

# Technology Law Analysis

December 24, 2019

## PRIVACY IN INDIA - WHEELS IN MOTION FOR AN EPIC 2020

### I. BACKGROUND

The much-awaited *Personal Data Protection Bill, 2019* ("**PDP Bill**") was introduced in the lower house of Parliament in India on December 11, 2019.

The PDP Bill is an omnibus, cross-sector privacy law, with similarities to the E.U. General Data Protection Regulation (GDPR) and the California Consumer Privacy Act. It is a substantially revised version of the *draft* Personal Data Protection Bill, 2018, that was proposed in July 2018 by a Committee of Experts set up by the Government, chaired by retired Supreme Court judge, Justice Srikrishna ("**Committee**"). Along with the bill, the Committee had released their report with views and deliberations giving context to the bill ("**Report**").

On December 12, 2019, the PDP Bill was referred to a Joint Parliamentary Committee for further debate and examination ("**Parliamentary Committee**"). The Parliamentary Committee has been instructed to give its report to the Lok Sabha on the first day of the last week of the Budget Session, 2020. The Parliamentary Committee has invited comments from stakeholders on the PDP Bill, based on which further changes may be made in the PDP Bill, along with the inputs of the Parliamentary Committee.

The PDP Bill will need to go through the following steps before it becomes binding law:

1. Submission of the Parliamentary Committee report;
2. Passing by both Houses of Parliament;
3. Presidential assent followed by notification in the Official Gazette.

However, since the PDP Bill does not have any transitional provisions (such as the GDPR or the California law), businesses should strongly consider beginning preparation for its implementation. The implementation of various provisions is dependent on the Government notifying such provisions into law. Some reports suggest that the Government is likely to give companies a two-year window to comply,<sup>1</sup> although this remains a matter of discretion and we would suggest that a transition period is provided for in the text of the PDP Bill.

The PDP Bill seems to dilute provisions with respect to data localization and cross-border data transfers, as well as provisions for criminal liability as compared to the earlier avatar. However, it introduces some new concepts and provisions such as 'social media intermediaries', a 'consent manager' and the provision of a regulatory sandbox.

This hotline discusses the highlights of the PDP Bill, along with our analysis of significant changes.

### II. HIGHLIGHTS OF THE PDP BILL AND WHAT IT MEANS FOR YOU

- 1. Major overhaul of current data protection law in India:** The erstwhile data protection regime under the *Information Technology Act, 2000*, was limited in scope to electronic information, largely concentrating on sensitive personal data and information. It was a notice-and-consent-based regime, with minimal compliances. The PDP Bill is a far more complex and far-reaching than the current law.
- 2. Extra-territorial application:** It applies to entities outside India if they have a business connection to India or carry on profiling of individuals in India.
- 3. New data regulator (the Data Protection DPA, the "DPA"), adjudicating officers, and appellate tribunal:** The PDP Bill introduces a specialized regulatory approach to data protection. The DPA will be the first cross-sector data protection regulator in India and has significant regulation-making powers.
- 4. Subordinate legislation:** The PDP Bill delegates a host of important matters, including the specification of types of data, classes of regulated entities, and codes of practice to the Central Government and the DPA. A true compliance picture will form only when these rules and regulations are framed.
- 5. Wider categories of data protected:** Most parts of the PDP Bill apply to all 'personal data'. Higher benchmarks of compliance are prescribed for 'sensitive personal data' and 'critical personal data' (which are subsets of 'personal data').

Non-personal data / anonymized data does not qualify as 'personal data', and the compliance requirements applicable to personal data

## Research Papers

### Little International Guide (India) 2024

November 08, 2024

### Unmasking Deepfakes

October 25, 2024

### Are we ready for Designer Babies

October 24, 2024

## Research Articles

### The Bitcoin Effect

November 14, 2024

### Acquirers Beware: Indian Merger Control Regime Revamped!

September 15, 2024

### Navigating the Boom: Rise of M&A in Healthcare

August 23, 2024

## Audio

### Digital Lending - Part 1 - What's New with NBFC P2Ps

November 19, 2024

### Renewable Roadmap: Budget 2024 and Beyond - Part I

August 26, 2024

### Renewable Roadmap: Budget 2024 and Beyond - Part II

August 26, 2024

## NDA Connect

Connect with us at events, conferences and seminars.

## NDA Hotline

Click here to view Hotline archives.

## Video

### "Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FI8 event in Riyadh

October 31, 2024

### Analysing SEBI's Consultation Paper on Simplification of registration for FPIs

September 26, 2024

do not apply to these forms of data. However, as discussed below, the PDP Bill provides an important exception for the Government to direct organizations to provide their non-personal in certain circumstances.

6. *Data localization for sensitive data:* A copy of all 'sensitive personal data' must be stored in India but may be transferred outside India. 'Critical personal data' (which will be defined by the Central Government) must be processed only in India, with exceptions. Organizations processing sensitive personal data should prepare their infrastructure for data localization.
7. *Cross-border transfer restrictions:* Mere personal data (that is non sensitive personal data or critical personal data) has been exempted from cross-border transfer restrictions.
- Sensitive personal data may be transferred outside India if there is:
- (a) Explicit consent of the individual, and
- (b) Either:
- i. A regulator-approved contract or intra-group scheme for the transfer; or
- ii. A regulator-approved transferee entity or country.
- Data notified as 'critical personal data' may be transferred outside India on certain narrow grounds.
8. *Privacy principles:* The principles underlying the PDP Bill are largely in line with global regulation, and include consent (with exceptions), purpose limitation, storage limitation and data minimization.
9. *Rights-based law:* The rights conferred on individuals include:
- the right to data portability;
  - the right to be forgotten;
  - and the rights to access, correction, and erasure.
- Data fiduciaries (those that determine the purpose and means for processing) will need to implement processes to honor these rights when exercised by individuals.
10. *Consent managers:* A new concept of registered 'consent managers' who liaise between individuals and data fiduciaries, including for the exercise of the above rights, has been introduced.
- The idea of 'consent managers' is innovative but relatively untested. It appears intended to mitigate the concern of 'consent fatigue' and help educate the uninitiated. These entities will be a new class of players in the data ecosystem. It will be interesting to keep an eye on the implementation of the consent manager framework.
11. *Three types of regulated entities:* In increasing order of compliance obligations, these are:
- a. Data processor (akin to the eponymous GDPR concept);
- b. Data fiduciary (akin to the GDPR 'data controller'); and
- c. Significant data fiduciary (a subset of data fiduciary).
- Significant data fiduciaries ("SDFs") are treated as full-fledged regulated entities and are required to implement independent data audits, appoint a data protection officer, and carry out data protection impact assessments prior to carrying out any processing with a risk of significant harm, among other obligations. SDFs include 'social media intermediaries' with over a certain number of users.
12. *Data breach notification:* In case of a data breach, the DPA is to be intimated, who may require that the data breach be reported to affected individuals and that remedial action be taken.
13. *Special provisions on children's data:* The PDP Bill provides for age verification; parental consent; and raised obligations for 'guardian data fiduciaries' (a class of designated entities whose services are directed at children or who process large volumes of children's personal data).
14. *Innovation sandbox for artificial intelligence and emerging technology:* The innovation sandbox is supervised by the regulator, and eligible data fiduciaries can avail of relaxations from certain obligations of the PDP Bill up to a maximum period of 3 years.
15. *Government requests for anonymized and non-personal data:* The Central Government has been given the power to direct that anonymized / non-personal data be shared by any entity with the Central Government, in certain circumstances.
- This is a provision directed at the use of data for public good; Rules in this connection are awaited to flesh out more detail. A separate

16. *GDPR-like penalties:*

government-appointed committee is also examining this subject. The PDP Bill provides for civil compensation; financial penalties such as fines (up to 4% of global turnover); and criminal penalties in the limited case of unauthorized de-identification of data.

*Our detailed analysis of the PDP Bill is available [here](#).*

*We have recently conducted two global webinars wherein we have discussed our analysis of the PDP Bill.*

*The recording of our webinars are available [here](#).*

**Technology & Privacy Law Team**

<sup>1</sup> <https://tech.economictimes.indiatimes.com/news/internet/companies-may-get-up-to-2-years-to-comply-with-data-law/72432037>, last visited on December 18, 2019.

---

**DISCLAIMER**

The contents of this hotline should not be construed as legal opinion. View detailed disclaimer.

This Hotline provides general information existing at the time of preparation. The Hotline is intended as a news update and Nishith Desai Associates neither assumes nor accepts any responsibility for any loss arising to any person acting or refraining from acting as a result of any material contained in this Hotline. It is recommended that professional advice be taken based on the specific facts and circumstances. This Hotline does not substitute the need to refer to the original pronouncements.

This is not a Spam mail. You have received this mail because you have either requested for it or someone must have suggested your name. Since India has no anti-spamming law, we refer to the US directive, which states that a mail cannot be considered Spam if it contains the sender's contact information, which this mail does. In case this mail doesn't concern you, please unsubscribe from mailing list.