21 February 2020

The Director
Lok Sabha Secretariat
Room No. 152
Parliament House Annexe
New Delhi-110001

Via Email to: jpc-datalaw@sansad.nic.in and mrs.mlekhi@sansad.nic.in

Dear Sir / Madam:

Joint Parliamentary Committee's Consultation on Draft Personal Data Protection Bill (PDPB), 2019

The Asia Securities Industry & Financial Markets Association (**ASIFMA**)[1] and its members are grateful for the opportunity to comment on the impact that the draft Personal Data Protection Bill (PDPB) will have on India-based, and India-facing, banks and financial institutions. ASIFMA appreciates the Joint Parliamentary Committee's (JPC) efforts to solicit industry feedback.

We would very much appreciate an opportunity to have an in-person meeting with the JPC on the PDPB and its impact on the international financial services industry in India.

We highly admire the Indian Government's successful and commendable efforts so far in shaping the PDPB, while consulting with the industry along the way. For reference, ASIFMA has also submitted comments on the PDPB-2018, once in January[2] 2018 to the Justice B.N. Srikrishna Committee, and twice in September[3] 2018 and August[4] 2019 to the Ministry for Electronics and Information Technology (MEITY).

GENERAL COMMENTS

Increasing global regulatory focus on data often stems from concerns regarding privacy and data security among non-regulated entities in the broader economy; however, in the context of already regulated financial institutions poorly targeted data localisation rules can in fact undermine the resilience and security of financial systems and institutions.

Further, incompatible new restrictions introduce conflicts of law in areas such as anti-money laundering (AML) safeguards where, for instance, international financial institutions need to share

[1] ASIFMA is an independent, regional trade association with 130+ member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

[2] "ASIFMA response to the White Paper of the Committee of Experts on Data Protection Framework for India", *ASIFMA*, 31 January 2018. https://www.asifma.org/wp-content/uploads/2018/08/asifma-response-to-india_s-white-paper-on-data-protection-final.pdf

[3] "ASIFMA Response to the Draft Personal Data Protection Bill, 2018 (PDPB)", *ASIFMA*, 28 September 2018. https://www.asifma.org/wp-content/uploads/2018/11/asifma-response-to-the-draft-personal-data-protection-bill-2018-pdpb.pdf

[4] "ASIFMA comments on MEITY additional consultation on the PDPB", *ASIFMA*, 23 August 2019. https://www.asifma.org/wp-content/uploads/2019/08/asifma-comments-on-meity-pdpb-august-2019-v20190823-final.pdf

information across affiliates and jurisdictions to generate information necessary to file suspicious activity reports.

India is a key participant in the international banking ecosystem and an established and favoured outsourcing location for global banking (and non-banking) services and activities. But, compared to other jurisdictions' approaches to allowing data mobility whilst protecting data privacy, the PDPB could threaten India's role as a competitive outsourcing location and as a place to do business, due to the logistical and legal impediments emanating from the current PDPB proposals.

In general, we have a number of broad key concerns relating to:

- PDPB focusing on technology prescriptive means to address privacy and security when the ability to transmit data is so fundamental to enabling a healthy, secure financial system and when alternatives to data localisation exist for achieving the same policy objective and are being deployed in other leading jurisdictions, including in Asia Pacific;
- The scope of the draft law being so broad in terms of the sectors covered, particularly in light of existing policy and regulation to which the financial industry is subjected to in order to protect customer privacy and data integrity, as well as covering data principals who are not Indian citizens or residents; and
- The draft Bill's blanket requirement to provide notice and seek consent from data principals, which in is unworkable in a modern financial context, for example when firms are dealing with multiple entities including institutions, corporations and trusts where there is no direct relationship with underlying representatives.

SECTION-WISE COMMENTS

Just as importantly, we also provide the following specific comments on the PDPB-2019 draft following deliberation and discussion with our members, in the spirit of constructive dialogue targeting a safe data environment for Indian citizens while protecting the resilience and security of financial systems and institutions, and supporting India's ability to retain its place as a key participant in the international banking ecosystem.

Section 1: Commencement

Due to the complex nature of the issues covered in the PDBP and the technical challenges implementation will present to stakeholders, we recommend that a transition period of three years (from the date final rules and regulations are notified after PDPB is enacted into law) be incorporated into the Transitional Provisions (such as Section 97 of the previous version of the PDBP-2018).

Section 2A: Application of Act to Processing of Personal Data

We are concerned about the expansive scope of PDPB. The scope of the PDPB appears to cover all data collected or processed in India and the offering of goods and services to individuals throughout India, including Data Principals who are non-Indian citizens, non-Indian residents and tourists. We are concerned about this expansive scope of the PDPB as it would likely apply to activities that involve not only data collected in India, but also data processed by many large and small entities inside India that originated from outside controllers and data fiduciaries. This is important for data fiduciaries covered under the PDPB, which are already GDPR compliant and processing EU data. We propose that the definition of personal data be clearly confined to Data Principals who are citizens and residents of India. Firms that are data fiduciaries/controllers of personal data of foreign data subjects are already required to comply with foreign data protection laws elsewhere e.g. GDPR. hence the Bill's expansive definition is unnecessary and sets up conflicting requirements. We welcome clarification by the Government, the future Data Protection Authority (DPA) or sector specific regulators regarding these scope issues in order to understand how the requirements in the

PDPB apply to our stakeholders and supports a robust, open business climate. A revised version of the bill should take into account that personal data received from non-Indian residents is already subject to privacy regulations of their home jurisdiction. The revised PDPB should consider and recognise personal data protected under foreign privacy laws/regulations and avoid duplicative overlay.

Section 3: Definitions. (36) "Sensitive Personal Data"
We submit that the definition of SPD is too broad, and problematic. Section 3(36)(i) should not include financial data. Not all categories of financial data are always "sensitive", nor would loss of certain categories result in a real risk of "harm" (as defined in the PDPB) or discrimination to the Data Principal. Information Technology - Reasonable security practices and procedures (IT RSPP) rules stipulate financial information such as bank account/credit card/debit card/other payment instrument details as SPD, and the criteria for SPD, which includes similar types of financial data and also passwords, could be resulting in an onerous and challenging requirement. We submit that the PDPB consider retaining the definition of SPD as in the IT RSPP rules & not add increased categories.

We recommend against applying a blanket approach to classifying financial data as SPD. Financial data is significantly different from other data categories under this definition which largely relate to one's person such as their biometric data, genetic data, and sexual orientation, among others. Financial data results from, for example, the opening of a bank account, engaging in a financial transaction, or purchasing an insurance policy. Similarly, not all health data should be considered sensitive. Examples of non-sensitive data such as height, weight, non-major ailments and medication information relating to such ailments, medical leave information should not be considered sensitive data. Other Examples of non-sensitive financial data include relationship with financial institution, type of policy, etc. EU GDPR and the Australia data privacy rules do not explicitly define SPD to include financial data. In addition, we note that the Bill allows the government to define additional categories of sensitive data creating uncertainty from a business perspective. We note that the EU GDPR uses an exhaustive list approach. Due to sector-specific regulations, it is unnecessary to include financial data in the definition of SPD.

Section 7: Obligations of Data Fiduciary
In relation to Section 7. (1) (c), we believe that it is not practically feasible for the data fiduciary to provide the Data Principal with the contact details of the data protection officer (DPO) at the point of collection of data. In the GDPR, for example, the controller or the processor publishes contact details of the data protection officer and communicates them to the supervisory authority.

The Bill has introduced the concept of data fiduciary on the premise that the relationship between the individual and entities with whom the individual shares personal data is one that is based on a fundamental expectation of trust. The Government on 31 July 2017 constituted a "Committee of Experts on Data Protection" chaired by Justice B.N. Srikrishna. The Committee examined issues on data protection and submitted its Report on 27 July 2018, and noted "an individual expects her data to be used fairly and in a manner that fulfils her interest and is reasonably foreseeable. This is the hallmark of a fiduciary relationship and this translates to a duty of care to deal with such data fairly and responsibly expected by the Data Principals and makes such entities data fiduciaries."

Across jurisdictions, data privacy laws consider personal data as the 'property' of the Data Principal or data subject. Accordingly, the Data Principal continues to be the owner of his/her data and in this regard, is offered with wide variety of rights in order to protect and respect the ownership on such data. The PDPB moves away from this concept, however, and uses the term 'data fiduciary' denoting a fiduciary relationship between the Data Controller and Data Principal. Under Indian law, a fiduciary is a person to whom power or property is entrusted for the benefit of another. Considering this, the

personal data continues to be the property of the Data Principal and the PDPB allows only the Data Principal to determine the use and purpose of such data and restricts the data fiduciary from using the data beyond the permitted scope, and the data fiduciary neither has the power nor authority to act 'for the benefit' of the Data Principal – in fact, the data fiduciary is under a duty to act 'in accordance' with the instructions of the Data Principal. Consequently, the data fiduciary will not be discharging fiduciary obligations as understood in the context of Indian law. To treat the relationship between Data Principal and data fiduciary under the PDPB as a fiduciary relation is accordingly incorrect and inappropriate.

We recommend removing the requirement for establishing a fiduciary relationship between the Data Principal and data controller/processor and an approach similar to global policymaking practice in this area be introduced, and that the Bill use the concept of 'data controller' in place of 'data fiduciary'.

Section 11: Processing of Personal Data on the Basis of Consent
Our members observe that clients are reluctant to sign complex documents. If negotiated on a case-by-case basis, the components of the consent prescribed by Section 11 would make the process cumbersome and elongated, hampering business and subjecting financial institutions to demands which would compromise compliance with this section.

When data is shared between two data fiduciaries, it is relevant for the PDPB to clarify on which data fiduciary the obligation of notice and consent requirements fall. A blanket requirement of providing notice and seeking consent from the Data Principals, when a data fiduciary is receiving information from another data fiduciary is impractical, especially, when dealing with institutions/ corporations/trusts where there is no direct relationship with the underlying representatives/Data Principal. For example, banks receive from institutions/corporations/trusts, personal/sensitive personal data regarding their employees, directors and other authorised representatives during the KYC process. This will poseogistical and practical challenges including administration, tracking and monitoring of notice and consent. Further, organisations collecting data from employees would in any event be subject to the provisions of the PDPB already and, therefore, the individuals' rights would already provided for. In comparison, Singapore's Personal Data Protection Act, 2012 permits data collected during employment to be shared and processed by the employer with another organisation during ordinary course of business for undertaking business transactions. The PDPB must consider and provide similar relaxations.

Banks, for the purpose of complying with Anti-Money Laundering laws, investigating international fraud o undertaking audits are required to share data, including sensitive personal data, across Indian borders. We recommend acknowledgement from the Data Protection Authorities for an appropriate waiver of consent from Data Principal for such cases.

We also note that it is difficult to rely on consent as a ground for processing in many instances if such consent is able to be withdrawn. For example, where processing is necessary for performance of a contract or to comply with laws (whether domestic or global), organisations will not be able to rely on consent in practice because they will be required to continue processing such personal data under other obligations, even if the consent is withdrawn. We therefore recommend that additional lawful grounds for processing are introduced as they have been in other laws (e.g. the GDPR) so that the use of consent is reserved for instances where it is appropriate.

Section 12: Contractual Necessity as Ground for Processing

A separate ground of contractual necessity (also called "performance of a contract") should be included in the law as one of the bases for processing personal data. We recommend the below additional ground for processing of personal data without consent to be included in Section 12:

- Where processing is necessary for the performance of a contract, to which the Data Principal is party or in order to take steps at the request of the Data Principal prior to entering a contract;
- Where processing is necessary for compliance with a legal obligation to which the data fiduciary is subject; and
- Where processing is necessary for the performance of an activity carried out in the public interest or in the exercise of official authority vested in the data fiduciary.

We request that from ease of doing business, the provisions of the PDPB consider and make provision for the fact that many of the financial institutions and GSCs that could be in scope are multinationals that are already subject to GDPR, and deal with Indian data. For example: unlike GDPR, the PDPB does not mention "contractual necessity" as one of the legal bases for processing. This means the only option available to companies is to seek consent of the Data Principal for processing data, unless one of the narrow and situation-based lawful bases is available (e.g. legal compliance, medical emergency, or employment).

Sec. 11. (4) of the bill states, "The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, shall not be made conditional on the consent to the processing of any personal data not necessary for that purpose." We submit to take out the word "not" from the text above, and the revised text should read as follows: "The provision of any goods or services or the quality thereof, or the performance of any contract, or the enjoyment of any legal right or claim, can be made conditional on the consent to the processing of any personal data necessary for that purpose." Now the text already provides contractual necessity as a bases for processing data.

Section 13: Processing of Personal Data Necessary for Purposes Related to Employment

As discussed above, it would not be appropriate in the context of an employment relationship to rely on consent for personal data processing, in particular because it may be difficult to demonstrate that it has been freely given and due to the fact that withdrawal of such consent would be deeply problematic in practice. However, the exemptions to the requirement for consent in Section 13 are currently not sufficiently broad to allow many business-critical processing activities that involve the processing of employee data. For example, consent should not be required for: 1) administration of the employment contract and/or relationship; or 2) defence of employment-related litigation; or 3) appropriate business record keeping and management (e.g. transaction and communication data which necessarily often includes employee data).

We therefore recommend Section 13 be expanded to include the following addition: "(e) any other activity relating to the performance of the employee's duties or the administration of the employment contract and/or relationship, both during the employment relationship and after its termination". We also recommend the concept of employee be made broad enough to capture other types of workers, such as contractors, secondees or agency workers.

The PDPB helpfully provides for processing by a data fiduciary, of personal data when necessary for purposes such as employment of data principals. In this regard, Section 13 says that any personal data that is not sensitive personal data, may be processed by a data fiduciary, if the processing is necessary for (a) recruitment, (b) termination of employment, (c) provision of any service or benefit, (d) verifying attendance; or (e) any other activity relating to the assessment of performance,

where the consent of the data principal is either not appropriate having regard to the employment relationship, or would involve disproportionate effort on the part of the data fiduciary. However, given the definition of "sensitive personal data"[5], the issue that arises from this exclusion is that it will not always be possible to categorically segregate between what is sensitive personal data or not in situations that associate with the described aspects that relate to employment, e.g., financial, health or biometric data, and thus this should be reconsidered as else, since personal data for the purposes referred to in Section 13 may often include aspects of sensitive data, this exception will potentially be largely defeated.

Section 14: Processing of Personal Data Necessary for Other Reasonable Purposes

The examples of personal data necessary for other reasonable purposes would include but not be limited to personal data processed for employment purposes, including data necessary for hiring, managing, terminating and evaluating an employee and conducting any internal investigations (such as suspected non-compliance with laws and company policies); and personal data processed for conducting any investigation or proceedings, such as claims assessment.

For financial institutions such as banks in India, the minimum data (i.e. including personal and sensitive personal data) to be collected is already prescribed by the Reserve Bank of India (RBI) along with the associated purpose e.g. for Know Your Client (KYC). Therefore, collection of this data is necessary to comply RBI requirements. In addition, financial institutions are subject to a broad range of non-domestic laws and regulations that govern the provision of financial services in a global environment. Hence, the test of reasonableness or public interest or the other provisions of this section should not apply to banks and financial institutions. Instead, an exception should be provided for banks and other financial institutions (as exempted entity types) or for the provision of financial services (as an exempted type of activity), which are regulated and are required by sectoral regulation or by applicable law to obtain and deal with such information. It is critical that this exemption be in effect when the Act comes into effect, to avoid business uncertainty.

Section 14(1)(b) refers to whether the data fiduciary can reasonably be expected to obtain the consent of the Data Principal as one of the factors to consider for establishing "reasonable purposes". This is contradictory as consent does not need to be obtained for processing necessary for reasonable purposes. We suggest that this is instead rephrased to reflect reasonable likelihood that the Data Principal would not object to such processing of their data.

We also suggest that it may be appropriate, in addition to "reasonable purposes" specified in regulations, to build in a mechanism by which data fiduciaries are able to process personal data for purposes of their legitimate interests or those of a third party, where consent cannot reasonably be obtained and where such interests are not overridden by those of the Data Principal. This could be coupled with requirements to: 1) document the assessment of such interests (to ensure accountability); and 2) articulate such interests in notices provided to the Data Principal (for transparency). This would bring the Act more in line with the approach taken in other laws (e.g. GDPR) and would relieve the Central Government and the Authority of the burden of prescribing an

---

5 "personal data" is data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling.

"sensitive personal data" means such personal data, which may, reveal, be related to, or constitute: (*i*) financial data; (*ii*) health data; (*iii*) official identifier; (*iv*) sex life; (*v*) sexual orientation; (*vi*) biometric data; (*vii*) genetic data; (*viii*) transgender status; (*ix*) intersex status; (*x*) caste or tribe; (*xi*) religious or political belief or affiliation; or (*xii*) any other data categorised as sensitive personal data under section 15.

exhaustive list of “reasonable purposes”, while allowing for oversight, where required, since the documented assessments could be inspected when necessary by the Authority.

Section 14(2)(g) refers to processing of publicly available personal information as one of the “reasonable purposes”. It should be separately addressed and made clear that such personal information in the public domain does not require consent since it does not relate to purpose or grounds for data processing.

Section 17 and 18: Rights to Confirmation and Access, Correction and Erasure
The right of access granted to the Data Principal to seek information on the personal data with respect to its processing or can potentially be misused by the Data Principal. The explicit consent taken from the Data Principal, at the time of collection of the personal data, providing the purpose, further distribution of the personal data etc. should suffice as a record for the Data Principal.

It is also important to note the logistical and regulatory challenge that the Right to Erasure raises for banks and other financial sector organisations. Unlike, the right to be forgotten, the right to erasure does not include a carve-out for retention of information for compliance with applicable law/regulations and may conflict with such an institution’s retention policy based on the other domain regulatory requirements and the requirements of other applicable law. Even if data fiduciaries are allowed to retain the personal data, there is a requirement for this information to be labelled as disputed which would then lead to question around the sanctity of the information retained itself. Any right to erasure retained within the PDPB should have a carve-out for legal and regulatory obligations and address the sanctity of disputed information retained by data fiduciaries.

If Access, Correction and Erasure principles remain provided for in the Act, these should be limited to prevent abuse or misuse, such as providing for exceptions from such requests. Such exceptions may include:

- Data used for investigations or proceedings;
- Opinion or evaluative data;
- Personal data which may reveal confidential commercial information;
- Where the burden or expense would be unreasonable and disproportionate to the interests of the individual; and
- Trivial, vexatious or frivolous requests.

There should not be a need to provide justification to the Data Principal where the reason for providing for the above exceptions would be impinged. For example, if an organisation refuses to provide access to a Data Principal as the data requested for is relevant to an ongoing internal investigation of wrongdoing, providing such a justification may lead to the Data Principal attempting to cover their tracks.

Section 19: Right to Data Portability
The right to data portability by Data Principals should be limited to data collected rather than broadly processed through automated means. It should be clarified that it does not create an obligation for firms to convert manually stored data to electronic formats to facilitate transfer. Also, the right for Data Principals to receive their personal data in 19(1)(1) should only for the purpose of confirming instructions for data porting requests so as not to create unnecessary burdens for firms.

Lacking a standardised format and mechanism for data sharing, technologies used by financial institutions on the one hand and by a Data Principal on the other will be different. Data Fiduciaries will be required to install additional technology to convert processed data into a machine-readable format. We believe the term ‘machine-readable format’ needs a clear definition. There are also

competitive issues which require laws to promote cross-sectoral data sharing. Further consultation with the industry is required before these obligations are implemented. Further, we believe that the scope of this provision should not extend to "inferred data" or "derived data" which may attract technical complication and IP right issues.

There are also compelling reasons which even suggest that this right be removed from the Act altogether:

- *The security of personal data that is subject to a data portability request:* Data portability requirements will increase the risk to the security of personal data given the different standards of security and levels of maturity between sending and receiving organisations. Organisations within specific industries collect certain types of data which may have a greater impact (e.g. identity theft or fraud risk) on data subjects should a data leak occur during the sending of such data pursuant to a data portability request;
- *Potential avenue for unscrupulous organisations to obtain personal data without valid authorisation:* Such organisations may promise incentives to data subjects without any intention to fulfil this promise, or they may use such personal data for purposes other than what has been notified. This may be exacerbated by such organisations being based outside of PDPB's jurisdiction, which may make enforcement challenging;
- *Costs:* Data portability obligations add substantial costs to comply with and administer, and invariably some of these costs may be passed on to consumers who may not benefit materially from the data portability requirement;
- *Curtailing Innovation:* Data portability obligations may curtail investment in data analytics and innovation. It would be challenging to make a business case for the considerable investments needed for such projects when the benefit of such investment would be passed on to competing organisations which do not undertake such investments

If data portability requirements are retained, they should be limited to personal data provided by the data subject. Organisations in certain industries like financial institutions are likely to hold data which consist of commercially sensitive and/or confidential information and which are ordinarily commingled with personal data. Also, the liability for any breach during or after the porting of data should be clearly demarcated between the sender and recipient.

Section 20: Right to be Forgotten

We suggest that these obligations should not apply to collection of information by banks and financial institutions because the KYC process is an ongoing process. Further, customer data such as financial history, credit history etc. is essential to be maintained by banks for posterity and regulatory reporting, and we propose that GDPR should be followed on this.

Section 21: General Conditions for the Exercise of Rights in this Chapter

We have observed that the "Consent Managers" definition, and role are not provided for in the Bill, and request it to be provided. It is likely that the provision for consent managers, without strict regulation of such consent managers, might give rise to an industry of unscrupulous companies whose strategy would involve harassing legitimate organisations with systematic frivolous and vexatious requests for access, correction, erasure and data portability requests. This might not benefit anyone while adding considerable cost and burden for organisations.

Section 22: Privacy by Design

Section 22(1)c requires that technology of a commercially accepted or certified standard be used to process personal information. To truly ensure privacy protection, we recommend PDPB follow and adopt technology-neutral and outcome-focused privacy principles, and allow data fiduciaries the

flexibility to choose technologies and protections appropriate to specific risks and also enable continued innovation and competitiveness in light of a very dynamic and fast evolving technology landscape.

The mandatory requirement for a data fiduciary to submit its privacy by design policy to the DPA for approval will have the potential of creating a logistical challenge for both data fiduciaries and the DPA, with the DPA being inundated with a multitude of such documents. We suggest that the requirement to have the policy approved by the DPA be applied on a case-by-case basis where there is high level of risk to Data Principals.

Further technical aspects of this policy may be proprietary to each data fiduciary or contain confidential information and accordingly publishing the same may not appropriate or feasible. The policy along with the certificate provided by the DPA can be published on the website of the data fiduciary.

Further, since banks are intensively regulated and subjected to regular inspections by the sectoral regulator, it should be considered whether banks, and any similarly placed financial institutions, should be excluded from the purview of application of such provisions.

Section 25: Reporting of Personal Data Breaches

Section 25 requires every data fiduciary to notify the DPA about any data breaches likely to cause harm to any Data Principal. Section 3(20) defines harm, which includes "(viii) any denial or withdrawal of a service, benefit or good resulting from an evaluative decision about the data principal", which is distinct from "significant harm" defined under Section 3(38).

Under Section 25, the notification threshold appears to be very low, as all breaches with any likelihood of harm will require to be notified to the DPA. This may result in the DPA being inundated with a high volume low risk data breaches and create both delays and excessive operational overheads for data fiduciaries without any corresponding benefits for the Data Principal. Additionally, a denial or withdrawal of service resulting from an evaluative decision may be entirely justified and may not cause the Data Principal to suffer any real harm.

The generally understood objective of a mandatory breach notification requirement is 1) to enable individuals to mitigate the risk of identity theft or fraud; and 2) to allow the DPA to take action to correct any persistent or systemic data security issues. We recommend that 1) notification of breaches should be mandated only if there are likely to cause significant harm to the Data Principal; and 2) Section 3(20)(viii) should be removed.

In deciding whether a mandatory breach notification requirement meets this objective, the DPA should consider the following:

- Given the proliferation of social media in India and a technology savvy population, serious data breaches are likely to come to light and make the news quickly;
- The number of breach notifications that the DPA would expect to receive will be high. In this regard, as it stands the reporting threshold is very low. This would generate a substantially disproportionate amount of work, both on the part of data fiduciaries and the DPA. The DPA and data fiduciary would have to devote an inordinate amount of resources in investigating each matter (on the part of the DPA), responding to the DPAs requests for information (on the part of data fiduciaries) and responding to queries from the public (both the DPA and the data fiduciary). These resources could be better spent on improving and strengthening data protection measures of each individual data fiduciary and developing the data protection ecosystem;

- Notification fatigue on the part of individuals would undermine the objectives of a breach notification requirement;
- While reserving mandatory breach notifications for the most serious cases where there is a systemic data risk and a real likelihood of substantial harm will likely mitigate the inordinate resources devoted to work arising from a mandatory breach notification requirement, it is very likely that data fiduciaries will still over report to be cautious. This problem of over-reporting is likely to be exacerbated given that the Act is new and data fiduciaries would take time to understand how to comply with the Act in practice; and
- The DPA may want to consider a statutory undertaking regime with regard to other mechanisms which would meet the objectives of a mandatory breach notification without its shortcomings. A well calibrated statutory undertaking regime would encourage data fiduciaries to self-report even without a mandatory breach notification requirement and can be dealt with quickly while ensuring that the data fiduciary undertakes to remediate the matter and implement the necessary measures to mitigate the risk of similar incidents.

Section 26: Classification of Data Fiduciaries as Significant Data Fiduciaries

Financial institutions are already subject to significant regulation including by the RBI and are subject to Banking Secrecy and confidentiality legal and regulatory requirements including under the Banking Regulation Act, 1949 and the Prevention of Money Laundering Act, and various regulatory frameworks. Heavily regulated industries such as FIs should not have additional compliance requirements placed on them. We submit that the PDPB will subject such institutions to additional requirements that are not necessary including as the processing of personal data (and its categories) is an incidental activity associated with the products and services offered by banks and they are not in the business of collecting and processing personal data (and its categories) of Data Principals whether based in India or overseas. It is not clear in the PDPB as to what would make a data fiduciary "significant", and we would be grateful for a descriptive definition.

The Bill introduces governance and accountability measures for data fiduciaries. Additionally, the Bill requires that significant data fiduciaries (the Bill does not specifically list them but defines them as data fiduciaries as notified by the Authority) to comply with certain additional governance measures. These include 1) registering as a significant data fiduciary with the Authority; 2) conducting data protection impact assessments; 3) maintaining records of processing; 4) appointing data protection officers; and 5) an audit of its records and processing activities annually by a data auditor.

As banks are already regulated by RBI and other sectoral regulators, and are required to maintain records and are audited annually including with regard to its data policies and measures, we recommend that the banks should not be classified as significant data fiduciaries under the Bill.

Section 27: Data Protection Impact Assessment

In regard to the data protection impact assessment requirement, we request clarity as to the criteria regarding "use of new technologies" or "large scale profiling criteria", what would be within the scope of "large scale profiling", and what is the threshold for "large" scale. As this involves the reporting of the assessment results by the DPO to authority, such clarity is particularly critical.

Section 29: Audit of Policies and Conduct of Processing

With reference to the requirement that an independent data auditor perform annual audits (for a significant data fiduciary), we seek more clarity on whether such auditor should be a third party, or whether an independent control function from within the data fiduciary's organisation would be able to fulfil the requirement.

Sections 33 and 34: Data Flow and Data Localization

We submit that the PDPB should establish data protection principles or parameters (e.g. legal binding instruments, requiring organisations to ensure adequate data protection on data transferred overseas) and place the responsibility on organisations to determine the appropriate actions to fulfil these parameters before transferring Personal Data and Sensitive Personal Data overseas.

Large multi-national organisations use global platforms including back-up systems, situated at different locations in the world, in order to not only serve clients well in and across geographies but also for the purposes of robust resilience, business continuity and disaster management. Data, particularly for clients who have an international footprint or receive their services in a clustered format (e.g., particular locations overseeing and managing a number of geographies), is often processed at different locations and also at global levels as the relationship may vest in geographical locations originating the relationship. Restricting the flow of data will severely hamper and restrict the ability of financial institutions to service clients. It would also limit data pools which are a key resource enabling businesses to employ artificial intelligence (AI) and future technologies to improve existing services, create entirely new products to the benefit of consumers, and potential new businesses including in India.

We therefore submit that the requirement for data localisation be removed. We previously laid out how regulatory objectives to ensure privacy is not related to the location of data and undermines other important regulatory objectives, for example, such as cyber security and monitoring illicit activities. In addition, data localization has a negative economic impact on innovation, an area important to the future of India.

In addition, restrictions in data sharing of key information hinder holistic risk management by firms and will impact consistent enterprise risk management approaches including effective cybersecurity measures. Data localisation requirements also pose obstacles to the adoption of cloud services and will negatively impact India as a choice location for outsourcing of such third-party services. We submit that the need for approval of an intra-group arrangement should be reconsidered.

The Bill requires that the consent of the individual Data Principal be obtained as a requirement for cross border transfers of sensitive personal data despite the adoption of other protective mechanisms (e.g. transfer to White List countries). This makes it considerably more onerous than data protection laws in other jurisdictions. GDPR contains numerous provisions with regard to the transfer of data to third countries or international organisations. (Chapter 5 – Arts 44 – 50), aiming to ensure that the data protection is not undermined by transfer to a third country. These conditions include adequacy decisions (depending on the definition in the PDPB this could be very similar to the "whitelisting"), other "appropriate safeguards", and binding corporate rules. We request that this provision be reconsidered, and other effective mechanisms be assessed including from the point of view that the requirements of various jurisdictions be aligned to facilitate ease of doing business. In this context, the EU provisions should be examined. We suggest that the Central Government should specify a White List of countries, entities or international organisations within a given timeframe from the implementation of the Act.

Certain provisions of the Bill localise certain types of data determined to be critical or sensitive. The inclusion of financial data as sensitive data (e.g. trading inputs, prices) would have a negative impact on innovation in the financial sector without resolving for a relevant data risk. The development of new technologies like AI analytics and machine learning (ML) would be impacted as firms restrict the use of different data sets that do not represent Personally Identifiable Information (PII).

We submit that in the White Paper of the Committee of experts on Data Protection Framework for India (referring to Chapter 8 and 9), the expert committee has recommended that cross-border data flow needs to continue to be encouraged and that regulators should focus on adequacy of protection while handling sensitive personal information. The paper also mentions that all-encompassing data localisation mandates are not seen in most countries. We recommend that all data localisation requirements be eliminated from the PDPB in order to continue to permit borderless processing, thus enabling organisations to harness scalable and secure IT infrastructures.

Currently, the PDPB includes the designation of certain data as critical data, and that it may not be transferred outside India. The scoping of critical personal data will be at the discretion of the Government, without guidelines to provide any certainty what data could potentially be covered by this term. Entities will be faced with significant uncertainty with regard to planning their processing activities. Given it is difficult to define or categorise critical data under the boarder concept of personal data, we submit that the concept of critical data be removed entirely from the Bill. This would reduce uncertainty and bring India's proposed legislation in line with other major data protection regimes globally.

If it is decided that the critical data classification will continue, we submit that stakeholders be consulted, and transparency be applied in the process of its classification. We also believe it would be valuable to have discussions regarding the actual compliance obligations associated with the provisions of the Bill.

In relation to data storage, under clause 33, the Bill imposes data localisation requirements for two types of data: critical personal data and sensitive data. We urge that these requirements be reconsidered. Data localisation, including mirroring, presents significant risks for the financial sector and does not support personal data protection objectives. The location of data does not make it more secure or enhance privacy. The tools that a financial institution employs in its systems ensure the most secure and operationally resilient environment.

The policies that financial institutions utilise under these conditions also ensure that they meet a country's privacy standards. We submit that "How", not "Where", is the correct question for consideration. Data localisation of financial data also carries with it the undermining of financial regulatory objectives related to the monitoring of illicit activities, tracking terrorist financing flows, sharing of information among regulatory authorities and governments, and ensuring sound prudential policies that promote financial stability, worldwide. Unlike in other sectors, financial institutions have a long and positive track record in regard to ensuring that access to data is appropriately provided for regulatory and supervisory purposes. We would like to engage with the Indian authorities with regard to how financial institutions already ensure access to data regardless of where data is stored or retained.

The Bill also requires deletion of data that is sent offshore for processing. We submit that deletion of data is not appropriate for financial institutions as it undermines their ability to adhere to complex KYC requirements as well as to monitor illicit activities such as terrorist financing flows. For financial institutions, it would be inconsistent with sound prudential practices and regulators set high standards for financial institutions to maintain data for extended timeframes including for audit, stability aspects and other matters. We suggest that the requirement for deletion of data should not be applied to the financial sector.

We submit that financial institutions, in compliance with the requirements of home and host country regulators have for long stored and processed data outside India, and we request that the

ability to do so be maintained to ensure appropriate mitigation of the significant risks described above.

Section 37: Exceptions
GSCs primarily support their global entities, may be affiliates of the non-Indian data controller/fiduciaries or third parties, and act on the instruction of their global entities to process or support the processing of data owned by the global entities. These global entities, which are data controllers or fiduciaries in their own right, are subject to the data protection laws (e.g. EU GDPR) of the country where the personal data is collected. Therefore, the PDPB should not apply to processing of foreign personal data in India. We submit that the processing of personal data of foreign Data Principals by GSCs be excluded from the provisions of the PDPB, and we would welcome dialogue on this aspect so that we can be of assistance.

Section 40: Sandbox for Encouraging Innovation
The Bill has included a provision on the establishment of a regulatory sandbox to encourage innovation in AI and ML vis-à-vis personal data and that data fiduciaries may be exempt from certain provisions of the PDPB. This is a positive forward-looking provision. Clarification on the scope of application and how the exclusion operates would be beneficial as the regulatory sandbox is not defined.

Section 57: Penalties and Compensation
The proposed law is a new branch of law in India unlike the EU's data protection laws which have been in place for a significant period of time and there is well developed jurisprudence on this subject.

Some of the proposed grounds in the PDPB on which penalty can be levied are subjective. We submit that the proposed penalties are also significant and may be disproportionate to the alleged breach, and result in certain unintended consequences. We submit that penalties should be commensurate to the contravention, and that the maximum amounts of penalty be capped, with increases for repeated contraventions.

The penalty regime may be considered a significant deterrent with respect to doing business in India particularly when read with provisions of the PDPB which carry significantly enhanced requirements of obligations and associated costs and effort of compliance for data fiduciaries, coupled with lack of clarity in certain instances as regards the provisions of the law. These might make India a less attractive place to carry on business or economic activity, and further deter innovation and entrepreneurship, including domestically.

The blanket provision to levy penalty on global turnover disregards the separateness of a legal entity. An entity in a group which has no role in any breach, would be exposed to penalty arising out of an unrelated business activity of another group company. Group companies should be penalised only where they have a direct role in the contravention in question.

Section 83: Offences
The offences under the proposed law should be non-cognisable and bailable. We recommend the punishment of imprisonment should be only for failure to comply with orders of Adjudicating Officer. This measure would be in consonance with steps being taken in India to decriminalise offences under other laws such as the Companies Act, 2013.

Section 91: Act to Promote Framing of Policies for Digital Economy

The Bill empowers the central government to direct any data fiduciary/ processor to share anonymised data or non-personal data to enable better targeting of delivery of services. Given that anonymised personal data and non-personal data are not connected with the right to privacy, they should not have been included in the Bill.

The very objective of the Bill is the regulation of personal data, which is at odds with the apparent intent behind Section 91(2). This is because the policy objectives of personal data protection are fundamentally different from non-personal data. The former is premised upon protecting the privacy of individuals, while the latter is driven by very different considerations depending on the type of non-personal data involved, e.g. ownership and commercial interests in the case of intellectual property and trade secrets, etc. A policy to regulate non personal data would require distinct considerations and deliberations of each of the different types of non-personal data, and therefore cannot form a part of this Bill. We recommend deleting Section 91(2) from the Bill.

Chapter 6: Transparency and Accountability Measures

More guidance is required to enable firms to practically achieve transparency and accountability measures laid out. Other factors to be considered include the intended role of the data protection officer to assess and review activities related to data processing. Our concern is that the role of the DPO in overseeing data processing suggests a level of management of the process and continuous approach that couldn't realistically be achieved by the DPO.

We submit that this should be substituted with something like "provides advice to functions processing data on how to monitor compliance and acts as a point of escalation". Firms should also be allowed to approach the governance role of the DPO tailored to how a firm organises its data processing functions rather than suggest a one-s-fits-all checklist of activities.

Further clarity on the interaction between the responsibilities of a data fiduciary and a data processor would also be welcome, specifically to define the situations where a data processor would bear all or partial liability in case of breach of the requirements under the Bill. For example, it would be challenging to operate commercially in an environment where data fiduciaries who 1) issue appropriate instructions to data processors; 2) have appropriate contractual terms in place with such processors; and 3) have appropriate programs for auditing compliance with such terms, nevertheless bear sole liability in the event that such processors breach their contractual terms or do not comply with the instructions of the data fiduciary. In such circumstances, Chapter 6 should clarify that at minimum, recovery through contractual terms would be permitted.

Other Specific Concerns

Grounds of Processing of Personal Data and Consent Managers (S.5, 6, 12-15, 21 & 23):

- Apart from consent, the Bill allows other grounds for processing personal data including processing that is necessary for "reasonable purposes" as specified by regulations after taking into consideration the interest of the data fiduciary, public interest and reasonable expectation of the Data Principal, etc., which scope may include prevention and detection of unlawful activities and processing of publicly available personal data.
- It is unclear if the processing activities based on "reasonable purposes" as permitted under Section 14 applies to sensitive personal data. Given Section 11(3) requires consent to be explicitly obtained for processing of sensitive personal data, clarity is therefore needed to avoid doubt or inconsistency. We note that apart from consent, many overseas data protection laws including the GDPR (see article 9) allow other grounds for processing sensitive personal data.

Obligations, Rights and Accountability:

- *Consent Manager:* The Bill introduces the concept of "consent managers", who appears to be the proxy of a Data Principal, enabling him (irrespective of mental or physical capacity) to gain, withdraw, review and manage consent. They need to be registered with the future DPA (s. 21 & 23 of the Bill). We submit that such requirement is likely to add complexity for entities that collect multiple types of personal data from different sources, and lead to high administrative costs for the future DPA. The appropriateness and feasibility of such mechanism should be re-examined.

- *Annual Audit and Data Trust Score:* One of the imposed obligations for "significant data fiduciaries" include an annual audit by independent auditor on their policies and conducts as well as record keeping, appointment of data protection officer and performance of data protection impact assessment (s. 27-30 of the Bill). Furthermore, the independent auditor may assign a rating or data trust score to a "significant data fiduciary", which will be made transparent in the DPA's website (s.49). Entities are required to be transparent about the rating and score and include such information in their notice to Data Principals (s.7 of the Bill). However, there is no appeal channel available to challenge the scoring or rating.

  When compared with the voluntary certification scheme under the GDPR, while also bearing in mind that the GDPR certification is valid for three years, the obligation of a mandatory annual audit under the Bill appears too onerous. Another question is how such scoring mechanism will interact with the cross-border transfer mechanism. It is not clear whether certified organisations will be allowed to transfer personal data overseas as permitted under the GDPR regime. While the certification mechanism is still at development stage in different parts of the world, we recommend these proposed requirements be re-considered.

IMPLEMENTATION

Grandfathering clause

We recommend the provision of a grandfathering clause so that data fiduciaries may rely on consents, that have already been obtained, and that any data transfer/data localisation requirements should not apply to data that has already been transferred, before the Act becomes effective.

Timelines for Transition

Under the PDPB-2018, Section 97 provided timelines for transition. The current Bill does not expressly provide any timelines for implementation. We submit that as the PDPB will introduce new concepts and compliance requirements will have to be understood and the infrastructure of controls will have to be implemented by Data Fiduciaries and Data Processors to be compliant with law, this factor needs to be considered and adequate timelines be provided for the law to be deployed.

Clarification

Prior to implementation, we specifically request the following important clarifications:

- It is not clear in the PDPB as to what would make a data fiduciary "significant", and we would be grateful for a descriptive definition as that would be of assistance.
- It appears that all types of personal data breaches, provided they involve personal data processed by a data fiduciary, will have to be reported to the Authority for assessment for further reporting to the Data Principal. This process may prove to be onerous. If this is considered for inclusion in the law, we would be glad to offer assistance with the assessment of guidelines on the reporting process if they can be provided to us for the purpose.

- As regards the data protection impact assessment requirement, we request clarity as to the criteria regarding "use of new technologies" or "large scale profiling criteria", what would be within the scope of "large scale profiling", and what is the threshold for "large" scale. As this involves the reporting of the assessment results by the DPO to authority, so we need more clarity.

With reference to the requirement that an independent data auditor perform annual audits (for a significant data fiduciary), we submit to seek more clarity that whether such auditor of necessity have to be a third party, or whether an independent control function from within the data fiduciary's organisation would be able to fulfil the functionality.

ASIFMA would appreciate further opportunities to engage in-person with the JPC on the PDPB and its potential impact on the banking and financial services industry in India. Should you have any further questions or would otherwise require any further information, please contact me (mausten@asifma.org or +852 2531 6510) or Matthew Chan, ASIFMA's Head of Policy and Regulatory Affairs, at mchan@asifma.org or +852 2531 6560.

Sincerely,

Mark Austen
Chief Executive Officer
Asia Securities Industry & Financial Markets Association

Kenneth E. Bentsen, Jr.
President and Chief Executive Officer
Securities Industry & Financial Markets Association