Namrata Bhagwatula Senior Associate
namrata@gamechangerlaw.com

Srikanth Bhaskar Associate
srikanth@gamechangerlaw.com

GameChanger Law Advisors, New Delhi

India fastens its seatbelt on the data protection band wagon

The Supreme Court of India passed, on 24 August 2017, a landmark judgment in the case of *Justice K. S. Puttaswamy (Retd.) & Anr. v. Union of India & Ors*.[1] where it upheld that every citizen of India has a fundamental right to privacy. The right to privacy judgment, along with the changing global tone on data protection set the ball rolling for India to jump on to the data protection band wagon. For this purpose, the Supreme Court of India, during the proceedings of the right to privacy case, directed the Central Government to frame a comprehensive policy to regulate privacy in India. Namrata Bhagwatula and Srikanth Bhaskar, Senior Associate and Associate respectively at GameChanger Law Advisors, provide an analysis of the features of the Personal Data Protection Bill 2018 ('the Bill') which seeks to form India's data protection regime.

The requirement of data localisation is against the ideals of a liberal economy and may act as a trade barrier for many companies intending to engage in business in India.

The path forged by the B. N. Srikrishna Committee- the salient features of the Bill

The Government set up a nine member expert committee in July 2017, led by Justice B.N Srikrishna to study issues relating to data protection in India ('the Committee'). The White Paper of the Committee of Experts on a Data Protection Framework for India ('the White Paper')[2] was issued in November, 2017. The White Paper called for responses and suggestions from the public and the stakeholders. Thereafter, the Committee submitted, on 27 July 2018, its report with the draft legislation to the Indian Ministry of Electronics and Information Technology ('the Report')[3]. The draft legislation in the Report was the Bill[4].

The Bill proposes the establishment of a data protection regime which will cover within its scope both the state as well as non-state actors. Some of the salient features of the Bill are as follows:

Applicability

The Bill applies to:

- any data that has been collected, disclosed, shared or otherwise processed within India;
- any data processed by either the State, an Indian citizen or any entity incorporated in India; and
- any data processed by data fiduciaries or data processors outside India, in connection with any business carried out in India or any activity which involves profiling of data principles within India. Further, the Bill excludes from its applicability, all anonymised data.

Data principal and personal data

The Bill defines personal data as any data that may be used to directly or indirectly identify an individual. The Bill further defines a data principal as the natural person to whom such personal data relates. The Bill also creates a distinction between personal data and sensitive personal data, with the later having been defined to include financial, medical, and other sensitive data such as the individual's caste, religion, sexual orientation, biometric data etc. The Bill also empowers the Data Protection Authority ('DPA') to prescribe any additional categories of data that is to be treated as sensitive personal data. The distinction between personal data and sensitive personal data becomes relevant as the grounds for 'lawful processing' of personal data and sensitive data are different. Personal data can be processed on the following grounds:

- consent of the data principal;
- for functions of the State;
- in compliance with law or order of any Indian court or tribunal;
- necessitated by the requirement of prompt action such as medical emergency, safety etc.;
- required for recruitment or employment related function;
- other reasonable purposes such as prevention of unlawful activity, fraud, mergers and acquisitions, whistleblowing and other such purposes prescribed by the DPA.

However, the grounds of lawful processing of sensitive personal data are only limited to the first four grounds in the paragraph above.

Data fiduciary

The Bill defines data fiduciary as such persons, including the State, any entity or any individual who determine the purpose and means of processing of personal data. The Report suggests that the concept of data fiduciary was added to the Bill as the Committee believes that as opposed to the treatment of personal data as property, the relation between the individual and entities with whom the individual shares her personal data is one that is based on a fundamental expectation of trust.

As the data fiduciary is the primary data controller, all the primary obligations and liabilities with respect to the protection of the personal data of the data principal. Such duties include:

- duty to collect and process personal data in a manner that respects the privacy of the data principal;
- duty to collect and process personal data for only those purposes that are clear and specific;
- duty to collect only such data as is necessary for the purpose of processing;
- duty to provide a notice to the data principal in a clear, concise manner as to what data is being collected and for what reasons such data will be used;
- duty to take all precautions and steps in order ensure that the data stored is accurate, complete and not misleading; and
- duty to store data for only such period of time as is necessary to satisfy the purpose for which the data is processed, unless otherwise mandated by law.

The Bill also creates a duty on the data fiduciary to appoint a data protection officer to advise the data fiduciary on all matters relating to data protection and monitoring the processing of personal data by the data fiduciary. The data fiduciary is also required to maintain proper procedures and effective mechanisms to address grievances of data principals efficiently and in a speedy manner. Needless to say, the above obligations add a far greater degree of regulation on the data fiduciary and will ultimately increase the cost of doing business for all data fiduciaries.

It is however, interesting to note that the Bill relaxes some of the above duties for data fiduciaries which are small entities which process data through means other than automated means as long as:

- they have annual turnover less than INR 20,00,000 (approx. € 23,491);
- they do not collect personal data to be disclosed to any other third party; and
- they have not processed personal data of more than 100 data principals in one day in the preceding 12 months.

Rights of the data principal

The Bill tries to achieve a balance between the rights of the data principals and empowering the state to access and process personal data in certain specific situations.

continued

The Bill lists the following bouquet of rights that the data principal has with respect to her personal data collected by a data fiduciary, upon making a request in writing to the data fiduciary with respect to such data and upon paying such fees as prescribed by the data fiduciary:

- right to confirmation of and access to the personal data collected and processed by the data fiduciary;
- right to correct or update any inaccurate, incomplete, misleading or outdated personal data collected or processed by the data fiduciary;
- right to data portability; and
- right to be forgotten;

Data processor

The Bill defines data processor as any person, being the State, an entity or an individual who processes data on behalf of the data fiduciary. While all the primary obligations and the penalties for such obligations lie on the data fiduciary, the data processor also has certain obligations under the Bill. Further, the Bill also necessitates the existence of a valid contract between the data fiduciary permitting the data processor to process data on behalf of the data fiduciary. Unless authorised in the contract or explicitly permitted by the data fiduciary to do so, the data processor does not have the right to engage, appoint or use other data processors for processing personal data on behalf of the data fiduciary. The data processor also has the obligation to process data only in accordance with the instructions of the data fiduciary.

Data localisation

The Bill imposes a duty on data fiduciaries to store at least one copy of personal data on a server or data centre in India. The Bill also empowers the Central Government to notify categories of personal data which shall be referred to as critical personal data. Such data which is notified as critical data by the Central Government may only be processed in India. Any cross-border transfer or personal data or sensitive data is only permitted on certain limited grounds provided in the Bill.

The data localisation requirement proposed by the Committee has been highly criticised for being regressive and impractical. The requirement of data localisation is against the ideals of a liberal economy and may act as a trade barrier for many companies intending to engage in business in India. Further, the Bill further does not provide for a time period within which the entities will need to move their information onto local servers. Such a provision is expected to add massive costs to small businesses intending to do business in India.

The Data Protection Authority of India

The Bill envisages the creation of a separate regulator in order to regulate the implementation of the Bill. The DPA shall be a statutory body created under the Bill which will have the following powers and functions:

- to protect the interests of data principals, prevent any misuse of personal data, ensure compliance with the provisions of the Bill and to promote awareness of data protection.
- create public awareness about data privacy;
- monitor and enforce the provisions of the Bill; and
- take prompt action in the event of data breach etc.

The Bill also makes the DPA an adjudicator for all disputes that arises out of the Bill.

Data fiduciaries - the biggest losers of the balancing act performed by the Committee

The Bill tries to achieve a balance between the rights of the data principals and empowering the state to access and process personal data in certain specific situations. We believe that the biggest loser in this balancing act is the data fiduciary. The multiple obligations imposed on data fiduciaries would not only be operationally challenging for companies but will also add enormously to operational costs.

While the application of the Bill extends to data fiduciaries which are incorporated outside India but are providing services to and collecting personal data from data principals in India, the mechanism for enforcement of the Bill on such data fiduciaries is unclear. Further, the requirement of maintenance of store at least one copy of personal data on a server or data centre in India will particularly be an operational challenge to such data fiduciaries. The Bill, while seemingly adopting the extra-territoriality principal from the European Union General Data Protection Regulations, appears to have ignored the practical challenges relating to operation as well as enforcement of such provisions. However, as of the date of this article, the Bill is just a proposed legislation. Whether the Parliament adopts the Bill, and if yes, to what extent, is yet to be seen.

1. https://www.sci.gov.in/supremecourt/2012/35071/35071_2012_Judgement_24-Aug-2017.pdf
2. http://meity.gov.in/writereaddata/files/white_paper_on_data_protection_in_india_171127_final_v2.pdf
3. http://meity.gov.in/writereaddata/files/Data_Protection_Committee_Report-comp.pdf
4. http://meity.gov.in/writereaddata/files/Personal_Data_Protection_Bill%2C2018_0.pdf