



ECONOMIC  
LAWS  
PRACTICE  
ADVOCATES & SOLICITORS



# Overview of the Digital Personal Data Protection (DPDP) Bill, 2023

## OVERVIEW OF THE DIGITAL PERSONAL DATA PROTECTION (DPDP) BILL, 2023

On August 3, 2023, the Government of India, introduced the fifth iteration of India's proposed personal data protection legislation, i.e., the Digital Personal Data Protection Bill, 2023 (**DPDP Bill**) in Parliament. Previously, in December 2022, the Ministry of Electronics and Information Technology had released a draft version of the bill (**2022 Draft**), inviting public comments thereto.

Once in force, the DPDP Bill aims to amend and omit some of the key provisions of the Information Technology Act, 2000 (**IT Act**) and provisions of the Right to Information Act 2005.

Summarized below, in a Q&A format, is our note addressing some of the key issues that the 2023 version of the DPDP Bill addresses, as well as some key differences in comparison to the 2022 Draft.



### What is the legislative scope of the DPDP Bill?

**Applies:** The DPDP Bill applies to personal data<sup>1</sup> that is: collected within India (i) through an online mode; and (ii) offline mode but is then digitized; and collected outside India, if this processing is in connection with any activity relating to offering goods or services to data principals<sup>2</sup> within India.

**Does not apply:** The DPDP Bill, presently, does not apply to (i) personal data processed by an individual for personal or domestic purpose; (ii) personal data made available publicly by the data principal himself, to whom such data relates; and if it is made publicly available under an obligation under any law. **Notably, the list of data to which the DPDP Bill does not apply has been narrowed in the latest iteration of the Bill compared to the 2022 Draft.**

**Exemptions:** Additionally, the DPDP Bill exempts the application of certain provisions relating to the duties of data fiduciaries and the rights of data principals in certain scenarios. These include the investigation of offences, assessing the financial status of defaulters, processing of data of principals outside the territory of India pursuant to any contract by any person based in India.



### Are data principals required to be provided with prior notice for collection of their personal data?

Yes, the DPDP Bill requires that data principals be provided with a notice in clear and plain language which describes the personal data that is sought to be collected, purpose of such collection, details of the way data principals may exercise their rights to withdraw consent and grievance redressal; and details on how data principals may file a complaint with the Data Protection Board (**DPB**).

The notice by the data fiduciaries<sup>3</sup>, as per the DPDP Bill, is required to be either in English or any local Indian language specified under the Eighth Schedule to the Constitution of India (as understood by the data principal).

The DPDP Bill also sets out a list of "legitimate uses" for which data may be processed without consent. As opposed to the 2022 Draft, the DPDP Bill does not use the terminology of "deemed consent". Legitimate uses include (i) when a user voluntarily shares her data and does not deny consent for the use of the same; (ii) for the State to perform its function under any law; (iii) court orders; (iv) medical emergency; (v) epidemics; (vi) disasters; (vii) employment.

**Notably, the DPDP no longer includes the grounds of "public interest" and "fair and reasonable" purpose that were contained in the 2022 Draft.**



### Will the requirement to obtain consent from data principals be applicable retrospectively to cases where the personal data was already collected from data principals?

Yes, the DPDP Bill states that the requirement to obtain consent in accordance with the DPDP Bill will be applicable retrospectively where, if data principals have provided their consent to the collection of their personal data prior to commencement [of the DPDP Act], then all data fiduciaries would be required to furnish a notice to such data principals setting out the description of personal data [already] collected from them and the purpose for which such personal data was processed. However, it is pertinent to note that presently, the DPDP Bill does not prescribe a

<sup>1</sup> The DPDP Bill defines 'personal data' as any data about an individual who is identifiable by or in relation to such data

<sup>2</sup> The DPDP Bill defines 'data principals' as the individual to whom the personal data relates and where such individual is a child includes the parents or lawful guardian of such a child

<sup>3</sup> The DPDP Bill defines 'data fiduciaries' as entities determining the purpose and means of processing of personal data

timeline within which the data fiduciary is required to comply with the said requirement, but all it requires is that the same be obtained “as soon as reasonably practicable”.



### What are the obligations of data fiduciary(ies) under the DPDP Bill?

The DPDP Bill, much like the 2022 Draft, sets out a specific provision listing all obligations of a data fiduciary and holds the data fiduciary ultimately responsible for processing personal data. The DPDP Bill further requires the data fiduciary(ies) to ensure that all reasonable safeguards are taken to prevent personal data breaches, including for any processing undertaken on its behalf by data processors<sup>4</sup>.

The DPDP Bill also sets out the concept of a ‘significant data fiduciary(es)’ based on the significant volume and sensitivity of personal data that will be collected by such data fiduciary including risk of harm to data principals. The DPDP Bill requires that such significant data fiduciary is required to comply with additional obligations such as appointment of a data protection officer residing in India, appointment of an independent data auditor, undertake data protection impact assessments and ensure compliance with other measures as may be prescribed.



### What are the obligations of data fiduciary(ies) when collecting personal data from children?

The DPDP Bill states that in case personal data from individuals, who are less than 18 years of age, is proposed to be processed, then a prior verifiable parental consent (including consent of a guardian) shall be required to be obtained. The DPDP Bill also states that data fiduciaries are not permitted to undertake the processing of data which is likely to have a “detrimental impact” on the well-being of the child. **This terminology is in contrast to the 2022 Bill which utilizes the concept of “harm”.** Data fiduciaries are also prohibited from engaging in tracking and behavioural monitoring of children or sending targeted advertisements directed at children. **The DPDP Bill further expands on the 2022 Draft by introducing exemptions relating to the processing of the personal data of children.** Upon satisfaction that the data processing by the data fiduciary is in a verifiably safe manner, the Central Government may exempt such data fiduciary from such obligations when processing data of children above a certain age (as may be notified).



### What are the obligations of data processors under the DPDP Bill?

The DPDP Bill provides that data processors have a duty to protect personal data in their possession or control by taking reasonable security safeguards to prevent breaches. The DPDP Bill also mandates that data processors cease processing personal data on withdrawal of consent. Additionally, once the retention of the personal data is no longer necessary for compliance with any law, the data processor must erase any such personal data. **Notably however, primary responsibility for reporting breaches as well as liability for failure to report is placed only on data fiduciaries as opposed to the 2022 Draft.**



### Who has the authority to determine non-compliances and impose penalties under the legislation?

The DPDP Bill proposes to establish the DPB<sup>5</sup>, which will be an independent body corporate, operating digitally (to the extent possible)<sup>6</sup> and be responsible for determining non-compliances under the legislation and imposing penalties. The DPDP Bill gives powers to the DPB to take actions (as prescribed under the DPDP Bill) on receipt of complaints. **Compared to the 2022 Draft, the 2023 Bill provides further details concerning the composition of the DPB and membership criteria.**

The DPDP Bill also provides for an appellate mechanism in the form of an Appellate Tribunal<sup>7</sup> i.e. the Telecom Disputes Settlement and Appellate Tribunal, which has the authority to review, repeal or reinforce the orders or directions of the DPB. Aggrieved individuals may approach the Appellate Tribunal within 6 months<sup>8</sup> of receiving the DPB's orders or

<sup>4</sup> The DPDP Bill defines ‘data processors’ as any person who processes personal data on behalf of a data fiduciary

<sup>5</sup> Clause 18, Digital Personal Data Protection Bill, 2023.

<sup>6</sup> Clause 28, Digital Personal Data Protection Bill, 2023.

<sup>7</sup> Clause 29, Sub-Clause 1, Digital Personal Data Protection Bill, 2023.

<sup>8</sup> Clause 29, Sub-Clause 2, Digital Personal Data Protection Bill, 2023.

directions. The Tribunal, in turn, shall endeavour to dispose the appeals within 6 months<sup>9</sup>. The DPDP Bill clarifies that every order made by the Tribunal will be enforceable akin to a decree made by the civil court<sup>10</sup>.



### Can personal data of data principal be transferred outside India?

The DPDP Bill permits cross-border transfer of all personal data, however, the Central Government may notify countries and territories outside India wherein such transfer of personal data is restricted<sup>11</sup>. The Bill also stipulates certain situations wherein the cross-border transfer of data may be mandated<sup>12</sup>. **This is in contrast to the 2022 Draft which permitted transfers only to notified countries and territories.**



### In which case, does the DPDP Bill set out any provision(s) regarding data localization?

The DPDP Bill continues to not contain any provisions relating to data localization. However, the provisions on cross-border transfer contained in the DPDP Bill would be subject to other laws governing data transfer in the country.<sup>13</sup> Hence more stringent sectoral regulations, such as RBI regulations, will remain applicable, whereby, sectoral data localization is not entirely off the table.



### How different is the DPDP Bill from its 2022 version in respect of the provisions relating to cross border data transfer?

Tabulated below is the comparison between the DPDP Bill and the 2022 version of the data protection bill in relation to cross-border data transfer clauses:

S. No.	Particulars	DPDP Bill (2022) <sup>14</sup>	DPDP Bill (2023) <sup>15</sup>
1.	Nature of Personal Data allowed to be transferred across borders	All personal data	All personal data
2.	Countries to which cross-border transfer of personal data is permitted	Countries or jurisdictions notified by the central government	All countries and territories, unless notified otherwise by the Central Government
3.	Factors to be considered while notifying eligible countries or entities	Any factors that the Central Government may consider necessary	Unspecified .

**The shift from a "whitelist" to a "blacklist" approach in the 2023 Draft Data Protection Bill reflects a significant change in India's policy on cross-border data transfers.** However, the exact implementation and criteria for determining such restricted countries remain to be seen.

<sup>9</sup> Clause 29, Sub-Clause 6, Digital Personal Data Protection Bill, 2023.

<sup>10</sup> Clause 28, Sub-Clause 7, Digital Personal Data Protection Bill, 2023.

<sup>11</sup> Clause 16, Digital Personal Data Protection Bill, 2023.

<sup>12</sup> Clause 17, Digital Personal Data Protection Bill, 2023.

<sup>13</sup> Clause 16, Sub-Clause 2, Digital Personal Data Protection Bill, 2023.

<sup>14</sup> Clause 17, Draft Digital Data Protection Bill, 2023

<sup>15</sup> Clause 16, Draft Digital Data Protection Bill, 2023



## What are the penalties that are prescribed for non-compliance under the DPDP Bill?

The penalties under the DPDP Bill range from up to INR 10,000 to up to INR 250 crores for different offences, **with the maximum penalty being lower than the 2022 Draft**. The DPDP Bill also sets out the factors that need to be considered while determining the penalty. **Unlike the 2022 Draft it appears that only data fiduciaries will be subject to penalties.**

**Notably, clause 37 of the DPDP Bill also empowers the Central Government to advise, in the interests of the general public, blocking access for the public to any information generated, transmitted, received, stored or hosted, in any computer resource that enables such Data Fiduciary to carry on any activity relating to offering of goods or services to data principals within the territory of India.**

### Conclusion

The DPDP Bill has undergone some key changes from its 2022 version. Amongst other changes, it provides comprehensive details on the powers and functions of the proposed Data Protection Board of India, provides the Central Government with blocking powers and introduces an appellate mechanism before the Telecom Disputes Settlement and Appellate Tribunal. Notably, the Bill also demonstrates India's business-friendly approach by adopting an open policy towards cross-border data transfers, unlike its previous iteration. Another significant aspect of the DPDP Bill is that it vests the Government with powers to create delegated legislation concerning various aspects of the Bill. This will bring further clarity on issues like the processes for reporting data breaches and other related matters.

During the tabling of the Bill, Members of Parliament raised several concerns, including compensation for victims of breaches, protection of the fundamental right to privacy, and the absence of restrictions on government data processing. The Government now faces the task of addressing these questions.

After discussion and passing in the Lok Sabha is completed, the Bill will then proceed to the Rajya Sabha for further consideration. Once enacted, the Digital Personal Data Protection Act is expected to be implemented in a staged manner

*We trust you will find this an interesting read. For any queries or comments on this update, please feel free to contact us at [insights@elp-in.com](mailto:insights@elp-in.com) or write to our authors:*

**Sanjay Notani, Partner** – [SanjayNotani@elp-in.com](mailto:SanjayNotani@elp-in.com) ;

**Vinay Butani, Partner**- [VinayButani@elp-in.com](mailto:VinayButani@elp-in.com) ;

**Naghm Ghei, Principal Associate** - [NaghmGhei@elp-in.com](mailto:NaghmGhei@elp-in.com);

**Akash Manwani, Associate**- [AkashManwani@elp-in.com](mailto:AkashManwani@elp-in.com)

*Disclaimer: The information contained in this document is intended for informational purposes only and does not constitute legal opinion or advice*