August 2018

ALMT Legal
ADVOCATES AND SOLICITORS

9 August, 2018

PERSONAL DATA PROTECTION BILL HIGHLIGHTS

In this fast-paced digital age, where technology forms a part of our daily lives, the need to relook at how personal data is protected in a constantly changing digital environment has emerged as an imperative requirement. In the recent years, various leaks of data such as the Facebook data leak case, Yahoo data leak case, JP Morgan data leak case have raised the awareness of individuals and governments towards the changes required in current data protection regimes for more effective protection of personal data. This has resulted in various countries formulating new policies with respect to data protection, be it the European Union with its much talked about European Union - General Data Protection Regulation (EU-GDPR) effective from 25th May, 2018 or India setting up a committee under the chairmanship of Justice B.N. Srikrishna for recommendations on protection of privacy ("**Srikrishna Committee**").

Although, India currently has data privacy regulations, which were introduced in 2011, and which were promulgated as the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (**"Rules**") under the Information Technology Act, 2000, certain short comings have become evident over the years, including problems relating to implementation.

As a result of the above, the Srikrishna Committee was set up, which has now drafted and published the Personal Data Protection Bill, 2018 ("**Bill**") and a report called "A Free and Fair Digital Economy Protection Privacy, Empowering Indians" which seeks to explain the basis on which the Bill has been drafted. The Bill and report were made public on 27th July, 2018.

While the Srikrishna Committee was in the process of the final stages of drafting the Bill and the report, the Telecom Regulatory Authority of India ("**TRAI**") published recommendations on privacy, security and ownership of data in telecom sector on 16th July, 2018. This created a lot of confusion amongst the public, since it was unclear whether the TRAI had the authority to draft and publish these recommendations, especially in view of the work being done by the Srikrishna Committee. It was clarified by TRAI that the recommendations were no more than just recommendations and were

focused only on the telecom sector. Some key recommendations of TRAI were: (a) restraining entities in digital ecosystem to use metadata to identify individuals; (b) all entities, controlling or processing this data should be bought within the framework; (c) consent, data portability, right to be forgotten should be introduced; (d) encryption of personal data of telecommunication consumers should be undertaken during processing and storage; and (e) a common platform should be created for sharing of information relating to data security breaches by all entities in the digital ecosystem including telecom service providers.

The Bill is now subject to review and is likely to be amended prior to implementation. The Bill once promulgated into law is likely to have a sweeping impact across sectors on both individuals and businesses. Businesses will need to get geared to make changes in how they deal with data whether it relates to their service providers, customers, employees or third parties, etc.

In view of the above, the main highlights of the Bill have been discussed below.

HIGHLIGHTS OF THE BILL

- The Bill uses the term 'data fiduciaries' (data collecting entity) which now include the States and juristic entities and 'data principal' (natural person providing the data), to set out the two key players under data protection laws.

- The Bill introduces various obligations on the data fiduciary for collection and processing of data including a list of information to be provided by them to the data principal during collection of data such as purpose of collection of data, the source of collection, the procedure for grievance redressal, etc. The Bill also lays down provisions for maintenance of data quality such as uploading or correcting incorrect data and also limits data storage.

- The Bill, similar to the Rules, distinguishes between sensitive personal data and personal data. However, sensitive personal data now includes a much wider list of data within its definition. One of the important items covered under sensitive personal data is the Aadhaar number. This appears to be included since there was a huge outcry regarding the use of the Aadhaar number and the government's capability of protection of the data collected and linked to the same.

- The processing of 'personal data' and 'sensitive personal data' is also distinguished under the Bill with consent being a major component. Personal data requires consent of the data principal, but sensitive personal data requires the *explicit* consent of the data principal. While mere consent may be a generic consent wherein the data principal agrees to provide rights to data fiduciary for collection, processing and storing of data, under an explicit consent, the data principal is specifically required to consent to the entire process such as the purpose of collection of data and uses of different categories of sensitive data collected. On a reading of the Srikirshna Committee report with the Bill, one may note that there is substantial emphasis on the importance of consent and therefore data fiduciaries may chose to be more cautious and obtain explicit consent irrespective of whether data collected is personal data or sensitive personal data.

- The Bill also sets out various grounds regarding when, 'personal data' and 'sensitive personal data' may be processed in relation to purpose for processing the data, such as, processing data (a) as a function of State; (b) when required by law or any order of court or tribunal; (c) where prompt action is required; (d) in the case of employment; and (e) for reasonable purposes as may be specified.

- The Bill envisages a higher degree of care while processing of personal data and sensitive personal data for children. There may be certain practical difficulties in implementing this since while the Bill provides for taking parental or guardians' consent for processing of data it may be difficult to verify the authenticity of the same on online platforms.

- While the erstwhile Rules did not include any specific rights available to data principals, under the Bill the following rights are made available to data principals: (i) to ask for the status of processing of data, access to the data or a summary of the data processed; (ii) to correct anything that is incorrect, update or complete any data provided; (iii) to retrieve the data and transfer it to another data fiduciary; ; and (iv) the right to be forgotten i.e. to restrict or prevent disclosure of data once the purpose has been served or consent has be withdrawn or disclosure is made contrary to any law.

- The Bill aims at achieving the highest standards of data protection by including transparency in general practices for processing of data; security safeguard measures such as de-identification or encryption; procedure to be undertaken during a personal data breach; record keeping of the processing cycle; data audits procedures; data protection impact assessment and grievance redressal mechanism.

- The Bill provides for appointment of a data protection officer by the data fiduciary. The data protection officer is required to undertake functions such as monitoring of processing activities, providing advice to data fiduciaries, being a point of contact for grievances and providing assistance to the authorities.

- The Bill distinguishes between significant data fiduciaries, data fiduciaries and entities other than data fiduciaries based on volume of data processed, sensitivity of the data, turnover of the data fiduciary, use of technologies, risk of harm, etc. The penalties for significant data fiduciaries are higher in comparison to other data fiduciaries, however, the basis of classification for identifying a significant data fiduciary appears to be wide enough to allow the authority under the Bill to exercise substantial discretion as to who should be classified under this category.

  Further, the Bill provides for restrictions and conditions on cross-border transfer of personal data. A key restriction is the requirement of storing at least one copy of personal data on a server located in India. Further the Central Government may notify categories of personal data as critical personal data that shall only be processed in a server or data centre located in India.

- The Bill carves out certain exemptions available wherein the proposed provisions may not be applicable such as for (i) security of the state following the procedure established by Parliament; (ii) prevention, detection, investigation and prosecution of contravention of law as authorised under the law; (iii) processing of data for legal proceedings; (iv) research, archiving data or collection of data for statistical purposes; (v) data process by persons for personal or domestic use; (vi) data processing for journalism; or (vii) manual processing of data by smaller entities. While the above exceptions may have been made to the general provisions incorporated herein, the entities collecting data for the above are not exempted from fair and reasonable processing and security safeguard provisions. The aforesaid exemptions however give flexibility to organisations or authorities to process and collect data as may be required under the law without following the tedious compliances of the Bill.

- The Bill also envisages the setting up of a data protection authority in India for purposes of monitoring and inquiring into the activities of a data fiduciary with respect to processing of data. The Bill gives wide powers to this authority therefore allowing it to operate without much intervention and promptly tackle issues that crop up with respect to data protection and breaches. The data protection authority also has the power to call for information, conduct inspections, etc. and for undertaking the same is vested with powers similar to that of civil court such as power to summon or enforce attendance of a person, issue commissions, inspect books, etc. and accordingly the authority has the power to issue directions to data fiduciaries or data processors. The Bill also provides for appointment of adjudicating officers to impose penalties, with any appeals to the orders of the adjudicating officers to be referred to an appellate tribunal to be set up under the Bill.

- As opposed to the blanket penalty of imprisonment for a term not exceeding three years, or with a fine not exceeding up to five hundred thousand rupees, or with both, under the Rules, the Bill provides for differential penalties for various non-compliances and breaches depending upon the grievousness of the offence which penalties are substantially higher than those provided in the Rules. Some penalties specified are (i) contravention by data fiduciary while processing may attract a penalty of one hundred and fifty million rupees or 4% of its total worldwide turnover in the preceding financial year, whichever is higher; and (ii) failure to furnish reports, etc. may attract a penalty of ten thousand rupees per day till such default continues to a maximum of two million for significant data fiduciaries and five hundred thousand rupees for other entities The Bill also provides for a punishment of imprisonment or fine or both in cases of obtaining or transferring or selling of data contrary to the provisions of the Bill. The Bill also provides for a mechanism of claiming of compensation by the data principal.

A lot of debate and discussions around data protection laws in India have already ensued in the light of the above Bill. India being a developing country and many data fiduciaries being private owned companies, it would be interesting to see how the government and these companies invest in manpower, technologies, process implementation etc for carrying out their obligations under this Bill.