



Summary of The Digital Personal Data Protection Bill, 2023

The Digital Personal Data Protection Bill, 2023 being introduced in the Lok Sabha on 3rd August, 2023 is a welcome move, and a concrete step forward in India's journey towards establishing a comprehensive data protection regime.

KEY TERMS

Data Fiduciary

The DPDP Bill introduces the term 'data fiduciary' to refer to any entity or individual that determines the purpose and means of processing personal data. This includes organizations that collect personal data for various purposes, such as providing services, conducting research, or marketing products.

Data Principal

As per the DPDP Bill a 'data principal' is the natural person to whom the personal data pertains. Essentially, the data principal is the individual whose data is being collected, stored and processed. This individual has certain rights under the DPDP Bill including the right to access and correct his/her data, the right to data portability and the right to be forgotten.

Consent

The consent given by the Data Principal shall be free, specific, informed, unconditional and unambiguous with a clear affirmative action, and shall signify an agreement to the processing of her personal data for the specified purpose and be limited to such personal data as is necessary for such specified purpose.

Consent Manager

Consent Manager means a person registered with the Board, who acts as a single point of contact to enable a Data Principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform.

Significant Data Fiduciary

A 'Significant Data Fiduciary' (SDF) is a special category of data fiduciary that is subject to additional obligations under the DPDP Bill. An entity is classified as an SDF based on factors such as the volume and sensitivity of personal data, its processes, its turnover, its use of new technologies for processing and the risk of harm to data principals from its processing. SDFs are required to implement additional

measures, such as conducting data protection impact assessments and appointing a data protection officer.

The DPDP Bill is not the first instance that SDFs have been referred to in an Indian draft law on data protection. Provisions in past iterations of DPDP – such as Clauses 38 and 26 of the Personal Data Protection Bills of 2018 and 2019 respectively – had contained references to SDFs as well.

Children's data

The Bill retains the definition of a 'child' – an individual below the age of 18 years – from the 2022 Bill. Data fiduciaries must continue to obtain 'verifiable' parental consent to process children's data. It also prohibits tracking and advertising targeted towards children and processing that is likely to cause any 'detrimental effect' – characterized as 'harm' in the 2022 Bill – on the well-being of a child. The Government can exempt classes of data fiduciaries and processing for certain purposes from the requirement of obtaining parental consent and prohibiting behavioural monitoring.

Previous Indian iterations had provided for a separate class of data fiduciaries which are involved in operations and services similar to what Children's Online Privacy Protection Act (COPPA) envisages, including in respect of processing large volumes of children's data. Accordingly, entities falling in this category, called 'guardian' data fiduciaries ("**GDFs**"), were proposed to be regulated via separate rules. While DPDP has done away with such GDF categorization, it has imposed additional obligations under Section 10 on all data fiduciaries that process children's data.

Cross-border data transfers

The Bill moves from the white-list approach (recommended in the 2022 Bill) to a negative list. This means that data transfers are allowed to all jurisdictions except those barred by the government through notification. The principles/conditions under which such countries will be barred are not specified. Any stricter sectoral restrictions on data transfers – like the Reserve Bank of India's payments data localization mandate – will continue to apply.

Principles underlying the Bill

1. Principle of Lawful, Fair & Transparent Usage of Personal Data
2. Principle of Purpose Limitation
3. Principle of Data Minimization
4. Principle of Data Accuracy
5. Principle of Storage Limitation
6. Principle of Accountability

7. Principle of Reasonable Security Safeguards

General obligations of data fiduciary

The Digital Personal Data Protection (DPDP) Bill, imposes several obligations on data fiduciaries to ensure the protection of personal data and the privacy rights of individuals. These obligations apply to all data fiduciaries, with additional requirements for those classified as "Significant Data Fiduciaries".

Obtaining Valid Consent

One of the primary obligations of data fiduciaries under the DPDP Bill, is to obtain valid consent from data principals before collecting and processing their personal data. Consent must be free, informed, specific, clear and capable of being withdrawn.

Ensuring Data Security

Data fiduciaries are required to implement appropriate security safeguards to protect personal data from unauthorized access, disclosure, alteration, or destruction. These safeguards should be proportionate to the potential harm that could result from a data breach and should consider the nature and purpose of data processing, the risks associated with the processing and the current state of technology.

Strict Compliance norms

Noteworthy business-oriented provisions, of the DPDP Bill is that it exempts startups and does not contain criminal penalties for non-compliance. However, the Bill does make a mention of financial penalties in case of data breaches. The Bill also allows for international data transfers, highlighting a commitment to fostering a conducive environment for enterprises.

Easy for them to understand

Overall the Bill is simple and is easy to comprehend.

BUSINESS IMPLICATIONS

Upon its passing, the law will significantly alter how business collect and use digital personal data. In practical terms, this means organizations must take steps to ensure transparency and compliance with data protection standards at every level of operation. This could involve redesigning user

interfaces to include essential details, popup notices, and checkboxes that inform and seek consent from users about their data collection and use.


It also requires updating privacy policies and notifications to ensure that they are in line with the latest regulations, are comprehensive, and is understood by users. Companies need to be proactive in reviewing vendor contracts and assessing their data handling practices before initiating any engagement. It would be advisable to include specific clauses related to data protection in vendor agreements to ensure external compliance.


Moreover, the Bill highlights the need to train employees across various departments including product development, business operations, sales, marketing and others. This training should aim to educate and sensitize them about the implications of data use, the importance of safeguarding user data, and the need to adhere to data protection guidelines.


Amidst the following developments, it is crucial organisations find partners that can mobilize quickly by leveraging their knowledge and experience based on similar data privacy engagements and seek customizable gap assessment tools that will help in quick validation of the prior gap assessment conducted and ensure that no key areas are left out




Contact Us

 +91-1244045954, +91-9312580816

 BSMT, Building no. 2731 EP, Sector 57, Golf Course Ext. Road,
Gurugram, Haryana, India – 122003

 sunil@atheniantech.com

 www.atheniantech.com