KHAITAN &CO
Advocates since 1911

NEWSFLASH

ERGO
Analysing developments impacting business

COMING SOON: A NEW DATA PROTECTION LEGISLATION

16 December 2019

After a gap of over 15 months, the final draft of the Personal Data Protection Bill, 2019 (Bill) has finally been tabled before the lower house of Parliament. The Bill, which is a culmination of process over more than two-years, seeks to significantly transform the existing legal and regulatory landscape relating to data protection in India.

Broadly speaking, the Bill is heavily inspired from the European Union's General Data Protection Regulation (GDPR) in many ways and introduces aspects that are absent from the present framework. These unprecedented concepts aim to bolster data protection reform in India, which is not only a bare necessity in this age of data, but also desirable because nearly every major country in the world has a comprehensive data protection legislation.

While many of the Bill's provisions remain unchanged from the draft Personal Data Protection Bill, 2018 (Draft Bill), which was released in July 2018 by the committee of experts headed by Justice B.N. Srikrishna (Retd.), there are some notable departures between the two drafts. This ERGO aims to highlight the key differences between the Draft Bill and Bill.

Widening the definition of '*personal data*'

The definition of '*personal data*' under the Bill now encompasses both online or offline forms of characteristics, traits, attributes or any other feature of the identity of a natural person. Notably, the definition also includes '*any inference drawn from such data for the purpose of profiling,*' which is likely to widen the ambit of '*personal data*' significantly.

Modifying the definition of 'sensitive personal data'

The Bill has kept the definition of '*sensitive personal data*' from the Draft Bill intact, except that "*password*" has been removed from it. This is a welcome step as "*password*" also figures in the definition of '*sensitive personal data and information*' under the present framework and has been a bone of contention amongst several corporates, who are then required to comply with the present requirements merely because they collect passwords for *inter alia* authentication and verification purposes.

Expanding the grounds for 'reasonable purposes of processing'

To provide some context, the Bill provides certain grounds for processing of '*personal data*' without the consent of the data principal (i.e. the person to whom the '*personal*

data' relates). Under the Draft Bill, these grounds included grounds such as prevention and detection of any unlawful activity and detection of fraud, whistle blowing, credit scoring and processing of publicly available personal data. Under the Bill, another ground – '*operation of search engines*' has been added to the list. This is also a much desirable change as it is not possible for search engines to rely on consent for processing personal data.

Empowering data principals with additional rights

Data principals have been granted an additional right under the Bill, in comparison to the Draft Bill. Now, data principals can also seek a '*right to erasure*' in addition to '*right to be forgotten,*' which was postulated under the Draft Bill. Resultantly, data principals may now be able to seek erasure or deletion of '*personal data*' which is no longer necessary for the purpose it was processed. The addition of this element brings the Bill at par with provisions of GDPR. However, it may pose a challenge for many data fiduciaries (i.e. the entity that determines the purpose of processing '*personal data*'), as erasing data from all records may not be possible without investing in technology increasing the cost of compliances. Also, vesting of this right to the data principals may not add much significance considering the Bill already provides for the 'right to be forgotten' and data minimisation principles.

Different connotation of 'data localisation' requirement

With respect to personal data, the requirement of storing a serving copy of all personal data on a server in India has been done away with in entirety in the Bill.

'Sensitive personal data' can be transferred outside India, subject to explicit consent of the information provider and fulfilment of certain additional conditions such as intra group schemes approved by the Data Protection Authority of India (Authority), permission from the Central Government; etc.

Critical data (definition yet to be provided) can only be processed in India (as was the case under the Draft Bill) and can be transferred outside India only where the transferee is engaged in the provision of health service or emergency services or where the Central Government has deemed such transfer to be permissible or is of the opinion that the transfer does not prejudicially affect the security and strategic interest of the country.

Reducing grounds for imprisonment

Another heavily criticised aspect under the Draft Bill was the stringent penalty scheme prescribing imprisonment for data fiduciaries who infringe the provisions relating to obtaining, transferring, or selling '*personal data*' and '*sensitive personal data*' and in case of re-identification and processing of de-identified '*personal data*'. Under the Bill, imprisonment for the offence of re-identifying and processing de-identified '*personal data*' only has been prescribed.

Revised composition of Selection Committee

The composition of the Selection Committee for recommending appointment of the Authority has been significantly altered under the Bill. In the Draft Bill, the Selection Committee was to comprise of the Chief Justice of India or a Supreme Court judge as the chairperson of the committee, the Cabinet Secretary, and an expert nominated by the Chief Justice or Supreme Court judge. According to the Bill, the Selection Committee will have the Cabinet Secretary as the chairperson, and the Secretaries to the Government in the Ministry/Departments dealing with legal affairs, and electronics and IT, as other members.

Notable additions

The Bill makes some notable additions, which earlier did not form part of the Draft Bill. Some of the important new additions have been discussed below:

- Social media intermediaries

  The Bill introduces an altogether new category of data fiduciaries and data processors, namely '*social media intermediaries*' (SMI). SMI is an "*intermediary who primarily or solely enables online interaction between two or more users and allows them to create, upload, share, disseminate, modify or access information using its services*". If SMIs fulfil certain criteria and threshold of users (yet to be spelt out) then according to the Bill, such SMIs would be classified as '*significant data fiduciaries*'. Consequently, such SMIs would be subject to an additional layer of obligations such as carrying out Data Protection Impact Assessments, record keeping, appointing Data Protection Officer, and undertaking annual audits. Importantly, the Bill also requires certain SMIs to incorporate voluntary identification methods for their users, which seems cumbersome and rather misplaced in the present context. It will also increase the cost of compliance for such SMIs.

- Certification of '*privacy by design*' policy

  According to the Bill, '*privacy by design*' policies prepared by the data fiduciary are required to meet the prescribed criteria and then may be submitted to the Authority for certification. Such entities whose policy is certified may get exemption to apply for inclusion in sandbox (described below). This added step of certification may prove to be cumbersome for most entities and the Authority as well.

- Creation of Sandbox

  With a view to foster innovation in artificial intelligence, machine-learning or any other emerging technology, the Authority is entitled to create a '*sandbox*'. This is likely to provide a fillip to start-ups that are functioning in such domain and develop more advanced solutions.

- Exemption of government agencies

  The Bill empowers the Central Government to exempt, by an order in writing, any government agency from the application of all or any provisions of the Bill with respect to processing '*personal data*' on grounds such as public order, prevention and incitement to the commission of any cognisable offence relating to the sovereignty and integrity of India, security of state. This provision has been heavily criticised by various stakeholders, as it has widened the powers of Central Government. Under the Draft Bill, such exemptions were only available to the Central Government pursuant to a law passed by the Parliament.

- Anonymised data

  The Bill also empowers the Central Government, in consultation with the Authority, to direct any data fiduciary or data processor to provide anonymised 'personal data', or other non-personal data to enable better targeting of delivery of services or formulation of evidence-based policies by the Central Government. While such data is anonymised and non-personal in nature, it must be appreciated that entities spend significant amounts in research, development and creation of such data. Permitting the Government to seek such data is not only unfair to such entities, it also raises questions as to how

such data will be used by the Government. Further such a provision is misplaced in a legislation aimed to protect personal data.

Comment

The modifications carried out in the Bill are, as noted above, both laudable and concerning at the same time. For instance, while some provisions of the Bill are intended to incentivise research and development, other provisions empower the Central Government to seek anonymized data or other non-personal data from both data fiduciaries and data processors. Further, while the rights of the data principal have been strengthened, the Central Government is entitled to grant a blanket exemption to certain agencies. As such, the Bill presents several dichotomies, which will need to be ironed out before the Bill is enacted as law. This is certainly a very promising development in relation to the data protection framework of India and we hope that robust assessment will be carried out by the Joint Select Committee (which is presently assessing the Bill) in order to weed out shortcomings that exist in the Bill today.

- *Data Privacy Group at Khaitan & Co.*

For any queries please contact: editors@khaitanco.com

We have updated our Privacy Policy, which provides details of how we process your personal data and apply security measures. We will continue to communicate with you based on the information available with us. You may choose to unsubscribe from our communications at any time by clicking here.

For private circulation only

The contents of this email are for informational purposes only and for the reader's personal non-commercial use. The views expressed are not the professional views of Khaitan & Co and do not constitute legal advice. The contents are intended, but not guaranteed, to be correct, complete, or up to date. Khaitan & Co disclaims all liability to any person for any loss or damage caused by errors or omissions, whether arising from negligence, accident or any other cause.

© 2019 Khaitan & Co. All rights reserved.

Mumbai
One Indiabulls Centre, 13th Floor
Tower 1 841, Senapati Bapat Marg
Mumbai 400 013, India

T: +91 22 6636 5000
E: mumbai@khaitanco.com

New Delhi
Ashoka Estate, 12th Floor
24 Barakhamba Road
New Delhi 110 001, India

T: +91 11 4151 5454
E: delhi@khaitanco.com

Bengaluru
Simal, 2nd Floor
7/1, Ulsoor Road
Bengaluru 560 042, India

T: +91 80 4339 7000
E: bengaluru@khaitanco.com

Kolkata
Emerald House
1 B Old Post Office Street
Kolkata 700 001, India

T: +91 33 2248 7000
E: kolkata@khaitanco.com