KHAITAN &CO ADVOCATES SINCE 1911

Key recommendations of the Joint Parliamentary Committee on the Personal Data Protection Bill, 2019: Inching closer to the new data protection law

01 Timeline for implementation

The Joint Parliamentary Committee (JPC) has recommended that specific but reasonable timelines (post consultation with stakeholders) should be provided to enable the data fiduciaries (akin to data controllers under the General Data Protection Regulation 2016/679 (GDPR)) and data processors sufficient time for transitioning. At present, the key recommended timelines include commencement of registration of data fiduciaries within 9 months and all provisions of the 'Data Protection Bill, 2021' (2021 Bill) to be implemented within 24 months from its notification. While the staggered implementation approach may afford time for entities to lay out a strategy and take measures towards compliance, one major aspect of timely implementation will also be dependent on the constitution and proactiveness of the Data Protection Authority of India (DPA). In this regard, the JPC has recommended that the DPA start its activities within 6 months of the 2021 Bill becoming law.

02 Common framework for the regulation of personal and non-personal data

Further to the government's proposal of a governance framework to regulate 'non-personal data', the JPC has recommended the inclusion of non-personal data within the purview of the 2021 Bill. This, according to the JPC, was pertinent to effectively protect privacy, considering the impossibility to differentiate between personal data and non-personal data in certain cases. The JPC has also proposed the administration and regulation of all data (including non-personal data) by a single body, namely the DPA. A separate regulation on non-personal data may also be expected, following the enactment of the 2021 Bill. With the drastic expansion of the scope of data covered under this forthcoming law, it will be interesting to see how the regulation of 'non-personal data' plays out through the lens of data protection and privacy, bearing in mind the distinct nature of the two kinds of data sets.

03 Data localisation

A prominent recommendation of the JPC is with respect to sensitive data and critical data stored abroad. The JPC has proposed that the Central Government should take concrete steps for a mirror copy of all such data available with foreign entities, to be mandatorily brought to India in a time bound manner. Further, the JPC has recommended that the Central Government, in consultation with sectoral regulators, develop a comprehensive policy on data localisation. Although, this may provide predictability with respect to localisation obligations, given that it appears that one of the primary reasons of the JPC for such a policy is economic, an analysis of the compliance burden should also be taken into consideration while preparing such a policy.

04 Transfer of sensitive and critical data

With respect to the transfer of sensitive personal data, which was permitted, inter alia, through contract or an intra-group scheme approved by the DPA, the JPC has recommended that the DPA should ensure consultation with the Central Government for according such approval. Further, the JPC has recommended that the data transfer may still not be approved if such contract or intra-group scheme is against public policy. Further, provisions in relation to adequacy decisions (regarding data transfer to approved countries) have been amended to ensure that onward transfer of sensitive personal data to any foreign government / agency should require the prior approval of the Central Government, in order to protect against mala fide actions by a foreign country. While most of the recommendations of the JPC take into account practical concerns and seek to protect individuals, the requirement of the DPA to consult the Central Government should not become a time-consuming affair and one which may be reconsidered given that the DPA is envisaged to be well suited to deal with such aspects.

05 Amplifying regulation for digital media

With a view to regulate the digital media sphere (and in particular the class of 'social media intermediaries'), the JPC recommends that certain aspects, such as collection and hosting of data by social media intermediaries / platforms and processing of personal data for journalistic purposes should be regulated more actively. The JPC has proposed that a statutory media regulatory authority (akin to the Press Council of India) should be set up for, inter alia, regulation of content on different media platforms and safeguarding privacy rights of individuals in press and journalism. The JPC also recommends that social media platforms must set up an office in India and certain social media platforms (depending on their role) may be classified as 'publishers' and be held accountable for the content they host. It will be interesting to see how this culminates and harmonises with, firstly, the safe-harbour provisions under the information technology laws, and secondly, the rules issued for intermediaries and digital media platforms earlier this year especially because the said rules already set out a framework for social media platforms (through due diligence obligations for intermediaries) and digital media platforms / publishers (through a 'code of ethics', three-tier grievance redressal and oversight mechanism).

06 New mechanism for certification of digital and IoT devices

With prolific growth of emerging technologies, such as internet of things (IoT) and artificial intelligence, among others, the potential risk of breach of privacy is inevitable. In the absence of specific provisions under the earlier draft of Personal Data Protection Bill, 2019 (2019 Bill) to regulate hardware manufacturers that collect data through digital and IoT devices, the JPC has recommended framing of separate regulations for hardware manufacturers and related entities and an official body for monitoring, testing and certification of hardware and software in computing devices. Interestingly, there already exists prescribed 'Mandatory Testing & Certification of Telecommunication Equipment' (MTCTE) procedures notified under the Indian Telegraph (Amendment) Rules, 2017 for telecom equipment, including IoT and machine to machine (M2M) devices. It will be worthwhile to see how the existing and proposed mandatory testing and certification mechanisms (which include testing of security parameters) will be integrated to address potential data security concerns arising out of the manufacture of new digital devices.

07 Crystallising norms for reporting of data breaches

Deliberating on the forms and procedures of reporting data breaches, the JPC has suggested specific amendments to the 2019 Bill on reporting of data breaches. Notably, taking a leaf of the GDPR's book, the JPC has recommended a fixed time period (i.e. 72 hours) for reporting data breaches to the DPA. Further, in light of the potential challenges that may arise out of requiring data fiduciaries to report all breaches to the data principal (i.e. data subject), the DPA has been recommended to give such direction only after assessing the breach as well as the severity of harm resulting from such breach. The DPA may also direct the data fiduciary to adopt urgent measures to remedy such breach or mitigate any harm caused to the data principal. With respect to breaches involving non-personal data, the DPA has been authorised to take necessary steps, as may be prescribed. While the proposed recommendations certainly add clarity to the norms on data breach reporting, several other aspects seem to be deferred to the regulations. Considering the significance of this obligation and for the benefit of all entities, it is crucial that these regulations iron out all ambiguities pertaining to reporting of data breaches.

08 Processing of children's data

The JPC has provided some noteworthy recommendations for entities processing children's data. The key obligations, inter alia, are: (i) registration with the DPA for entities dealing exclusively with children's data; and (ii) fresh consent to be obtained 3 months before the child attains the age of majority (18 years). The provision of services to the individual should not cease unless and until the individual opts out or gives fresh consent. Interestingly, as part of another recommendation, 'the processing of data relating to children or provision of services to them' has been added as a qualifying factor for determination of a data fiduciary as a significant data fiduciary (SDF), which will attract additional compliance obligations. This will have a major impact for sectors dealing with data of minors such as ed-tech platforms, which have seen a tremendous boost during the COVID-19 pandemic.

09 Data processing by employers

The JPC has observed that employers should not be given complete freedom to process personal data of the employee without their consent for employment purposes and the employee should have the opportunity to ensure that the personal data is not being processed for unreasonable purposes. Considering the relationship between an employer and employee where an employer has an advantageous position, the JPC has recommended that the processing may happen if such processing is necessary or can reasonably be expected by the employee. The avenue for enabling processing of personal data for employment purposes had been incorporated in the 2019 Bill to provide operational flexibility and the move of the JPC to ensure that this does not however result in unfair processing of personal data is a welcome one, given the overall intent of the proposed legislation.

10 Retention of data

The JPC has provided a recommendation in relation to the provision relating to data retention under the 2021 Bill. In the 2019 Bill, the data was required to be deleted after processing. In this regard, the JPC has recognised that such a requirement is detrimental for entities which process personal data numerous times for welfare purposes. Accordingly, it has been proposed by the JPC that the personal data is required to be deleted only when the purpose of processing the personal data has been satisfied and the same is not required to be retained for such purpose. This will undoubtedly provide much needed clarity for digital businesses and also reduce their compliance burden.

11 Exploring the role of data protection officer

For certain categories of 'data fiduciaries' regarded as SDF, the 2019 Bill envisions that SDFs must appoint a 'Data Protection Officer' (DPO) based in India for, inter alia, monitoring personal data processing activities, providing advice to the data fiduciary in respect of the obligations and requirements under the said framework, acting as the point of contact for data principals for grievance redressal, among others. In this regard, the JPC has suggested that there should be further clarity regarding the qualification / position of the DPO. It recommends that as the DPO plays a 'vital role', such officer should be holding a key position in the management of the SDF (for instance, senior level officer in a State or a key managerial personnel in relation to a company) and must have adequate technical knowledge in the field. This will be a crucial clarification for foreign entities who may fall within the category of SDFs and will be required to appoint a DPO based in India. The JPC has also not specifically commented on the requirement for the DPO to be based out of India, hence it appears that the position remains unchanged in this regard.

12 Flexible penalties with upper limit

Citing the evolving nature of digital technology, the JPC propounds that penalties prescribed under the 2019 Bill should be subject to a maximum cap (instead of a fixed penalty) and the quantum to be imposed should be decided taking into account factors such as the size and nature of the data fiduciary (if it's a start-up or primarily engaged in research and innovation activities, among others). In case this is implemented in the final version of the 2021 Bill, it would be important that some guiding principles are provided in this regard, in the interest of overall transparency and to avoid any arbitrariness.

Next steps

The Report (along with the 2021 Bill) submitted by the JPC in the Parliament will now be deliberated upon. Further clarity on the timeline and content of the new law should emerge in due course.

- Data Privacy Team

For all queries on the subject please contact us at: editors@khaitanco.com