

## *Inside*

## THE ISSUE

- Interviews from women leaders in the corporate and legal fraternity
- Op-ed from the subject experts across the globe
- Articles from the professionals and researchers
- News
- Deals & clearances by CCI



The Corporate and Regulatory Affairs (CRA) E-Bulletin is an initiative of Department of Corporate and Legal Affairs at Associated Chambers of Commerce and Industry in India (ASSOCHAM). The aim of the E-Bulletin is to curate a platform for stakeholders to bring forth the evolving dynamics of corporate and regulatory sectors, challenges and plausible way forward. CRA E-Bulletin is an initiative to engage with the industry stakeholders which is circulated quarterly with rolling submissions on various contemporary themes and market dynamics.

## Interviews

- **Hiroo Mirchandani**, Independent Director on various corporate boards
- **Hetal Dalal**, President & COO, Institutional Investor Advisory Services (IIAS)
- **Vartika Malhotra**, COO, TMT Legal

## OP-ED

- **Prof. (Dr.) Harpreet Kaur, & Dr. Abha Yadav**, NLU-Delhi
- **Dr. Neeti Shikha**, University of Bradford, School of Law, UK
- **Avisha Gupta & Somya Yadav**, Luthra & Luthra Offices
- .....More

## Articles

- **Pallavi Bedi**, Partner, Phoenix Legal
- **Dr. (Prof.) Shilpi Bhattacharya & Kaustubha Kalidindi**
- **Pammy Jaiswal**, Partner, Vinod Kothari & Company
- .....More

# OP-ED

## An insight into the Digital Personal Data Protection Bill, 2022

*-Avisha Gupta & Somya Yadav*

### Abstract

The Ministry of Electronics & Information Technology (“MeitY”) on November 18, 2022, unveiled the draft of the Digital Personal Data Protection Bill, 2022 (“Digital PDP Bill”) for public consultation. The Digital PDP Bill is based on essential privacy and data protection principles of legality, purpose limitation, data minimization, accuracy, storage limitation, reasonable safeguards against unauthorized collection or processing of personal data and accountability for it. It seeks to establish a comprehensive legal framework governing digital personal data protection in India and providing for the processing of digital personal data in a manner that recognizes the right of individuals to protect their personal data, societal rights and the need to process personal data for lawful purposes. This article scrutinizes and highlights some of the key concerns with the Digital PDP Bill.

**Keywords:** Digital Personal Data Protection Bill, 2022, Data Protection Board of India, Screenless Technologies, Consent Managers

### Analysis of the Digital PDP Bill: Issues & Concerns

In an attempt to create a robust data protection framework in India, MeitY introduced the first draft of the data protection bill in 2018 which was later revised in the year 2019. Subsequently, it was referred to a joint committee of both the Houses of Parliament, which submitted the report on the bill in 2021 along with the new data protection bill i.e., Data Protection Bill, 2021. However, owing to the extensive changes made

to the 2019 draft, the same was revoked in 2022 and replaced with the Digital PDP Bill. The Digital PDP Bill is a significantly simplified, shortened and principal-based version of the previous bills and leaves many implementational aspects to be prescribed subsequently by the Government.

In contrast with the earlier version which included within its ambit ‘non-personal data’ and ‘data in physical form’, the scope of the Digital PDP Bill is limited to the processing of digital personal data (a) which is collected from data principals online; and (b) such personal data collected offline, is digitized. The Digital PDP Bill replaces the Data Protection Authority of India with the Data Protection Board of India (“Board”) while significantly reducing its autonomy and independence. Further, the Digital PDP Bill introduces certain duties for the data principal such as not registering false or frivolous grievance or complaint with a data fiduciary or the Board, which was absent from the previous versions of the bills. It also introduces the concept of consent manager which is tasked with the responsibility of enabling a data principal to give, manage, review and withdraw her consent through an accessible, transparent and interoperable platform. Further, the Digital PDP Bill provides enhanced financial penalties for non-compliance of its provisions and prescribes penalties in accordance with the subject matter of the non-compliance.

Although the Digital PDP Bill is drafted keeping in mind the understanding that emerged during the deliberations with the industry players in the

process of drafting previous data protection bills, however, certain concerns and new challenges emanating from the Digital PDP Bill remain - which needs to be addressed before the implementation of the Digital PDP Bill.

The Digital PDP Bill excludes from its ambit such personal data which are collected offline but not digitized illustratively, the data collected by Government agencies especially in rural areas, data collected by businesses which do not convert personal data into digital form subsequently, data collected and processed manually by organizations. Such classification between online and physical personal data is created without any express rationale and in effect, it may conflict with the agenda under the Digital India Campaign of the Government as the exclusion of offline and non-digitized data would dissuade the companies and the local government bodies from going digital owing to the reason of compliances applicable to digital data. Further, the Digital PDP Bill does away with the categorization of personal data into 'sensitive personal data' and 'critical personal data'. As a consequence, all the obligations and the restrictions are applicable to all types of personal data including sensitive personal data, which appears to be onerous and without regard to sensitivity of data.

Further, the Digital PDP Bill prescribes that a data principal is deemed to have given consent to the processing of his personal data if such processing is necessary for 'fair and reasonable purpose', 'public interest' etc., including for the purpose of credit scoring. The term 'fair and reasonable purposes' is fairly broad and ambiguous and may lead to misuse of data principal's consent. Notably, factors like credit scoring should be avoided to be included in the grounds for obtaining deemed consent and the Government

might consider providing an exhaustive list of purposes for which deemed consent would be considered.

The Digital PDP Bill proposes similar reporting obligations upon the data fiduciaries as provided under CERT-In directions related to cyber incidents, issued under Information Technology Act, 2000. Such an obligation of multiple reporting would prove to be counterproductive and onerous as the focus of the data fiduciary would shift from 'redressing the data breach' to 'complying with multiple laws'. Hence, more clarity is required in cases where the incidents are reportable under multiple laws.

The issue of multiple reporting is further exacerbated by the various sectoral laws that impose data privacy obligations including laws governing banking, telecommunications, healthcare, and securities. Although, it has been provided that the sectoral laws would be read in conjunction with and in addition to the Digital PDP Bill, however, it remains unclear as to how the provisions of the Digital PDP Bill will be reconciled with the provisions of these sectoral laws. For instance, RBI's data localization requirements in respect of payments data, will need to be read and given effect harmoniously with the Digital PDP Bill, which is silent on the aspect of data localization. However, as regards the exemptions provided for in the RBI localization circular (as that of permission to store copy of domestic component abroad for cross border transaction data, or to process data outside India provided it is brought back within 24 hours), there is no express clarity on whether such exemptions would continue to prevail to the extent of any personal data forming part of the payments data.

Another important aspect having a wide impact, is with respect to cross-border data transfer. The

Digital PDP Bill provides for prescription of specified countries and terms under which personal data can be transferred outside India. Notably, the Digital PDP Bill in its current form is vaguely worded and many important aspects have been left for prescription by the Government at a later point in time. This had caused much confusion on the precise form and structure of implementation of these provisions, including on aspects such as timelines for ensuring compliance and basis for Government's selection of permitted or white-listed countries.

The Digital PDP Bill empowers the Government to formulate laws on key areas, for instance, exempting the processing of personal data by any instrumentality of the State in the interests of sovereignty and integrity of India and for research etc. This appears to give much unfettered discretionary powers at the hands of the Government and requires to be balanced with some reasonable restrictions by way of well-defined process and procedures. Further, there are concerns around the functions and structure of the proposed Board as there is involvement of Government's discretion in deciding the powers and functions of the Board.

Another key industry concern on the Digital PDP Bill is in respect of financial penalty for non-compliance. It is provided that upon the conduct of an inquiry, if the Board finds non-compliance by an individual to be 'significant', it may impose a financial penalty for up to ₹500 Crores. Interestingly, the term 'significant' is a matter of subjective determination and hence open to interpretations. It would hence be important to have some defined benchmarks and standards around the term significant for determining quantum of financial penalties for transparency.

Lastly, with the fast-paced technological development, another aspect that requires

deeper thought is that apart from the collection of data by the companies through computer resource, significant amounts of personal data are also being collected ambiently through screenless technologies such as Internet of Things (IoT) smart devices or products, touch sensors, cameras and other ambient computing devices and artificial intelligence-based devices. Generally, the notice and consent framework involve the displaying of privacy policies on the screen through which the individual is made aware of the collection and processing of the personal data. However, in the present times, where human interactions with the technology goes beyond screens, out of the box thinking and technology-neutral approach in terms of notice and consent framework would be required to be developed.

### Conclusion

Remarkably, the introduction of the Digital PDP Bill is undoubtedly a step in the right direction as it provides the much necessary data privacy safeguards to the personal data of the individuals. However, concerns and gaps as highlighted in the Article and many others, would need to be reconsidered before the Digital PDP Bill is passed as law. Reportedly, the new data bill is to be tabled in the Parliament during the monsoon session in July. A practical, implementable law balancing both privacy and business considerations is hoped for.

**About the Authors:**

**Avisha** is Partner at Luthra & Luthra Offices. She has over 10 years of experience and specializes in Technology laws including Fintech, Data Privacy, and host of other

emerging technologies such as E-Commerce, Cloud based Services, OTT Platforms, AI, Crypto Currencies, Blockchain, IoT, Health Tech, and Digital Maps. Currently, she is working as a partner in Luthra and Luthra Law Offices.



**Somya** is currently working as an associate with the Technology, Media & Telecommunications team of Luthra & Luthra Law Offices.