KPMG

Building block of the Indian digital economy

Personal Data Protection Bill, 2019

Overview

Over the past few years, digital adoption across industries has skyrocketed generating more information about us than ever before. This has led organisations to perform demographics, psychographics, behaviour profiling and segmentation to name a few on their customers and employees. Data-rich India is bound to attract large scale foreign investments and regulatory scrutinies, so it's about time that India comes up with its own Data Protection Act.

India's Union Cabinet on 4 December, 2019 had approved the Personal Data Protection Bill, 2019 (the bill) to be introduced in the winter session of Parliament. The bill has been referred to a 30-member joint committee. This committee is expected to make its first report to the Lok Sabha by the last week of the Budget Session 2020. While the committee is reviewing the bill, organisations across India are preparing for this paradigm shift.

Key highlights

1. Under the bill, the right to be forgotten permits data principals to restrict or prevent the processing of their data. To exercise this right, an application must be made by the data principal to an Adjudicating Officer appointed by the authority
2. All the data fiduciaries will now be required to prepare a Privacy by Design policy and they may also submit it for certification to the authority
3. The bill proposes creation of a sandbox for encouraging innovation in the field of emerging technologies such as artificial intelligence and machine learning, in the public interest. Data fiduciaries whose Privacy by Design policy has been certified by the authority will be eligible to apply for inclusion in the sandbox
4. The authority may direct data fiduciaries to post details of personal data breaches on their website
5. Organisations, who are significant data fiduciaries, should have their policies and internal processes audited by an independent data auditor. The auditor may assign a rating in the form of a data trust score, the criteria for which will be provided by the Data Protection Authority of India (DPAI). Organisation can publish their data trust score to demonstrate their compliance with the requirements with the bill
6. Certain data fiduciaries may be designated as 'significant data fiduciaries', based on factors such as the volume of personal data processed, sensitivity of such data, annual turnover of the data fiduciary, the risk of harm from any processing undertaken by the data fiduciary, use of new technologies, and any other factor that may be relevant in causing harm to any data principal as a result of such processing. Significant data fiduciaries will be subject to increased compliance standards, under the bill
7. All social media intermediaries that have been classified as significant data fiduciaries are required to provide their users the ability to voluntarily verify their accounts and all such verified accounts are required to be provided with a mark of verification which is publicly visible
8. The bill has introduced a new role called Consent Manager. These Consent Managers would be responsible for obtaining, withdrawing, reviewing and managing the consent from the data principals. This may create a new industry of consent managers who shall have the required capabilities and expertise. Data principals can utilise their services in dealing with data fiduciaries
9. The new data localisation requirements allows processing of sensitive personal data outside India however mandates organisations to store a local copy within the territory of India
10. Certain public/private entities will be exempted from obligations under the bill for purposes including national interest, prevention of crimes, journalistic or research work, technological advancement under the sandbox to name a few.
11. Any offence punishable under the bill will be considered cognisable and non-bailable as per their definitions under the Code of Criminal Procedure, 1973.

Our point of view

- Official identifiers and financial data have been categorised as sensitive personal data. Since these data types are recorded by most of the organisations from their employees, identifying the appropriate legal grounds for processing will be a topic for deliberation
- Data fiduciaries can publish the certified Privacy by Design policy in their website and authority's website. This will be a useful reference for organisations who are embarking on their privacy compliance journey
- The timeline for compliance to the bill once passed has not been defined in the current version of the bill vis-à-vis the 18-month period that was defined in the erstwhile version. To ensure seriousness and define a starting point of enforcement, the bill could consider 24 months like General Data Protection Regulation (GDPR) to adhere to the requirements of the bill
- As per the GDPR, organisations have been going through challenges in adhering to the 72 hours timelines to report the breaches to the supervisory authorities. The bill has not currently stipulated a defined timeline for reporting breaches. Though this comes as a relief to the organisations, one must consider the harm caused by the breach to the data principals
- All significant data fiduciaries need to provide their data protection impact assessment with findings to the authority for review as per the guidelines defined. Considering the authority can direct data fiduciaries to cease processing of such activities causing harm to data principals, a robust process should be established for timely review and response
- Industries such as EdTech, gaming, social media to name a few which provide services to children below 18 years of age, should refrain from monitoring, behavioural tracking, and targeted advertisements. This may require such organisations to relook at their business model and marketing strategies
- Organisations can charge the data principal a fee for providing a summary of the processing activities on their data and also for porting their data. This may curtail the data principals from exercising these rights due to the cost implication.

Way forward:

While the bill undergoes deliberation and amendments based on the recommendations of the joint select committee, organisations across India need to kickstart their journey for a privacy ready future. It is critical to have a strong foundation to build a robust Enterprise Privacy Management framework and organisations are advised to take the following considerations into cognisance:

Step 01

Is it applicable to you?

It is applicable if your organization	It is not applicable if your organisation
Processes personal data in the territory of India	Processes anonymised data
Processes personal data of Indian citizens	non personal data
Provides systematic activity of offering goods or services within the territory of India	
Profiles data principals within the territory of India	

Step 02

What is your role?

- Data fiduciary
- Significant data fiduciary
- Guardian data fiduciary
- Data processor

Step 03

Understand the scope. What data do you possess?

- Personal data
- Sensitive personal data
- Financial data
- Anonymised data
- Biometric data
- Genetic data
- Health Data
- Critical personal data (yet to be defined).

Step 04

Create an implementation roadmap. How to prepare?

1. Identify your role and applicability of the regulation
2. Develop policies, procedures and enterprise level frameworks
3. Incorporate privacy as a design in processes and applications
4. Implement security safe guards by improving technical and organisational measures
5. Conduct training and awareness sessions
6. Provide a privacy notice to consumers
7. Establish a process to adhere to Data Principal Rights
8. Maintain an updated and accurate inventory of records
9. Conduct data protection impact assessments (DPIA)
10. Monitor cross border data flow in relation to sensitive and critical personal data
11. Implement processes surrounding data breach management
12. Establish a mechanism for managing consumer grievances
13. Appoint a Data Protection Officer (DPO)
14. Identify retention timelines and establish a mechanism to dispose data that is not necessary for the purpose of processing

KPMG in India contacts:

Akhilesh Tuteja
Partner and Head
Risk Consulting
Co-Leader - Global Cyber Security
T: +91 124 336 9400
E: atuteja@kpmg.com

Atul Gupta
Partner and Head
IT Advisory - Risk Consulting
India Cyber Security Lead
T: +91 124 307 4134
E: atulgupta@kpmg.com

Mayuran Palanisamy
Director
IT Advisory - Risk Consulting
Data Privacy Lead
T: +91 44 39145218
E: mpalanisamy@kpmg.com

#KPMG josh

Follow us on:
home.kpmg/in/socialmedia