ASIAN BUSINESS LAW INSTITUTE

8 March 2020

Smt. Meenakashi Lekhi, (New Delhi) M.P.
Chairperson
Joint Parliamentary Committee on the Personal Data Protection Bill, 2019
Via e-mail: mrs.mlekhi@sansad.nic.in

Dear Smt Lekhi,

Joint Committee on the Personal Data Protection Bill, 2019

We refer to the invitation to submit views and suggestions on the above Bill.

The Asian Business Law Institute appreciates the opportunity to comment on the Bill which is an important development in India and for the region.

Since 2017, the Asian Business Law Institute has been studying the regulation of cross-border transfers of personal data in Asia and we believe that the knowledge and experience we have acquired as a result will be of assistance to the Committee.

Below we set out a brief background to the Asian Business Law Institute and the regional work we have been undertaking in respect of the matters addressed by the Bill.

The Asian Business Law Institute

The Asian Business Law Institute (**ABLI**) is a non-profit neutral permanent institute based in Singapore dedicated to providing practical guidance in the field of Asian legal development and promoting the convergence of Asian business laws. We seek to address key problems resulting from legal diversity in Asia identified by stakeholders in the public and private sectors.

ABLI's long-term strategic direction is set by a Board of Governors, chaired by the Honourable the Chief Justice Sundaresh Menon of the Supreme Court of Singapore. The Board of Governors comprises representatives of the judiciaries of Australia, China, Singapore and India, including the Honourable Justice A K Sikri formerly of the Supreme Court of India, Mr. Rahul Singh of the National Law School of India University, and Mr. Parag P Tripathi, Senior Advocate of the Supreme Court of India.

More information on ABLI is available on our website at https://abli.asia.

Asian Business Law Institute
1 Supreme Court Lane
Level 6, Singapore 178879

Tel: (65) 6332 4388
Email: info@abli.asia
Web: www.abli.asia

ABLI's Data Privacy Project

Since 2017 ABLI has undertaken a multi-stakeholder project focusing on the regulation of international data transfers in 14 Asian jurisdictions, including India (**Data Privacy Project**). This project is run in close cooperation with the Data Protection and Privacy Commissions and governments of the region which are currently working on, or reviewing, their data protection frameworks.

The Data Privacy Project is led by Dr Clarisse Girot, a Senior Fellow with ABLI. We should be happy to offer Dr Girot to appear before the Committee if the Committee would find that of assistance. To that end, we **enclose** a copy of her profile.

More information on ABLI's Data Privacy Project is available on our website at https://abli.asia/projects/data-privacy-project.

In May 2018, ABLI published *Regulation of Cross Border Transfers of Personal Data in Asia* (**Compendium**). The first of its kind in Asia, the Compendium provides a holistic study of the regulation of data transfers in the 14 jurisdictions mentioned above, which goes beyond a mere study of data transfer provisions in Asian data privacy laws to address the wider spectrum of issues that have an impact on the legal framework of cross-border data flows. It is designed for governments, data privacy regulators, law practitioners and industry, in Asia and beyond, to understand the scope, the operation and the implementation of regulations applicable to data transfers and data localisation requirements in the region.

The Compendium is available at https://abli.asia/publications/Regulation_of_Cross-border_Transfers_of_Personal_Data_in_Asia.

The Compendium and the Project have met with much success. The Data Privacy Project has become a global reference and a unique regional platform of cooperation for all matters related to the convergence of data protection laws in the Asian region.

New publications in the form of comparative legal analysis and practical recommendations for regional convergence will soon be released by ABLI. We would be pleased to share our findings with the Committee.

We hope that our comments are useful to the Committee and remain at your disposal for any clarification which you may require.

Yours faithfully,

Mark Fisher
Deputy Executive Director
Email Mark_fisher@abli.asia

Dr. (Ms.) Clarisse Girot
Senior Fellow, Data Privacy Project Lead
Email Clarisse_girot@abli.asia

ASIAN BUSINESS LAW INSTITUTE

Comments of the Asian Business Law Institute on the Personal Data Protection Bill, 2019

Background

1. Several jurisdictions in Asia are in the process of adopting data protection frameworks, namely China, Indonesia, Vietnam and, of course, India. In addition, legal reform of existing frameworks is ongoing or has been announced in other jurisdictions of the wider Asia Pacific region, including Australia, Hong Kong SAR, Japan, Malaysia, New Zealand, Philippines, Singapore, and South Korea. These movements are heavily influenced by the EU General Data Protection regulation (**GDPR**), which came into force in May 2018. However, Asia-specific developments increasingly drive trends within the region.

2. In order for these frameworks to achieve their aims it is important that the frameworks be compatible or 'interoperable' with one another, regionally and globally. However, significant differences exist between Asian data protection frameworks. Such legal fragmentation has negative consequences for all stakeholders. By way of illustration, legal fragmentation in this area of the law:

    a. makes it hard for organisations with cross-border operations (local or foreign) to achieve multi-jurisdictional compliance. This is a particular source of business concern in a context where enforcement is taking off, penalties for non-compliance are increasing and data protection and privacy regulators are setting up regional and international networks to support joint enforcement initiatives;

    b. produces a chilling effect on economic activities when legal uncertainty and/or local discrepancies with other frameworks are too important. Companies effectively restrict the geographical scope of their data-related activities when the attached compliance costs or legal risks incurred in some jurisdictions are too high. Innovative projects tend to be put on hold in jurisdictions where they attract the applicability of provisions which have no equivalent abroad, and remain untested locally, with unpredictable consequences attached;

    c. does not necessarily demonstrably advance the situation of individuals through, for instance, enhanced data protection rights or increased oversight. In contrast, the optimization of multi-jurisdictional compliance efforts helps the internal resources devoted by organisations to the implementation of data protection laws and regulations to focus on effectively improving their data protection practices to the benefit of individuals, instead of being absorbed in unnecessary compliance efforts;

    d. is a proven obstacle to international regulatory cooperation, due to the creation of gaps in scope and regulatory powers which may prevent regulators from cooperating on the same facts. In contrast, maximum overlap between national legal frameworks increases the capacities of Data Protection Commissions (**DPCs**) to collaborate. It is, therefore, an important factor to facilitate regulatory cooperation, in line with the OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007) grounded in the OECD Privacy Guidelines (1980). This is particularly significant in a world where the cross-border flow of data faces little transaction costs.

3. The Data Protection Bill of India is considered to be a 'game changer' in the region. It is a modern law that, once passed, will generally be aligned on international data protection standards, including EU GDPR and the data protection laws of key Asian trade partners. Its strong regulatory structure will undeniably position India as a country that 'counts' in global data protection discussions, in which it has been largely absent until now.

4. The comments do not discuss the policies which undergird the Bill and are beyond the remit of ABLI. However, we observe that the Bill departs on many points from the frameworks of India's Asian neighbours. In addition, we observe that there are several provisions of the Bill that could benefit from further clarification so as to prevent the negative impact on the future data protection framework of India that could result from legal uncertainty. We set out the most salient of those matters below.

Key definitions and concepts

5. The Bill contains several provisions which are not defined or otherwise circumscribed. As ABLI's comparative experience clearly shows, there is a risk that the resulting legal uncertainty creates a chilling effect on data practices and data flows that goes beyond the original intention of the lawmaker.

6. **'Sensitive personal data' (s 3(36))**: the concept of 'sensitive personal data' (which is subject to explicit consent requirements, and also underpins the data localisation provisions) is open-ended (i.e. the list in not closed and may be expanded by Government notification under s 15). In legal regimes where a list of 'sensitive data' exists, it is commonly closed and defined in the relevant statute/code (rather than in regulations or other subordinate instruments), to acknowledge for the fact that the additional constraints put on the collection and processing of such data require strictly circumscribing the categories of data concerned.

7. **Financial data as 'sensitive personal data' (s3(36)):** Legal systems which implement the concept of 'sensitive data' traditionally define the concept by reference to the personality rights of the individual (e.g. religious beliefs, data revealing racial or ethnic origin, genetic data, data concerning health or sexual orientation, etc.). The Bill (like s43A of the Information Technology (IT) Act and the associated IT Rule 7 of s43A currently in force) departs from this practice derived from international standards, like the OECD Privacy Guidelines, by qualifying financial information as 'sensitive data', for the main purpose of imposing its storage in India. Whilst onshore storage of financial data has been made mandatory in other jurisdictions (e.g. China and Indonesia), we note that it has been prescribed in specific localisation laws or regulations rather than in statutory provisions referring to the protection of personal data.

8. **'Critical personal data' (s33(2))**: This concept which underpins the data localisation provisions of the Bill is undefined. Critical personal data must be processed *and* stored locally (in contrast to 'sensitive personal data' which appears to be subject to mirroring only[1]). Local processing requires using or building servers exclusively in-country. Given the compliance cost localisation imposes on business, such an important concept would benefit from definition.

9. **'Personal data' (s 3(28)), 'anonymised data' (s 3(3)) and 'non-personal data' (s 91(2)):** The distinction drawn between 'personal data', 'pseudonymised data', and 'anonymised data' is classic in data protection laws. However, in practice many technological challenges are attached to ensuring the effective 'anonymisation' of personal data (because of the difficulties to ensure the complete irreversibility of the anonymisation process).[2] Therefore, contrasting 'non-personal data' (being all data other than 'personal data') with 'anonymised data' (which one would expect to be 'non-personal') in the data protection law may generate confusion, as well as creates an unusual precedent.

10. **'Significant Data Fiduciary'** (**SDF**) **(s 26(1))**: the latest generation of data protection laws attach specific consequences to 'processing operations' that carry 'significant risks' for individuals, subject to a proportionality test, and criteria are generally provided to define such categories of 'risky processing'.

---

1 Data mirroring refers to the real-time operation of copying data, as an exact copy, from one location to a local or remote storage medium. In computing, a mirror is an exact copy of a dataset. Most commonly, data mirroring is used when multiple exact copies of data are required in multiple locations.

2 The first major study which demonstrated the limitations of anonymization was done by the Media Lab at MIT, 'Unique in the shopping mall: On the re-identifiability of credit card metadata', Science 30 Jan 2015: Vol. 347, Issue 6221, pp. 536-539.

The 'data controllers' or 'fiduciaries' that carry out such processing must comply with obligations like mandatory 'Data Protection Impact Assessments' (**DPIA**) or the appointment of a data protection officer (**DPO**). Their obligations are not prescribed *ex ante* for entire categories of organisations, but only for certain categories of 'processing operations.' The Bill departs from this global standard by attaching consequences primarily to SDFs rather than to specified categories of 'processing operations'. Under the Bill, SDFs must be notified as such by the Government, comply with obligations of registration, carry out DPIAs, be audited annually by independent auditors, appoint a resident DPO, among others. Yet, the factors retained to qualify SDFs are general and largely undefined (e.g. 'volume of data processed' and 'use of new technologies for processing').

11. **'Social Media Intermediary' (SMI) (s26(4))**: The Bill provides that SMIs must be notified as SDFs when the number of their users exceeds a threshold to be defined by the DPAI. In addition to obligations weighing on any SDF, SMIs are required to provide an option to users (registering from India or using the services in India) for voluntary verification of their accounts (s 93(1)(d)). Verified user accounts will be marked with a demonstrable verification mark (s 28(4)). Data auditors are required to evaluate SMIs for timely implementation of their obligations under account verification norms (s 29). We note that such provisions are not directly related to data protection matters and therefore to the objectives of the Bill, and that thresholds have generally proven to be inoperative in the data protection laws in the region and have therefore been removed (e.g. recently in Japan). Where such thresholds still exist, they create significant difficulties (e.g. SME exemption in Australia).[3]

Material scope – 'BPO exemption' (s 37)

12. The Bill provides that the Central Government may exempt 'any data processor' incorporated under Indian law from the application of the Act when the data relates to individuals who are not '*within the territory of India*'. The exemption of such foreign data is not uncommon in countries with a strong Business Processing Outsourcing (**BPO**) industry like India.

13. However, drawing on experience in Philippines, Sri Lanka and New Zealand, providing differentiated treatment of data depending on its origin contains many risks. Such exemptions must be carefully drafted to avoid the perception that the BPO industry is not bound by security requirements, which could prejudice, rather than support the BPO industry in India.

Transfers of personal data outside of India

14. By international and regional standards, the regulatory model applied to the data transfer provisions of the Bill (ss 33 and 34) is atypical on several points. We anticipate that these variations will create obstacles to the compatibility of the Indian law with the other data protection frameworks of the region (and beyond):

    a. The Bill intertwines 'classic' data transfer provisions (which exist in most Asian data protection laws and in EU GDPR) with data localisation provisions which require 'sensitive personal data' and 'critical personal data' to remain onshore, with different consequences and exemptions attached.

    b. In contrast to any data protection law containing data transfer restrictions, the Bill implies that personal data that does not fall in the categories of 'sensitive personal data' or 'critical personal data' is freely transferable. This approach has no precedent and has attendant risks. For instance, the Bill does not consider that 'non-sensitive' personal data may become 'sensitive' after it has been combined with other types of data available overseas (the purpose of transferring data is often to merge this data with data from other sources).

---

3 See Peter Leonard, 'Jurisdictional Report: Australia' in Clarisse Girot ed, *Regulation of Cross-Border Transfers of Personal Data in Asia* (2018, Asian Business Law Institute), Para. 57, p. 40.

c. Regarding sensitive personal data that may be transferred under defined circumstances, in the absence of a positive finding by the DPAI that the country of destination offers an adequate level of protection to the data transferred, the Bill restricts the choice of the exporting organisation to two types of data transfer mechanisms (contracts or 'intra-group schemes' to be approved by the DPAI): the extent of parity with the different mechanisms and schemes which exist in other jurisdictions (e.g. certification, codes of conduct) is uncertain.

d. The practical consequences of mandating the localisation of 'sensitive personal data' (i.e. whether localisation requires server mirroring or other measures such as backup servers) are unclear, with very significant financial consequences attached. Feedback from companies that must comply with similar requirements in other jurisdictions like China, Indonesia, or Vietnam, say that they are specifically concerned with any form of legal uncertainty that would surround the scope of these requirements. The two-fold requirement to obtain the individual's consent *and* to implement a specific data transfer mechanism for the transfer of sensitive personal data is atypical. We note that there has been a trend to roll back requirements to systematically obtain the individual's consent for any data transfers in most jurisdictions, including in so-called 'consent-based' data protection regimes, when other legal bases appear to be more appropriate (e.g. recently in South Korea).

e. Sectoral localisation obligations have been in place for several years in India.[4] The Bill does not address whether or how its transfer provisions interplay with localisation obligations mandated in specific sectoral regulations. Inconsistent requirements between the Bill and sectoral regulations will result in legal uncertainty.

Data protection rights of 'data principals'

15. The modalities of some data protection rights included in the Bill differ from those of other countries (e.g. categories of data to be 'ported' under the right of data portability). This will create challenges at the implementation stage for organisations that operate in multiple jurisdictions.

16. We further note that some data protection rights are absent from the Bill by reference to international standards (e.g. right to not be subject to decision based solely on automated decision-making, including profiling, in certain circumstances – cf. Art 22 EU GDPR). Although not all the laws of the region provide for such rights, the absence of such rights from the Bill may impact India's positive assessment by some foreign partners that implement a data transfer policy based on the 'white listing' of countries that apply 'comparable standards' of protection, particularly in the context of the development of artificial intelligence.

Obligations of 'data fiduciaries'

17. The Bill promotes the principle of 'privacy accountability', which requires that organisations put in place appropriate technical and organisational measures and be able to demonstrate what they did and its effectiveness when requested (s 10). This principle (which originates in Canada) is aligned with the international privacy standards long promoted by organisations like OECD and APEC. It has been implemented in all recent data protection laws, including in Asia. Related provisions are thus a strong factor of interoperability of the Bill with most regional and global frameworks.

---

[4] Among others: i) the Reserve Bank of India (RBI) Notification on 'Storage of Payment System Data' April 2018, ii) the Foreign Direct Investment (FDI) Policy 2017; iii) the Unified Access License (UAL), Department of Telecommunications 2016, iv) the Companies Act, 2013 and its Rules, v) the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017, and vi) the National Telecom M2M ('Machine to Machine') Roadmap adopted by the Department of Telecom. See, further, Elonnai Hickok and Amber Sinha, 'Jurisdictional Report: India' in *Regulation of Cross-Border Transfers of Personal Data in Asia*, p.129.

18. However:

    a. certain obligations imposed on SDFs under the 'accountability principle' are unprecedented. For example, the conditions for registration and compliance of a 'consent manager' (s 94(2)(h)), the assigning of a 'data trust score' (s 29(5)), yearly auditing (s 29), and their practical implications are still unclear.

    b. the appointment of DPOs is the keystone of all privacy management and data governance programmes. As such, the DPO's autonomy and protection from reprisals from management for performing the DPO role should be guaranteed in the Bill, as in Art. 38 EU GDPR (especially as the obligation to appoint a DPO weighs exclusively on SDFs).

Data Protection Authority of India (Chapter IX)

19. The role and powers of the future DPAI are vast, in part because it will 'wear multiple hats', and thus have a different profile from other Data Protection and Privacy Authorities in the region and beyond.

20. However, we see a risk that the capacity of DPAI to cooperate fully with its counterparts be limited under the Bill:

    a. The Bill does not contain any express provisions on international cooperation in policy or enforcement. Given the ease of cross-border data flows, modern data protection laws should expressly provide their national DPC with the power to engage in international cooperation in accordance with the recommendation to OECD Members to *'improve their domestic frameworks for privacy law enforcement to better enable their authorities to co-operate with foreign authorities'*.[5]

    b. The Bill does not prescribe that the members and staff of the DPAI are held by strict confidentiality requirements, which is often a pre-condition for the international sharing of information obtained in enforcement proceedings by a foreign counterpart. Such requirements also flow from the OECD recommendation to take *'appropriate steps to maintain the confidentiality of non-public information exchanged and respect any safeguards requested by the Privacy Enforcement Authority that provided the information'*.[6]

    c. The Bill provides that persons appointed to be members of the DPAI must be *'of ability integrity and standing'* (s42(4)) but the DPAI is also subject to directions which the Government '*may think necessary in the interest of the sovereignty and integrity of India, the security of the State, friendly relations with foreign States or public order*' (s 86(1)). Whilst a 'centralised' model is not unusual by Asian standards, this limitation on the DPAI's independence may create challenges for the DPAI to become a full member of organisations like the Global Privacy Alliance (formerly the International Conference of Data Protection and Privacy Commissioners) and for India to be white-listed by some jurisdictions.

---

5 Please refer to ABLI's Data Privacy Compendium, Jurisdictional Reports for Australia, Hong Kong SAR, Japan, Macau SAR, New Zealand, Philippines, Singapore, South Korea (Sections on 'International Regulatory Cooperation') for comparisons.

6 OECD Recommendation on Cross-border Co-operation in the Enforcement of Laws Protecting Privacy (2007).