



The Dialogue™  
INFORM ENGAGE IDEATE

# THE PERSONAL DATA PROTECTION BILL, 2019

## BUSINESS IMPLICATIONS

Karthik Viswanath



# BUSINESS IMPLICATIONS

## 1. Introduction

India's Personal Data Protection Bill 2019 ("PDP 2019") is currently being deliberated by the Joint Parliamentary Committee (JPC). The objective and reason for enacting this Bill dates to 24th August 2017 when the Supreme Court of India delivered its judgement on Justice K.S Puttaswamy and others vs Union of India, declaring privacy as a fundamental right under Article 21 of the Indian Constitution. The judgement also directed the Government of India to bring in a robust data protection regime for the country to safeguard the informational privacy of the citizens.

As India moves closer towards enacting a nuanced data protection regime, it is essential to deliberate on some of the PDP 2019's business-related considerations to allow for balanced trade-offs, which would enable innovation through protecting business interests in a digital economy. Some of the pertinent elements under business-related considerations discussed in this primer are compliance costs, the position of start-ups, cross border data flows, the inclusion of non-personal data within the ambit of the PDP 2019.

## 2. Business related considerations


### 2.1. Cross Border Data Flows

The movement of information across national borders drives today's global economy and is predicated on cross-border data flows. Facilitating free flow of data would be advantageous to the objective of enabling a trillion-dollar digital economy. Micro, Small & Medium Enterprises (MSMEs) would stand to be the biggest gainers (through e-commerce platforms) as they would be able to tap into global markets, reaching customers, suppliers and partners that would otherwise be inaccessible to them. The US Chamber of Commerce, in a 2016 study, estimated that removing barriers to cross border data flows could create 2.89 million new companies

(composed chiefly of MSMEs). The study also found that companies that relied on cross border technologies had higher survival rates (54%) than offline companies. But the provisions on cross border data flows as it stands in the PDP 2019 contradicts these ideals and would cause various issues, as discussed below.

**Security paradox:** The PDP 2019 places restrictions on the transfer of sensitive and critical personal data. In the 2019 Bill, the word 'only' has been omitted, therefore by necessary implication sensitive personal data may be mirrored in other jurisdictions. As for critical personal data, that may be stored only in India, except for certain exempted situations. However, placing restrictions on cross border data flows neither provides additional security/privacy of data and/or increased access to the same. Though often perceived so, the security of data is not a function of where it is stored.

**Slowdown in the process:** At present, there is a requirement to obtain the Data Protection Authority's (DPA) approval for cross-border transfers made pursuant to contracts. The usage



of contractual clauses to facilitate the cross-border transfer of data is commonplace. This would lead to a situation where every company will have to seek approval from the DPA to fulfil every cross-border contractual relationship and deed. Therefore, DPA would be inundated with requests, which would eventually delay the performance of contracts with overseas parties. This could be detrimental to India's vision of improving ease of doing business.

### Our Recommendations

- Develop tools that allow for cross border data flows- including preparing interoperable data protection regimes, data sharing agreements based on adequacy decisions etc.
- Narrowly specify designated data that cannot be shared- which is of strategic importance to India.


## 2.2 Removal of Non-personal data (NPD) sharing in the Personal Data Bill


The Preamble of the PDP 2019 defines its scope to the governance of personal data and protection of privacy of its citizens. Allowing the Government to direct companies to share their non-personal data, the PDP 2019 goes beyond its scope and causes various issues, as discussed below.

**Blocks innovation:** In any case, expanding the scope of the preamble to allow for the governance of non-personal data does not solve the fundamental problem associated with enabling government access to non-personal data, which clashes with the IP rights that companies enjoy over their proprietary information. This clash with the IP rights will also disincentivise businesses from producing new and innovative data-based products and services as their investment over the data will no longer be lucrative with disclosure mandates.

**Re-identification threat:** In the absence of appropriate safeguards, such access also poses serious privacy risks, since aggregated and anonymised datasets can be used to identify individuals through re-identification techniques.

**Complexity around regulating NPD:** It becomes a very complex topic, the implementation of which requires extensive consultation and analysis. While sharing non-personal data with the Government might enable legitimate benefits for society, such as providing better service delivery and implementing crucial policies for the digital economy, it must be done within a defined framework that allows businesses with sufficient bargaining power. Barring this, it might lead to a chilling effect on the operations of businesses in India both in new domestic and foreign investment and may work entirely against the Government sentiment of increasing trade in India.





**Clash with NPD governance framework:** Since a separate committee of experts formed under chairperson Kris Gopalakrishnan is deliberating upon the governance framework for non-personal data, it is ideal for the PDP 2019 to refrain from having provisions on non-personal data to smoothen the overlap in regulatory boundaries. The committee of experts had also recommended through their report that any provisions related to non-personal data, have to be deleted from the PDP 2019 to ensure that these two frameworks are mutually exclusive yet work in harmony.


### Our Recommendations


- Separate data protection framework and the enabling framework for facilitating non-personal data sharing. Combining the two before adequate consultation and thought can create widespread confusion.
- Harmonising provisions of NPD governance and the PDP 2019 for seamless implementation.
- In developing any such data sharing framework, the Government must consider concerns associated with sharing proprietary data (such as algorithms, trade secrets, confidential information, customer/vendor lists, etc.), which is critical to running businesses.

### 2.3. Implementation Timeframe

The PDP 2019 can have significant socio-economic implications across the entirety of India's digital landscape for both big and small-scale industries. Given how the Bill can fundamentally change the nature and functioning of organisations through its overarching reach, it is vital to provide organisations, enterprises, and industry bodies who are going to be impacted by or shall be working within the ambit of the PDP 2019, with the adequate time for understanding the basic principles and requirements espoused by the law, as well as to adapt to it. For instance, The General Data Protection Regulation in the European Union (the EU GDPR), which came into force in 2018, provided for a transition period of 2 years. While the Bill refers to a phased implementation, the importance of adequate timelines- not just for provisions of the Act, but also for any rules notified by the DPA- must be stressed; otherwise, it would cause various negative implications, as discussed below.

**One size fits all issue:** In India, the implementation of the privacy regime is a fresh start for regulators and domestic industries. This Bill will require a variety of industries, both digital and analogues ranging from Automotive, Retail, Oil & Gas PSUs, Power companies, Health services, and many others, to learn and comply. Therefore, provisions of the PDP 2019 can't be one size fits all where tailoring it horizontally (within the sectors including Government entities) and vertically (across various sectors) and operationalising the same would require sufficient guidance and customisation.





**Timeline issue:** Given the GDPR experience, there must be provisions that provide a clear timeline for transition, which will allow companies, especially start-ups, with the sufficient time needed to make modifications to their data processing mechanisms to ensure adequate compliance with the requirements of the Bill. Similarly, large corporations require time to streamline the international supply chain, integrate their IT systems, and re-negotiate contracts with multiple countries. If the time allowed for implementation is inadequate, it can not only bring some activities to a halt but can also damage India's image as a secure location for data processing.


### Our Recommendations

- There should be a minimum of 24 months for entities to prepare and comply from the date of notification of a particular standard/code of practice or rule.
- The phased implementation must occur in a manner similar to the following:
  - Step 1: Provide timelines for the formation of the DPA
  - Step 2: State minimum lay off periods of 24 months for applicability of any particular rule/standards/code of practice from the date of its notification. (This period will exclude the stakeholder consultation that the DPA must undertake before notification of such standard/code of practice or rule.)
- Account for extra time for data processors who deal with the data of foreign nations; there might be a need for additional timelines, as such changes would entail the need for international contract re-negotiations.

#### 2.4. Start-ups and Ease of Doing Business in India

As of 2021, there are about 490+ Unicorn companies globally, out of which 25+ are in India, making India the third-largest start-up ecosystem – only behind China and the USA. What changed from 2017 to 2018 for India was the addition of new and specialised sectors like ed-tech, food delivery, B2B, health tech, insurtech, etc. Besides, the stronghold of already thriving internet software & services – e-commerce & marketplace and fintech, only increased. As India is becoming a start-up hotspot, it is crucial to weed out the following issues emerging for the start-ups with the PDP 2019 enactment.

**Exemptions vs privacy:** Vagueness in definitions, steep compliances, stifling IP rights prove to be problematic for start-ups. The PDP 2019 mandates significant data fiduciaries to obtain registration, conduct independent audits, and comply with reporting requirements. This will likely increase compliance costs for start-ups, which may not be commensurable with their available resources and funds. The Bill must aim to promote innovation and entrepreneurship in the country, which could invite more investments. Moreover, the exemptions from certain compliances must be in a manner such that it is not prejudicial to the privacy of individuals






but at the same time beneficial for start-ups.

**Transition cost:** Start-ups require assistance and regulatory guidance to comply with the provisions of the PDP 2019. For start-ups to undergo a smooth transition from provisions on data protection under the Information Technology Act to the proposed PDP 2019 will require capacity building through various sessions and knowledge material. Apart from the technical personnel, they will have to hire regulatory experts, requiring extra capital investment from the start-ups. Despite these capital constraints, regulatory compliance costs will also stifle the start-ups' functions. Still, this transition would provide a reasonable starting point for start-ups and SMEs to begin exploring options and evaluating their current data protection standards with respect to the PDP 2019.

### Our Recommendations

- To ease the troubles of the start-up and MSME communities, there must be a carve-out with different and relaxed compliance standards. This could be based on a financial threshold and help these companies plan out compliance and improve their business.
  - It is vital to relook at the liability regimes under the Bill, as non-compliance will lead to drastic measures from DPA. This would stifle innovation, as many would-be fearful of criminal prosecution.
- 

The Dialogue is a public-policy think-tank with a vision to drive a progressive narrative in India's policy discourse. Founded in 2017, we believe in facilitating well-researched policy debates at various levels to help develop a more informed citizenry, on areas around technology and development issues.

The Dialogue was ranked amongst the Top-Ten think-tanks in the world to watch out for by the Think-Tank Civil Societies Programme, Lauder Institute, University of Pennsylvania, in their 2020 and 2021 ranking index.

Email: [info@thedialogue.co](mailto:info@thedialogue.co)  
Website: [www.thedialogue.co](http://www.thedialogue.co)



**The Dialogue**<sup>™</sup>

INFORM ENGAGE IDEATE