE OF DATA

The Act outlines certain instances of 'legitimate uses' through which a data fiduciary can handle the personal data of data principals without necessitating explicit consent from the data principal. One such legitimate use arises when a data principal willingly provides their personal data to the data fiduciary while utilizing or seeking a specific service for a particular purpose, and has not expressed a lack of consent to the utilization of their personal data.
Additionally, this legitimate use extends to the processing of personal data for the purpose of adhering to any judgement, court order, or decree issued under Indian law, as well as any judgment, decree, or order concerning claims of contractual or civil nature in accordance with laws outside India.

X. RIGHTS AND DUTIES OF DATA PRINCIPAL

An individual whose data is being processed ("**Data Principal**"), will have the right to:

(i) obtain information about processing,
(ii) seek correction and erasure of personal data,
(iii) nominate another person to exercise rights in the event of death or incapacity, and
(iv) grievance redressal.

The Act imposes certain duties on data principals, including the duty not to

(i) impersonate another person;
(ii) suppress any material information while applying for any document, unique identifier, proof of identity or address issued by the State or any of its instrumentalities; and

(iii) register a false or frivolous grievance or complaint with a data fiduciary or the Board.

XI. LEGAL OBLIGATIONS OF DATA FIDUCIARY

Data fiduciaries are responsible for compliance with the Act, including for processing of personal data undertaken by a data processor on their behalf. Where the data fiduciaries are processing personal data that is likely to be used to make a decision that affects the data principal or is to be shared with another data fiduciary, they are required ensure accuracy and completeness of such personal data. Data fiduciaries are also required to delete personal data, if the data principal withdraws her consent or if it is reasonable to assume that the specified purpose is no longer being served, unless such retention is necessary for compliance with law.

XII. CONCEPT OF SIGNIFICANT DATA FIDUCIARY

Central Government has the authority to identify specific Data Fiduciaries or groups of Data Fiduciaries as "Significant Data Fiduciaries" This determination is based on an evaluation of important factors that the government decides, including:

a) the volume and sensitivity of personal data processed;
b) risk to the rights of Data Principal;
c) potential impact on the sovereignty and integrity of India;
d) risk to electoral democracy;
e) security of the State; and
f) public order.

The Act imposes certain additional obligations on such significant data fiduciaries viz., the need to

(i) appoint a data protection officer based in India;
(ii) appoint an independent data auditor to evaluate the compliance by the significant data fiduciary with the provisions of the Act;
(iii) undertake a data protection impact assessment; and
(iv) undertake periodic compliance audits.

XIII. DATA PROTECTION OFFICER (DPO)

Significant Data Fiduciary is responsible to appoint a Data Protection Officer who will serve several key roles. This officer will act as the representative of the Significant Data Fiduciary as per the provisions of the Act, functioning within the geographical bounds of India. The Data Protection Officer must be an individual accountable to the Board of Directors or a similar governing body of the Significant Data Fiduciary. Additionally, this officer will serve as the designated point of contact for the grievance redressal mechanism specified within the Act.

XIV. CONSENT MANAGER

A data principal may give, manage, review or withdraw their consent to the data fiduciary through a Consent Manager. Consent manager has been defined as a person registered with the Board, and acts as a single point of contact to enable a data principal to give, manage, review and withdraw their consent through an accessible, transparent and interoperable platform.

XV. DATA AUDITS AND DATA IMPACT ASSESSMENTS

The Significant Data Fiduciary is obligated to fulfill certain requirements, which encompass appointing an independent data auditor responsible for conducting data audits. This auditor's role involves assessing the Significant Data Fiduciary's compliance with the stipulations outlined in the Act. Additionally, the auditor must carry out various actions, including periodic Data Protection Impact Assessment which means a process comprising description, purpose, assessment of harm, measures for managing risk of harm and such other matters with respect to processing of personal data, as may be prescribed. This assessment involves detailing the rights of Data Principals and the intended purpose of processing their personal data, evaluating and managing the risks to these Data Principals' rights, and addressing other pertinent aspects of this process as per the prescribed guidelines. The Data Auditor must also undertake regular audits and implement any other measures that align with the provisions of the Act.

XVI. PENALTIES

The Data Protection Bill contains severe financial penalties for those that do not comply with it. Specifies penalties for various offences such as up to:

(i) Rs. 200 crores for non-fulfilment of obligations for children,
(ii) Rs. 250 crores for failure to take security measures to prevent data breaches, and same penalty in breach in observing the obligation to give the Board or affected Data Principal notice of a personal data breach
(iii) Rs. 10,000 if a data principal fails to perform their duties as specified therein