

## **Digital Personal Data Protection Bill, 2022: Highlights and preliminary analysis**

The Ministry of Electronics and Information Technology (“**MeitY**”) released the Digital Personal Data Protection Bill (“**DPD Bill**”) on November 18, 2022. The DPD Bill is considerably more concise and ‘reader-friendly’ than the erstwhile Personal Data Protection Bill, 2019 (“**2019 Bill**”) and the subsequent draft Data Protection Bill, 2021 (“**2021 Bill**”). MeitY has [asked for chapter-wise feedback](#) on the DPD Bill by December 17, 2022.

The stated purpose of the DPD Bill is to “*provide for the processing of digital personal data in a manner that recognizes both the right of individuals to protect their personal data and the need to process personal data for lawful purposes*”. We have summarised below the key highlights of the DPD Bill along with our preliminary views.

### **1. No Implementation Period**

The DPD Bill does not specify an implementation period, and simply states that its provisions will come into effect on the date(s) appointed by the Government. However, it states that different dates may be appointed for different provisions of the Act and therefore some provisions may be implemented in a phased manner. The 2021 Bill provided an 18 (eighteen) month implementation period (like the GDPR) and stakeholders had hoped this would be reintroduced in the current draft of the DPD Bill.

### **2. Covers all digital ‘Personal Data’; No concept of “Sensitive” or “Critical” Personal Data**

The DPD Bill does not define ‘Sensitive’ or ‘Critical’ Personal Data or recognize any other sub-set of Personal Data. The DPD Bill merely defines ‘Personal Data’ to mean “*any data about an individual who is identifiable by or in relation to such data*”. Notably, the DPD Bill does not apply to offline Personal Data (that is not digitized), non-automated processing of Personal Data, and Personal Data processed by an individual for any personal or domestic purpose.

### **3. Excludes Non-Personal Data**

The DPD Bill does not define or seek to cover ‘non-personal data’ or anonymised data. This comes as a huge relief to most businesses and stakeholders. The 2021 Bill specifically sought to govern the collection and processing of non-personal data and anonymised Personal Data.

#### 4. Territorial and Extra-Territorial Applicability

The DPD Bill only applies as follows:

(a) **Territorial** - processing of digital Personal Data within India, where:

- (i) Personal Data is collected online; or
- (ii) Personal Data is collected offline and then digitised.

**Note:** The DPD Bill now contains an exemption with respect to the processing of Personal Data belonging to foreign Data Principals (i.e., data subjects) by an Indian entity pursuant to a contract with a foreign person/entity. Such entities are now exempt from the provisions of the DPD Bill that deal with consent (Chapter 2). This is a positive development that will benefit the Indian outsourcing/BPO industry which routinely processes data of foreign nationals.

(b) **Extra-Territorial** - processing of digital Personal Data outside India, if it is in connection with profiling of, or offering goods or services to Data Principals within India.

#### 5. Cross Border Transfer of Data

The DPD Bill does not expressly prohibit cross-border data transfers or prescribe any specific compliances (such as standard contractual clauses or prior Government approval) for the transfer of Personal Data (or any subset of Personal Data) outside India. Instead, it permits a Data Fiduciary (i.e., a data controller) to transfer Personal Data outside India to such countries, and in accordance with such terms and conditions as may be notified by the Central Government.

Notably, the 2021 Bill proposed to impose partial and total data localisation obligations with respect to certain categories of Personal Data, i.e., Sensitive Personal Data and Critical Personal Data. In contrast, ordinary Personal Data was allowed to be freely transferred outside India. Section 17 of the DPD Bill completely disrupts this proposed framework and is expected to ease the free movement of data to trusted geographies.

The explanatory statement accompanying the DPD Bill also recognizes the importance of cross-border data transfers for a globalised economy. This explanation suggests that the Government will not be overly restrictive in its selection of trusted geographies.

#### 6. No Criminal Liability

The DPD Bill only prescribes monetary penalties (under Schedule 1 of the DPD Bill) for breaches and non-compliances and limits such penalties to breaches/non-compliances that the Data Protection Board determines to be 'significant'. The DPD Bill has done away with criminal liabilities, as well as penalties that are directly linked to the turn-over or revenue of an erring Data Fiduciary.

#### 7. Processing of Children's Data Simplified

Provisions relating to the processing of Children's Personal Data have been considerably simplified. Data Fiduciaries that process Children's Personal Data are still required to obtain consent from parents/guardians. However, the following requirements/provisions from the 2021 Bill have been done away with:

- (a) The need to verify the age of the child; and
- (b) The automatic classification of such Data Fiduciary as a 'Significant Data Fiduciary'.

Notably, however, the DPD Bill retains the age threshold for 'Children' at 18 (eighteen) years. Many companies had hoped that the age threshold would be reduced to 13 (thirteen) years (in line with the GDPR).

## 8. Data Protection Board of India

A Data Protection Board of India (the “**Board**”) is proposed to be set up by the Central Government to enforce the provisions of the DPD Bill and impose penalties on erring entities. The Board would be empowered to direct Data Fiduciaries to adopt urgent measures to respond to Personal Data breaches. Any appeal against an order of the Board would lie before the jurisdictional High Court.

## 9. Significant Data Fiduciaries (SDF)

The DPD Bill retains the concept of a ‘Significant Data Fiduciaries’ (“**SDFs**”) and allows the Government to notify an SDF based on, among other things, the volume and sensitivity of Personal Data processed by it, risk of harm to Data Principals, potential national impact and impact on public order.

Certain additional compliances continue to apply to SDFs including:

- (a) The requirement to appoint (i) a data protection officer based in India, as the representative/point of contact for grievance redressal; and (ii) an independent data auditor to evaluate compliance; and
- (b) The obligation to undertake data protection impact assessment (DPIA) and periodic audits.

## 10. Simplified Notice and Consent Requirements

The DPD Bill contains significantly less onerous notice requirements as compared to the 2021 Bill. The DPD Bill requires Data Fiduciaries to obtain consent from Data Principals prior to processing of their Personal Data – through an itemised notice containing a description of the Personal Data being collected and purpose of processing. However, the request for consent must be in clear and plain language and available in the 22 (twenty two) languages listed in the [8<sup>th</sup> Schedule of the Constitution of India](#).

The DPD Bill does not discuss unbundled consents or any requirement for specific consent for individual processing activities while the 2019 Bill and 2021 Bill contained provisions that suggested that separate consents would be required for processing Sensitive Personal Data for individual purposes.

## 11. Introduction of ‘Deemed Consent’

The DPD Bill introduces the concept of ‘deemed consent’ – enabling processing of Personal Data without explicit consent where it is “*reasonably expected that the Data Principal would provide such Personal Data*” and a number of other grounds, including for purposes related to employment (including biometric information) and public interest such as debt recovery, mergers and acquisitions, and prevention of fraud. This is a departure from the position under previous iterations of the DPD Bill (i.e., the 2019 Bill and 2021 Bill), and would likely simplify the consent collection process for businesses.

## 12. Clarity on Consent Managers

The DPD Bill provides further clarity on the role of ‘Consent Managers’. The DPD Bill clarifies that Consent Managers will be interoperable platforms registered with the Board. These platforms will enable individuals to manage, review and withdraw consent provided across Data Fiduciaries and platforms.

## 13. Exemptions

The DPD Bill retains the Central Government’s powers to exempt any instrumentality of the State from application of the Act in relation to processing of Personal Data but does away with the provisions from the 2019 Bill where such exemption is subject to safeguards and an oversight mechanism. Further, the DPD Bill now allows for the Central Government to notify certain Data Fiduciaries or class of Data Fiduciaries based on the volume and nature

of personal data processed, to whom certain provisions of the Bill (notice requirements, accuracy of Personal Data, data retention limits etc.) will not apply.

#### 14. Rights of Data Principals

While the DPD Bill continues to grant Data Principals rights in relation to their Personal Data, such as the right of correction, right of erasure and right to be forgotten – it does away with right to data portability which was earlier proposed under the 2019 Bill and 2021 Bill. The DPD Bill provides the right to nominate any other individual to exercise the rights of the Data Principal in the event of their death or incapacity.

#### 15. Duties of Data Principals

The DPD Bill also imposes certain duties on Data Principals, including the duty to comply with the provisions of “all applicable laws” while exercising their rights, and a duty to furnish only such information as is verifiably authentic while exercising the right to correction or erasure of Personal Data.

### Conclusion

The DPD Bill, in its current form, proposes a simplified and streamlined personal data protection regime for India that is more business friendly and forward-looking than its earlier iterations. The DPD Bill tones down some contentious clauses which caused industry pushback, particularly data mirroring and data localisation requirements. As set out in the explanatory note, many of the changes to the DPD Bill will ease and facilitate both domestic and cross-border domestic flows. While some consent and data-categorisation related changes could potentially impact the overall protection of individual data privacy rights, the Bill is likely to be welcomed by companies in the IT and tech sectors. Some aspects such as the functioning of the Board will need to be time-tested for efficacy.

### Information Technology Practice

JSA provides value added legal services across the whole range of innovative technologies. We advise creators, licensors, buyers, sellers and users of information and technology, on all aspects of technology law. JSA has developed an extensive technology practice in response to the global focus on the development of online systems and services. Our strong expertise and long-standing representation of leading software, telecommunications, and media companies have made us uniquely qualified to address the legal challenges associated with information and communication technology. JSA provides advice on highly sophisticated data management, data security and privacy issues. Our depth of experience gives our clients the crucial advantage of consistent and comprehensive, yet practical advice. We have carried out audit and risk assessments, customised global privacy and information management policies, helped create international data transfer strategies, structure and negotiate complex international data transfer agreements. JSA is well positioned to assist clients in managing the ever-increasing threat in cybersecurity. We routinely help clients in creating, managing and maintaining a secure cyber-presence in the face of escalating threats and legal requirements.

**This Prism has been prepared by:**



**Probir Roy Chowdhury**  
Partner



**Rupinder Malik**  
Partner



**Yajas Setlur**  
Partner



14 Practices and  
23 Ranked Lawyers



15 Practices and  
18 Ranked Lawyers



7 Practices and  
2 Ranked Lawyers



**IFLR1000 India Awards 2021**

10 Practices and  
34 Ranked Partners

-----  
Banking & Finance Team  
of the Year

-----  
Fintech Team of the Year

-----  
Restructuring & Insolvency  
Team of the Year



Among Top 7 Best Overall  
Law Firms in India and  
10 Ranked Practices

-----  
13 winning Deals in  
IBLJ Deals of the Year

-----  
6 A List Lawyers in  
IBLJ Top 100 Lawyer List



Banking & Financial Services  
Law Firm of the Year 2022

-----  
Dispute Resolution Law  
Firm of the Year 2022

-----  
Equity Market Deal of the  
Year (Premium) 2022

-----  
Energy Law Firm of the Year 2021



Ranked #1  
The Vahura Best Law Firms to  
Work Report, 2022

-----

Top 10 Best Law Firms for Women  
in 2022

For more details, please contact [km@jsalaw.com](mailto:km@jsalaw.com)

---

[www.jsalaw.com](http://www.jsalaw.com)



Ahmedabad | Bengaluru | Chennai | Gurugram | Hyderabad | Mumbai | New Delhi



This prism is not an advertisement or any form of solicitation and should not be construed as such. This prism has been prepared for general information purposes only. Nothing in this prism constitutes professional advice or a legal opinion. You should obtain appropriate professional advice before making any business, legal or other decisions. JSA and the authors of this prism disclaim all and any liability to any person who takes any decision based on this publication.