The Digital Personal Data Protection Bill, 2023 - Towards a progressive data protection regime

9 August 2023

Partners: *Rahul Matthan, Nikhil Narendran and Jyotsna Jayaram,* ***Counsels:*** *Thomas J. Vallianeth and Karishma Sundara*

On 9 August 2023, the Digital Personal Data Protection Bill, 2023 (**Bill**) was passed by the Upper House of Parliament. The Bill had been passed by the Lower House of Parliament on 7 August 2023, and all that remains for it to become law is the receipt of Presidential assent.

Once enacted, it will replace the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**Privacy Rules**) and become the definitive privacy law in the country. Unlike the Privacy Rules, which focused on protecting sensitive personal data or information (**SPDI**), the new law will establish a comprehensive framework to govern the processing of personal data.

The Bill has not specified a transitional period, although the central government has been granted the discretion to notify the commencement of different provisions of the Bill at different times.

The Digital Personal Data Protection Bill, 2023 has been passed by both Houses of Parliament and is set to create a comprehensive data protection regime in India, once brought into force. This update highlights the important provisions of the regime and offers some key takeaways for businesses processing personal data.

Once the law comes into force, businesses that process personal data will have to revisit their data processing practices and policies. Non-compliance will be subject to substantial penalties, with the amount of penalty for conjoint contraventions remaining uncapped.

The key changes that need to be kept in mind once the law comes into force are discussed below.

1 Applicability

The Bill will only apply to personal data that is digital. Personal data is defined as any data about an individual (called a **Data Principal**) who is identifiable either by such data or in relation to such data. The Bill does not distinguish between the various kinds of personal data based on sensitivity. In addition, personal data that has been made *'publicly available'* by the Data Principal to whom it relates or someone else who is under a legal obligation to do so, is not covered under the Bill.

The Bill primarily applies to entities that determine the purpose and means by which personal data is processed (**Data Fiduciaries**). Processing has been defined widely to include all automated (including partly automated) data processing operations such as collection, organisation, indexing, sharing, use, and alignment

or combination. Processing can be carried out by the Data Fiduciary itself or under a contract through a Data Processor. The Bill is agnostic to where the processing occurs and applies to the processing of digital personal data that occurs (a) within India, irrespective of whether the Data Principal is based in India or not; or (b) outside India in relation to offering goods or services to Data Principals in India.

The Bill does not, however, apply to the processing of personal data for any personal or domestic purpose. The Bill also exempts the processing of personal data by the government for certain prescribed purposes and the processing of personal data for research, archival, or statistics.

Data Fiduciaries must review their data processing activities to ensure that the manner in which they deal with digital personal data is aligned with what has been covered under the Bill.

2 Legal bases for processing

Barring limited exceptions, Data Fiduciaries are obliged to process personal data for a lawful purpose, based on consent or legitimate use.

2.1 Notice must precede consent

When personal data is processed on the basis of consent, the Data Fiduciary must provide a notice to the Data Principal as to (i) the personal data being processed; (ii) the purposes for which that data is being processed; and (iii) the manner in which the Data Principal may exercise its rights and make complaints to the Data Protection Board (**Board**). To ensure that consent is informed, this notice must be provided in English or, if the Data Principal so requires, in any of the other languages specified in the Eighth Schedule to the Constitution.

2.2 Consent – what does this involve under the Bill?

Consent must be free, informed and provided by a Data Principal through clear, affirmative action. Data Principals can always provide or review such consent, including through Consent Managers (entities that are registered with the Board for this purpose); and withdraw such consent but must bear the consequences (e.g., non-availability of a service linked to such processing). Once a Data Principal withdraws consent, the Data Fiduciary must cease processing of this personal data within a reasonable time, and subsequently delete this data.

To process with consent, Data Fiduciaries must provide notice, obtain consent, and enable the withdrawal of consent. Planning for such circumstances (e.g., putting in place standard operating procedures to identify data easily, segregate and treat it accordingly) is essential.

2.3 Legitimate use – how broad is this?

As an alternative to consent, personal data may also be processed for one of the identified legitimate uses, where (a) this data has been *voluntarily provided* by the Data Principal for a purpose; and (b) this purpose necessarily arises out of the nature of the interaction between the Data Principal and the Data Fiduciary. For example, the processing of data relating to a patient's symptoms provided by a patient to a doctor to enable diagnosis.

Other legitimate uses where personal data may be processed without consent include processing for employment purposes or to safeguard the employer, and other exceptional circumstances, such as health emergencies and public safety.

The extent to which businesses may be able to rely on these legitimate uses may still be limited, given that their scope tends towards the exceptional (e.g., emergencies).

2.4 How will these bases work for protected classes of Data Principals?

In relation to the processing of personal data of children under the age of 18, or persons with disabilities who have a legal guardian, Data Fiduciaries must obtain consent from parents or legal guardians using a method approved by the central government, unless (a) exempted by the central government; or (b) if parents or guardians voluntarily provide such personal data of their child or ward and such data is only processed for the limited purpose for which it was collected. Processing children's data is also subject to other prohibitions, i.e., businesses cannot track or monitor the behaviour of children; they also cannot target ads at children or process their personal data in a way that is likely to have a detrimental effect on them.

Data Fiduciaries will have to identify circumstances in which they may process such data, examine the purposes for which they may do this, and implement mechanisms to ensure they are not processing it in a way that breaches these prohibitions.

3 Key obligations

The Bill prescribes several obligations for Data Fiduciaries processing digital personal data. These include:

a. ***Data quality***: Where data is used to make a decision about Data Principals, or is disclosed to another Data Fiduciary, its completeness, accuracy and consistency must be ensured.

b. ***Technical and organisational measures and security safeguards***: Data Fiduciaries must implement technical and organisational measures to comply with this Bill as well as reasonable security safeguards to prevent personal data breaches, i.e., any unauthorised or accidental processing of data that compromises its confidentiality, integrity, or availability.

c. ***Breach reporting***: Personal data breaches must be reported to the Board and each affected Data Principal. This reporting obligation applies in addition to the existing requirement to report breaches to the Indian Computer Emergency Response Team (CERT-In). The Board may direct Data Fiduciaries to undertake urgent remedial measures in relation to a data breach.

d. ***Grievance redressal***: As with the Privacy Rules, Data Fiduciaries must establish a mechanism for grievance redressal and must publish the details of the person responsible for answering queries from Data Principals. The central government will specify the time period within which such grievances must be redressed. These decisions may be appealed to the Board.

e. ***Data retention***: Personal data must be deleted as soon as the purpose for which it was collected is no longer being served. The Bill permits the central government to specify time periods within which the specified purpose is deemed to have elapsed, contingent on the Data Principal *not approaching* the Data Fiduciary for the purpose for which the data was collected or to exercise its rights.

f. ***Restricted cross-border transfers***: The central government may introduce restrictions on the cross-border transfer of personal data to certain geographies, to which Data Fiduciaries must adhere.

g. ***Flow-down obligations to processors***: Data Fiduciaries may appoint Data Processors to process personal data for them. This requires a valid contract which must pass down the relevant obligations to the Data

Processor (including (b) and (f) above). However, passing down such obligations will not absolve the Data Fiduciary of its own obligations under the Bill, or penalties applicable for non-compliance.

Data Fiduciaries must examine their technological and organisational processes to ensure that they can meet the above-mentioned requirements. Contracts with data processors must be re-examined.

4 Significant Data Fiduciaries

The Bill creates a class of Data Fiduciaries called Significant Data Fiduciaries (SDF) that are subject to certain additional compliances. These include the requirement to carry out periodic audits and data protection impact assessments, and to appoint a Data Protection Officer (who must be based in India and responsible to the board of the Data Fiduciary). The central government will notify entities that fall within this classification based on factors including the volume and sensitivity of data involved, risks to the rights of Data Principals or electoral democracy, and public order.

Data Fiduciaries that undertake critical/sensitive/voluminous data processing must watch for this classification and be prepared to implement these compliances if so notified.

5 Data Principal's rights and duties

The Bill grants Data Principals certain rights: (a) the right to access information about the processing of their data; (b) the right to seek the correction or erasure of their data; (c) the right to have their grievances settled; and (d) the right to nominate another individual to exercise their rights in case of death or incapacity.

The Bill also confers certain duties on Data Principals, such as the duty not to impersonate another person, and to provide only such information as may be verifiably authentic when exercising their right to correction or erasure. Their failure to do so may carry a penalty of up to INR 10,000 (USD 120). However, it will not be a justification for a business failing to comply with its own obligations under the Bill.

Data Fiduciaries must ensure that they have the necessary technical and organisational processes in place to permit Data Principals to exercise their rights.

6 Enforcement, adjudication and voluntary undertakings

The Bill creates the first-ever regulator for data protection in the country - the Data Protection Board. The Board (once established) will enforce the enacted form of the Bill. The Board may, further to an inquiry upon a:

a. complaint by a Data Principal,

b. reference by the central government, or

c. direction by a court,

impose penalties (on primarily Data Fiduciaries) for significant contraventions of the Bill. The Bill provides for penalties for specific non-compliances, which may extend up to INR 250 Crores (USD 30 million) for a contravention. Companies may, however, approach the Board through a voluntary undertaking that admits its non-compliance and agrees to carry out rectification measures. If approved by the Board, the undertaking may lower the quantum of the applicable penalties and act as a bar against future proceedings relating to the concerned contravention.

The Bill also permits the central government, in the interests of the general public, to order intermediaries (like cloud service providers or internet service providers) to block access to information contained in any computer resource that enables a Data Fiduciary to provide goods or services to Data Principals in India, where the Data Fiduciary is a repeat offender that has been subject to a monetary penalty at least twice. If the intermediary fails to comply, it can also be subject to a fine of up to INR 50 Crore (USD 6 million). While the Bill does not treat any contraventions as criminal offences, its approach to penalties is markedly different from the more meagre sums under the existing framework, with uncapped compensation payable in only limited circumstances.

These penalties must be factored into by organisations in assessing their compliance costs. Processing activities must be documented to ensure that enforcement actions may be defended. Upon recognising a contravention, voluntary undertakings may be explored.

7 Conclusion

Despite the hefty penalties applicable to significant non-compliances, on the whole, the Bill is not unduly restrictive. While some obligations applicable to Data Fiduciaries may prove a heavier, operational burden in the short run (e.g., providing Data Principals the option to access notice-consent flow in Indian languages), the bulk of the obligations empower the Data Fiduciaries to apply steps suited to them, provided the objective is achieved (e.g., implementing reasonable security safeguards to prevent a data breach).

While certain processing activities concerning protected classes of Data Principals assume a greater risk under the Bill, the approach is not unfamiliar to multinational businesses that face similar requirements elsewhere. With India taking this important step to join other global economies in implementing a data protection regime, businesses will have to put in place appropriate processes to ensure compliance in accordance with the provisions of Indian law.

Having said that, many obligations under the Bill will be clarified through delegated legislation (e.g., how verifiable parental consent must be obtained), indicating that deciphering their precise contours will take time even after the Bill is enacted, giving businesses the time that they need to plan for the future.