KHAITAN &CO ADVOCATES SINCE 1911

NEWSFLASH

ERGO

Analysing developments impacting business

DIGITAL PERSONAL DATA PROTECTION BILL 2022 | A SNAPSHOT OF THE MUCH-AWAITED DRAFT LAW

19 November 2022

Introduction

In early August 2022, the Ministry of Electronics and Information Technology (MeitY) withdrew the Personal Data Protection Bill 2019 (2019 Bill), which was reworked on by the Joint Parliamentary Committee (JPC), promising that they would release a more comprehensive data protection framework to take into account the recommendations of the JPC.

Pursuant to this, on 18 November 2022, MeitY released the draft Digital Personal Data Protection Bill 2022 (the Bill) for public consultation. The Bill appears to be quite lean and focused, in comparison to the earlier 2019 Bill. Granular provisions and procedural aspects are expected to be issued subsequently as part of rules and regulations under the Bill.

Key Highlights of the Bill

1. ***Legislative scope***: The Bill will apply to personal data collected from data principals (i.e., individuals to whom the personal data relates to) within India if collected through: (i) online mode; and (ii) offline mode but is then digitized. The Bill also has an extraterritorial applicability which will extend to processing of digital personal data outside India, if such processing is in connection with profiling of, or activity of offering goods or services to data principals within India. While non-personal data does not fall within the scope of the Bill, it makes no express reference to whether anonymised data is included within its scope or otherwise.

2. ***Prior notice requirement and retrospective application***: Data principals are required to be provided an itemized notice (i.e., presented as individual items) in clear and plain language that describes the personal data sought to be collected from them and the purpose of such collection. This provision will also apply retrospectively where, if data principals have provided their consent to collection of their personal data prior to commencement of the Bill, then all data fiduciaries (i.e., entities determining the purpose and means of processing of personal data) would be required to furnish a notice to such data principals setting out the description of personal data collected from them and the purpose for which such personal data has been processed, as soon as reasonably practicable.

3. ***Manner of consent***: Consent has been prescribed as one of the legal bases for collection of personal data under the Bill. Consent from data principals is required

to be taken by way of a clear affirmative action, signifying agreement to processing of their personal data for a specified purpose. Data fiduciaries are required to provide data principals the option to access the abovementioned request for consent in English or any local Indian language specified under the Eighth Schedule to the Constitution of India.

4. ***Deemed consent***: To address the requirement of providing a legal basis for processing personal data where obtaining consent is impracticable or inadvisable due to pressing concerns, the concept of 'deemed consent' has been introduced. Deemed consent may apply in certain situations such as, *inter alia,* where the data principal is expected to voluntarily provide personal data (such as for availing any services), for purposes related to employment, and for fair and reasonable purpose after taking into consideration certain prescribed factors. Pertinently, the additional grounds available under deemed consent for processing of personal data would reduce excessive data collection requests and can become an effective remedy for consent fatigue.

5. ***Obligations of data fiduciaries***: The Bill has provided for certain specific compliances and obligations that will apply to data fiduciaries. Importantly, the Bill has clarified that a data fiduciary will continue to remain responsible for complying with the provisions of the Bill for any processing undertaken by it or on its behalf by a data processor (i.e., entity that processes personal data on behalf of data fiduciaries). In this context, data fiduciaries will have to ensure adherence to compliances such as implementing appropriate security measures and grievance mechanisms.

6. ***Additional obligations for significant data fiduciaries***: Data fiduciaries that will be classified as 'significant data fiduciaries' (on the basis of factors such as volume and sensitivity of personal data collected, risk of harm to data principals, etc.) are required to comply with additional obligations such as appointment of a data protection officer ***residing in India***, appointment of an independent data auditor, undertake data protection impact assessments and ensure compliance with other measures as may be prescribed.

7. ***Additional obligations in relation to processing of children's data***: Verifiable parental consent (including consent of a guardian) is required to be obtained prior to processing personal data of children. Data fiduciaries are not permitted to undertake tracking and behavioural monitoring of children or sending targeted advertisements directed at children. Any kind of processing that may cause significant 'harm' to children (as may be prescribed) is barred. Further, in case of children, parents or lawful guardians will be deemed to be data principals for the purposes of rights and obligations set out under the Bill.

8. ***Obligations of data processors***: The Bill provides that data processors have a duty to protect personal data in their possession or control by taking reasonable security safeguards to prevent breach of personal data.

9. ***Data Protection Board of India***: The Central Government will establish a Data Protection Board of India (Board), which will be responsible for determining non-compliances under the legislation and imposing penalties. This Board will be an independent body operating digitally (to the extent possible). The Board may, either *suo moto* or on receipt of complaint, take actions as prescribed under the Bill. Every order made by the Board will be enforceable akin to a decree made by the civil court.

10. ***Personal data breach***: Personal data breach has been defined to mean any unauthorised processing of personal data or accidental disclosure, acquisition, sharing, use, alteration, destruction of or loss of access to personal data, that compromises the confidentiality, integrity or availability of personal data. In the event of a personal data breach, data fiduciaries / data processors (as the case may be) would be required to notify the Board and each affected data principal, in such form and manner as may be prescribed.

11. ***Cross-border transfer of personal data***: The Central Government may, after a comprehensive assessment, notify specific jurisdictions outside India to which personal data may be transferred in accordance with such terms and conditions as may be specified.

12. ***Enhanced financial penalties***: Significant financial penalties for non-compliances have been provided under the Bill. Penalties of up to INR 250 crores (approx. USD 30 million) may be imposed for offences such as failure of a data fiduciary / data processor to take reasonable security safeguards to prevent personal data breach. However, for a single instance, the penalty cannot exceed INR 500 crores (approx. USD 60 million).

Comments

The Bill is indeed a simpler and reader friendly version, when compared to its predecessors. However, several aspects of the Bill currently appear to be vague in the absence of specific procedural guidance. The Bill, in a significant departure from the 2019 Bill, has done away with the categorization of personal data into sensitive personal data and critical personal data. Further, one of the most commendable aspects of the Bill is that it has eased data localisation restrictions which is bound to give a thrust to India's booming start-up economy and businesses.

Notably, although the Bill has provided for strikingly high financial penalties to the tune of INR 250 crores (approx. USD 30 million) which may even extend up to INR 500 crores (approx. USD 60 million), such penalties happen to be the highest amounts that can be ordered. Further, during adjudication of any non-compliance, the Board will take into account mitigating factors, such as gravity of contravention, duration and its repetitiveness and efforts undertaken by the entities to limit damage pursuant to the contravention, etc. while determining the quantum of penalty to be imposed.

The Bill beckons a new era in the data protection space in India. It seems that the Government has made a genuine attempt to simplify the legislation. A lucid, balanced and forward-looking law will certainly aid the industry in scaling greater heights and reinforcing India's position as an economic superpower.

- *Data Privacy Group*

For any queries please contact: editors@khaitanco.com