PRUDENT
THE FUTURE OF INSURANCE

KHAITAN LEGAL ASSOCIATES
INDIAN ADVOCATES

DATA PROTECTION BILL 2019

AN OVERVIEW

DATA PROTECTION BILL 2019

Data Privacy, Data Security and Data Sovereignty have been some of the most keenly debated subjects globally over the last decade. While the General Data Protection Regulation (GDPR) ushered in a new regulatory regime in the European Union, Indian lawmakers were developing the Indian regulatory architecture on data protection. After an elaborate and exhaustive pre-legislation exercise of over a year involving consultations and deliberations with stakeholders, the Government finally moved the Personal Data Protection Bill, 2019 (Bill) in Parliament on 11th December, 2019. The Bill has been referred to a Parliamentary Standing Committee and is expected to take final shape in the Budget session of Parliament in February 2020.

Personal data breaches have emerged as one of the most critical security challenges for companies across the globe. With the recent surveillance incident on the Facebook-owned messaging platform WhatsApp - which involved the compromise of private data of many individuals via a third-party spyware - there are strong reasons for the Indian government to take significant decisions regarding matters pertaining to the protection of personal data of Indian citizens.[1]

Although the Bill is a few steps away from its final form, it provides an insight into the direction of Government's thought in this regard. It is critical that the Bill is analysed and examined as it may have a significant impact on treatment of personal data and related processes.

Overview of the Bill

The Bill has been broadly based on the framework and principles of the GDPR and derives direction from the landmark judgement of the Supreme Court of India in Justice K.S. Puttaswamy (Retd.) & Anr. vs Union of India & Ors[2] wherein the Supreme Court of India upheld the right to privacy as a fundamental right under the Constitution of India. The Bill proposes to replace the existing India data protection framework that stems from Section 43A of the Information Technology Act, 2000 (IT Act) and the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (IT Rules).[3]

While the Bill stipulates that the processing of data is allowed when an individual gives consent, the Bill also stipulates certain instances where processing of personal data without such consent may also be allowed.

These include:

(i) If required by the State to provide benefits to the individual
(ii) In case of legal proceedings
(iii) To respond to a medical emergency.

The Bill regulates the processing of personal data of individuals (Data Principals) by government and private entities (Data Fiduciaries) incorporated in India and abroad. Further, the Bill mandates setting up of a national-level Data Protection Authority to supervise and regulate the working of Data Fiduciaries.

Key Features of the Bill

Broader definition of Sensitive Personal Data (SPD): Unlike GDPR, the Bill has defined SPD to include health data, sexual orientation, gender, financial data, biometric data, caste or tribe.[4] Various multinational companies and foreign companies would need to implement a strong compliance strategy to avoid a breach of such SPD under the Bill.

Excessive Liability: The Bill imposes liability on every officer of the company who, at the time of commission of the offence, was in charge of the conduct of the business of the company. However, no person shall be liable if he proves that the offence was committed without his knowledge.

Notice: The Data Fiduciary is obligated to provide the Data Principal with adequate notice before collecting and processing their data. The notice is required to be clear and concise, and if necessary and practicable, the notice shall be in multiple languages. In a country like India with multiple languages, this may be an operational challenge and may increase the cost of compliance.[6]

Periodic Review of Stored Personal Data: The Bill specifies that Data Fiduciaries are obligated to conduct periodic review of the personal data stored with them so that it is not retained beyond the period necessary for the purpose of processing.[5] There is no time-frame defined under the Bill for such reviews to take place. Further, this is most likely to increase operational costs for Data Fiduciaries.

Employment: Under the Bill, consent of Data Principals is not required in employment related matters with respect to use of personal data. However, such data would not include sensitive personal data within its ambit.

Penalties: Any offence punishable under this Bill shall be cognizable and non-bailable. The penalties for the offences under this Bill could range between INR 5 Crores* or 2% to INR 15 Crores or 4% of the company's total worldwide turnover.

*1 Crore = 10,000,000

How is the Bill different from GDPR?

1. There is no obligation on the Data Fiduciary to share with the Data Principal how long the data will be stored while collecting or at any time, as GDPR mandates.

2. Unlike GDPR, Indian draft legislation does not require the Data Fiduciary to share the names and categories of other recipients of the personal data with the Data Principal.

3. In case of a breach, there's no requirement under the Bill to notify data breach to the Data Principal. Rather, the Data Protection Authority shall determine whether such breach should be reported to the Data Principal. Under GDPR, it is mandatory for the Data Protection Authority to share such news with the Data Principals without unnecessary delay if they are of the opinion that such a breach would be a high magnitude risk for them.

Data Breaches After GDPR

In September 2018, leading airline British Airways announced that it had suffered a data breach caused due to a malicious criminal attack and that customer data had been lost. The company released details that the theft had occurred between 21st August 2018 and 5th September 2018, and that as many as 380,000 transactions had been affected.

This was one of the first large instances of data loss since the introduction of GDPR and the regulator announced its intent to impose a hefty fine on British Airways.

The GDPR stipulates that organizations must report a data breach within 72 hours of becoming aware of it. British Airways managed to announce the data breach within a day of discovery as well as providing specific details of who had been affected, and the kind of data that could have been compromised.

Nevertheless, the company suffered a hack, and this could indicate that they had not taken adequate precautions to protect their customers' private data.

Theoretically, British Airways could be fined as much as €20 million or 4% of their global turnover – whichever is higher (and in their case, this would be the global turnover). However, in terms of a data breach, this is not a truly catastrophic data loss. Some industry figures have suggested that the fine could be somewhere between €5 million and €10 million.

Data Protection Regime and Cyber Insurance

Whenever the new data protection regime comes into force, the risk and the liability landscape for businesses will alter significantly. There will be a greater need for adequate insurance cover for protection against cyber and data breach exposure of companies, especially in light of the proposed monetary penalties and criminal sanctions.

In Asia,[7] several carriers are offering policies with coverage for insurable fines and penalties. Reputed legal counsel do not foresee any prohibitions with respect to insurability of GDPR fines and penalties across major Asian markets. Insurers offering such coverage have signalled that they would pay related claims if legally permissible. Companies, however, should, of course, seek specific legal advice on insurability of such fines and penalties within the relevant jurisdiction in Asia.

The Way Forward

With growing digitization across all industries and an ever increasing flow of personal data across national borders, lawmakers face the challenge of balancing between the privacy rights of individuals and the legitimate needs of business to use personal data. We are monitoring the Bill's progress and will update you on further developments.

Meanwhile, companies need to look into their internal processes and must take appropriate precautionary measures to prevent data breach.

Notwithstanding the technological and other interventions, a data or cyber breach is unforeseeable. Hence, it is now imperative for companies to also seek necessary support to examine the appropriate insurance covers in order to protect themselves against potential financial exposures including but not limited to fines and penalties when the new regime is operationalised.

> Cyber liability insurance protects businesses from losses or damages resulting from cyber attacks and data breaches. These expenses can include data loss and restoration, extortion, legal fees, and regulatory fines and penalties.

1 http://economictimes.indiatimes.com/articleshow/72429680.cms?utm_source=contentofinterest&utm_medium=text&utm_campaign=cppst

2 (W.P. (Civil) No. 494 of 2012)

3 http://www.mondaq.com/india/x/727550/data+protection/The+Personal+Data+Protection+Bill+2018+Key+Features+And+Implications

4 https://analyticsindiamag.com/personal-data-protection-bill-india/

5 https://www.prsindia.org/billtrack/draft-personal-data-protection-bill-2018

6 https://www.indiatoday.in/india/story/personal-data-protection-bill-1625017-2019-12-04

7 https://fitsmallbusiness.com/cyber-liability-insurance/?__cf_chl_jschl_tk__=8eb39abaacb4d52ba6b06f2dbe804e42692c0dab-1575915839-0-AVGTkFtUGwopDIn5Qn4AuTT4KyfLDq1xtDQTuyjKDyw55LCTlKXjTstCX1W3qjXYrpvdCBo3FXWJ1v-AJkGOXR__o4xT2Sw8NR7mkGkPcUqzppIg3kV7PuP4P9Ksx4X30cpe1CwHOd_rcY26zbG2CrTO9seN7_qBZMe80sZeBiQJHS5HpS-V92o0Eivjhr4oUHPGr0SByHeG2cpSFrVvYb8FSXVuE4yUrnW9TuwhcOIxzU7lEv8h961CyFpNF4BJjWQqrjcsYkgtQ5KyY5mhf0u-V-DfClv5nVQnoAIL139R

ABOUT PRUDENT

LEADING INTERNATIONAL BROKER

10 Offices

700+ Team Members

3,000+ Corporates

120+ Global Partners

550+ Multinationals

Placing premium **US$ 225M** in the Indian market

Experienced team of **320+** Benefits specialists

Organising **3,000+** Wellness activities annually

Over **200,000+** employees benefit from our wellness activities

ABOUT KHAITAN LEGAL ASSOCIATES

Khaitan Legal Associates is a full service, independent Indian law firm with offices in London, Mumbai, New Delhi and correspondent offices across different cities in India.

For further information with regards to the Bill and risk transfer, please reach out to us

For Prudent: **tanuj.gulani@prudentbrokers.com**
For Khaitan Legal Associates: **jehaan.shroff@khaitanlegal.com**

www.prudentbrokers.com