IKIGAI LAW

DECODING INDIA'S PROPOSED DATA PROTECTION LAW

contact@ikigailaw.com | @ikigailaw

India's data protection law is close to being finalised. The Joint Parliamentary Committee (**JPC**) examining the Personal Data Protection Bill 2019 (**PDP Bill**) submitted its report (**Report**) in Parliament in December 2021. The JPC has recommended a fresh version of the law- the Data Protection Bill, 2021 (**DP Bill**). The change in the name of the PDP Bill reflects the expanded scope of the law to regulate non-personal data (**NPD**) (business information/anonymised data) as well. Here's a summary of the Report, and a clause wise mapping of the PDP Bill, against the Report.

Once enacted, the DP Bill will require companies (both Indian and foreign) to revamp their operational practices. This post provides an overview of the major practical concerns raised by this Bill.

1. Who is affected by the DP Bill?

In addition to Indian companies, the DP Bill applies to: (i) companies that process data in India, (ii) companies outside India that process data in connection with a business in India, and (iii) companies outside India that process data in connection with any activity which involves profiling of people within the territory of India. Therefore, even businesses outside India can be covered.

2. Will the DP Bill change how companies treat personal data?

The DP Bill sets out how companies should process personal data. Processing means the use, collection, recording, organisation, storage, alteration, indexing, disclosure and erasure of personal data, amongst other things. Since many tech companies perform these operations on personal data, they will be required to comply with the obligations in relation to processing.

Operationalising the privacy framework under the Bill will require companies to make significant changes to their data collection and processing practices.

For example, companies will now need to take fresh consent from their users for processing their data, as per the detailed consent requirements under the Bill. Companies will also need to prepare a 'privacy by design' policy. This policy should describe: business practices and technical systems adopted to protect personal data, strategies to anticipate and avoid 'harm' to individuals, and how individuals' interests are accounted for at every stage of data-processing.

3. What about non-personal data?

Both personal data and NPD including anonymised data, are covered by the DP Bill. The Report recommends that once separate regulation for NPD is finalised, it can be made part of the same law. And the Data Protection Authority (**DPA**) will be empowered to look into matters related to NPD as well. The DP Bill also allows the government to direct companies to share NPD/anonymised personal data for improving service delivery or policy making purposes.

4. Does the DP Bill restrict cross-border transfers of data?

The DP Bill makes it difficult for companies to transfer data outside India and calls for strict data localisation norms. Critical personal data (category of personal data which will be defined by the central government) must be stored in India, and can only be transferred under limited circumstances (eg. health purposes/emergency). Sensitive personal data (financial data, health data, biometrics) must also be stored in India, though it can be transferred outside India subject to certain conditions, such as through contracts/ intra-group schemes that are approved by the DPA, in consultation with the central government.

5. Will companies need to change the way in which they obtain user consent for processing personal data?

The DP Bill requires companies to acquire user consent in order to process even their personal data (for eg., names, e-mail ids etc.)- marking a shift from the current framework which requires companies to obtain consent for sensitive personal data (e.g., financial data) only. For consent to be valid- it must be freely given, informed, specific, capable of being withdrawn and indicated through affirmative action (meaning 'pre-checked' consent boxes may no longer work). While seeking user consent, companies will have to provide users with detailed notices at the time of collection of data.

6. Should companies be concerned by the classification of sensitive personal data under the DP Bill?

Financial data, health data, biometric data, genetic data, data indicating religious/political beliefs/sexual orientation or caste/tribe status are considered sensitive personal data under the DP Bill. The DP Bill imposes stricter standards for processing such data as compared to the standards under India's current data protection framework. For example, companies collecting or processing such data will need explicit user consent – meaning that they will have to inform users of the consequences of processing their data and inform them of processing which is likely to cause them significant harm, in addition to the regular notice and consent requirements.

7. Does the DP Bill apply different standards to different companies?

The DP Bill allows the government to notify certain companies as 'significant data fiduciaries' (SDF) based on certain criteria. This includes the volume of personal data processed, the sensitivity of data, processing of children's data, among others. Once classified as SDF, companies will have to comply with heightened obligations like conducting data protection impact assessments, appointing data protection officers, and in the case of social media companies, enabling their users to voluntarily verify their accounts. This means that large companies that process large volumes of personal data and have high turnovers can be notified as SDFs, and meet these additional obligations.

8. Will the DP Bill affect how companies should treat children's personal data?

The DP Bill defines "child" as any person below the age of 18. It bars all companies from profiling, tracking, targeting ads towards children or processing data in a way that causes them 'significant harm'. The DP Bill also requires all companies to implement age gating and obtain the consent of parents/guardians to process personal data of a child. The DPA will specify age gating mechanisms through regulations. Companies that process children's data may classify as SDFs and will be subject to additional obligations.

9. Are there any restrictions on the amount of data that can be collected by companies?

The DP Bill allows companies to collect data that is necessary for processing. This could create difficulties – as it may not always be possible to determine the exact purpose of data collection beforehand. For instance, with devices that work in an Internet of Things (**IoT**) ecosystem, the purposes for which data may be used are constantly evolving, and so it could be difficult to spell out exactly what purpose the data is going to be collected for.

10. Does the DP Bill have implications for proprietary rights of companies?

Companies will have to share information on 'fairness of algorithm', which may have implications on their intellectual property rights, especially if algorithms include source codes. At this stage, it is unclear what would be the threshold to judge 'fairness' and how much information will be sought.

Additionally, the DP Bill permits users to request companies to transfer/port their personal data to another company or themselves. The scope of personal data that can be transferred is broad as it includes data generated in the course of providing services to users and any data which forms part of a user's profile. Such data includes confidential business insights and trade secrets.

11. Does the DP Bill provide for any certifications?

The DP Bill empowers the DPA to create a framework to monitor, test and certify hardware and software for computing devices to prevent any malicious insertion that may cause data breach. If implemented, companies may have to comply with new, indigenous certification standards for both hardware and software elements of its computing device/tech products.

12. Who will regulate this new law?

The DPA will be responsible for the enforcement of the law. The JPC recommends that the same regulator should govern both personal data and NPD.

13. What are the consequences of non-compliance with the DP Bill?

Non-compliance can attract penalties of up to INR 15 crores or 4% of worldwide turnover, whichever is higher. The JPC recommends giving government the power to consider penalties for start-ups and smaller companies separately.

14. Will companies have time to comply with the DP Bill?

The Report recommends a phased implementation of the law- going up to two years' timeline for complete compliance.