asifma

Growing Asia's Markets

28 September 2018

Joint Secretary
Ministry of Electronics and Information Technology (MeitY)
Room No. 4016, Electronics Niketan,
6 CGO Complex, CGO Complex,
Lodhi Road,
New Delhi – 110 003.

Dear Madam/ Sir,

Re: ASIFMA Response to the Draft Personal Data Protection Bill, 2018 ("PDPB")

The Asia Securities Industry & Financial Markets Association ("**ASIFMA**")[1] welcomes the opportunity to comment on the draft data protection regime for India. ASIFMA and its members would like to sincerely thank Kriti Trehan (Partner), Law Offices of Panag & Babu for providing support and guidance on Indian law and policy around privacy and data protection. We have set out in this letter our comments to the provisions of the PDPB.

India is a key participant in the international banking ecosystem, and it excels as an outsourcing location for global banking (and non-banking), thanks to the considerable technological expertise available there. As a net importer of data, India is therefore uniquely positioned to be a global leader in setting data protection rules.

Financial services are highly regulated, with both the Reserve Bank of India ("**RBI**") and the Securities and Exchange Board of India ("**SEBI**") regulating and prescribing strict compliance vis-à-vis "client confidentiality." Any cross-sector data protection regime should therefore carefully consider provisions being drafted to ensure harmonisation and uniformity with existing rules, or existing rules will need to be harmonised or revoked to avoid inconsistencies.

[1] ASIFMA is an independent, regional trade association with over 100 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.

ASIA SECURITIES INDUSTRY & FINANCIAL MARKETS ASSOCIATION | Unit 3603, Tower 2 Lippo Centre | 89 Queensway Admiralty, Hong Kong | Tel: +852 2531 6500 www.asifma.org

To ensure that the best possible data protection regime is adopted, ASIFMA would appreciate further time and opportunities to more fully engage with India's authorities on these proposals, either through consultations or in direct meetings. If you have further questions or would otherwise like to follow up, please contact Wayne Arnold, ASIFMA's Executive Director and Head of Policy and Regulatory Affairs, at warnold@asifma.org or +852 2531 6560.

Sincerely,

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

GENERAL COMMENTS

- ASIFMA welcomes the regulatory initiative in India to create a dedicated data protection and privacy statute. India is a key player in the global technology ecosystem, including banking, and is therefore uniquely positioned to establish its own practices and procedures around ensuring privacy and protection of data.

- The PDPB is, for the most part, a great stepping stone to engage with industry. It identifies various relevant issues that any good privacy and data protection regime should address, and with expanded consultation with industry, the PDPB has the potential to become formidable guardian of personal data for the common person.

- As the honourable Ministry for Electronics and Information Technology, Government of India ("**MEITY**") is astutely aware, financial services are the subject of comprehensive sectoral regulation by, *inter alia*, the RBI and SEBI. Under such sectoral regulation, regulated entities are required to comply with requirements regarding protection of customer confidentiality. A wider, sector agnostic regulation, such as the PDPB, would best serve the cause of privacy and data protection so long as it establishes clear guidelines around uniformity and harmonisation between its own diktats and those of the sectoral regulators.

DETAILED COMMENTS

1. Scope and Applicability of PDPB

1.1 Section 2 of the PDPB sets forth a wide scope of applicability for the legislation. ASIFMA believes that in line with principles of jurisdictional sovereignty, the provisions of the PDPB should be applicable only to such entities that collect and conduct processing activities within India in relation to personal data/ sensitive personal data/ critical personal data of natural persons resident in India. In the interest of affording an adequate degree of protection to customer data, such a provision would also regulate the process of transferring such data out of India, as opposed to regulating processors in a different jurisdiction. Limiting the scope of the provisions to transfer processes would also ensure alleviating the enforcement costs and concerns that would accompany any legislative controls sought to be enforced extraterritorially without adequate diplomatic/ bilateral frameworks in place. Additionally, data which is protected under any offshore legislation should stand excluded from the PDPB regime (see paragraph 1.2 below). ASIFMA also recommends that data from heavily regulated sectors (such as the financial sector) which is located in low-risk and well-regulated jurisdictions should also be excluded from extraterritorial applicability of the PDPB.

1.2 India, as a fairly versatile outsourcing economy, would be prudent in structuring the extraterritorial applicability of the PDPB accordingly. By way of illustration, the Philippines, which is also a strong outsourcing jurisdiction, exempts data processors from compliance with the domestic data protection law in instances where data is collected from residents of foreign jurisdictions (i.e. outside of the Philippines) in accordance with the data protection laws of such foreign jurisdiction.[2] A similar clarification could be imported into the proposed Indian legislative framework as well.

1.3 Separately, it would be prudent to clarify how provisions of the PDPB apply in a Business-to-Business ("**B2B**") context (e.g. in the context of intragroup outsourcing arrangements) and where B2B data is specifically exempted. The spirit of the PDPB, generally speaking, is the protection and privacy of the data of data principals within India, who is the end user or consumer or customer, and it would be useful if the provisions specifically lend clarity to this as well by eliminating B2B from the realm of the PDPB to ensure that no data, which does not relate directly to data principals, is captured within the scope of the legislation. Additionally, ASIFMA particularly recommends that Section 3(14) be amended to reference the provision bearing the definition of Personal Data correctly - i.e. reference be made to Section 3(29) and Section not 3(28) of the PDPB.

1.4 Furthermore, from a logistical and enforcement perspective, we recommend that information pertaining to short term visitors (including but not limited to visiting employees) should be exempt from the purview of the PDPB.

[2] See section 4(g) of the Philippines Data Privacy Act of 2012 available **here**.

1.5 Additionally, the applicability of the PDPB and obligations thereunder appear to apply uniformly in most part to both data fiduciaries and data processors, despite a clear definitional distinction having been drawn between the two. ASIFMA requests that clarity be provided on the responsibilities of fiduciaries and processors separately, specifically clarifying that the fiduciaries have primary responsibility in complying with the PDPB and in particular processors are jointly responsible for the specific obligations detailed in Sections 31 (Security Safeguards) and 37 (Processing by entities other than data fiduciaries).

1.6 Finally, given that sectoral regulators like the RBI and SEBI already regulate the financial sector, including on questions of data protection, we recommend that sectoral regulators be invited to add the necessary nuances that are unique to the financial sector. The sectoral regulators should continue to be the nodal regulatory authorities for the financial sector, and should therefore be empowered to monitor regulatory compliance. This clear demarcation would help avoid the multiplicity, undue complexity and possibly inconsistency of regulation.

2. Sensitive and Critical Personal Data

2.1 The definition of *sensitive personal data or information*, under the presently applicable regime of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**2011 Rules**"), for most part adequately classifies sensitive information. ASIFMA recommends that the PDPB retain the spirit of the definition from the 2011 Rules.

2.2 We note that there are significant departures within the PDPB definition of sensitive personal data from applicable laws across jurisdictions, including the European Union General Data Protection Regulation ("**EU GDPR**"). Passwords, official identifiers and financial data should not fall within the purview of sensitive personal data. Additionally, the definition of sensitive personal data is open-ended as it includes any other category of data specified by the regulator under Section 22 of the PDPB. This inclusion will not only create uncertainty for the processing of personal data but will also create unrealistic expectations on data fiduciaries and processors who will have to stop processing already collected data that is subsequently deemed to be considered sensitive and will overburden data fiduciaries and processors to seek and data principals to provide explicit consent after the collection. We, therefore, recommend the deletion of the above inclusion. While ASIFMA can understand the rationale for such data to constitute sensitive personal data for non-financial institutions or affiliates, in the context of regulated financial services entities in the business of processing financial data on a daily basis, the PDPB approach would effectively supersede applicable RBI and SEBI supervision on confidentiality and information security.

2.3 ASIFMA, within this backdrop, specifically recommends removing financial data from the definition of sensitive (or, by extension in some instances, critical) personal data. Given the truly multinational nature of the financial sector, subjecting financial data to a regime inconsistent

with global regulation would pose severe implementation challenges for multinational corporations within the sector. Furthermore, the financial sector in India already finds itself heavily regulated, and adding cumbersome compliance requirements are both unnecessary and detrimental to ease of conducting business. To alleviate any concerns MEITY may have on security arrangements for such data, ASIFMA suggests that instead of including passwords, official identifiers and financial data in the definition of sensitive personal data, these items could simply be listed in Section 31 as types of data that data fiduciaries should take particular consideration of for the purposes of that provision.

2.4 Separately, on the issue of critical personal data, we note challenges in the language of Section 40(2), especially where the regulator is empowered to notify and expand the categories of critical personal data, which will then necessarily be required to be located within India as this will create significant legal uncertainty. Businesses that are considering establishing or maintaining business operations in India will have no way of knowing whether they will be impacted by future notifications in that regard. At a minimum, this broad authority should be explicitly limited to extraordinary circumstances and embedded within processes open to public consultation. Section 40 should also expressly require that any such notification should only apply to new data collected after a specified transition period, and not to data that has already been collected. ASIFMA strongly urges the Indian authorities to consider the cripplingly adverse business impacts of uncertain regulation generally, and the negative business effects this could have on the financial sector with an extraterritorial interface.

3. Grounds for Processing Personal/ Sensitive Personal Data

3.1 *Processing personal or sensitive personal data in compliance with a judicial order*: The grounds under Sections 14 and 20 of the PDPB are extremely narrow, and the legal basis for processing personal or sensitive personal data should include permission to process and transfer such data where it is necessary for the establishment, exercise or defence of legal claims. For clarity, claims would include contractual or legal claims within a judicial, administrative or out-of-court procedure, including procedures before tribunals, regulatory bodies or an arbitration. By way of example, this would include processing for criminal investigations, competition law investigations, investigations around insider trading etc., processing related to pre-trial discovery processes, as well as processing in public interest, including within the context of anti-money laundering, cyber-crime, terrorism financing etc. By way of corollary, the exemption granted under Section 44 of the PDPB should also extend to regulatory claims and administrative procedures.

3.2 *Processing personal data for employment purposes*: We recommend that this ground be expanded to include data pertaining to pre-screening of potential employees, as well as information pertaining to non-regular personnel, including part-time staff, labour (contract or otherwise), external consultants etc.

3.3 *Legitimate/ public interest and processing personal or sensitive personal data*: In line with the recommendations above, there must specifically be a carve out for processing personal and sensitive personal data with a legitimate interest. The legitimate interest purposes for processing personal and sensitive personal data should expressly include, as mentioned above in para 3.1, processing data in context of foreign regulatory requests and investigations, as well as on grounds of preventing money laundering, cyber-crime, terrorism financing etc.

3.4 *Processing of data for reasonable purposes*: Currently under the PDPB, the "reasonable purposes" ground is considered as a residual ground on which personal data may be processed for the limited rigid list of processing activities determined by the regulator. Firstly, we recommend that the reasonable purposes ground should be considered to be on equal footing with consent and not a residuary ground. All processing grounds should be placed on equal footing and data fiduciaries should be able to select the ground which is most appropriate for a specific processing operation. Consent should not be the default processing ground and is unlikely to be suitable for many modern-day processing operations. Secondly, the reasonable purposes ground should not be limited to a rigid list of processing activities determined by the regulator. There may be circumstances when organisations need to collect, use or disclose personal data without consent for a legitimate purpose apart from those authorised by the regulator. Examples of reasonable purposes are welcomed and the regulator can spell out which types of processing activities may fall under this ground under guidelines, but this should not be exhaustive. The essence of this processing ground is that it must be future-proof and adaptable to new processing operations by virtue of its risk-based approach that allows the data fiduciary or processor to precisely assess and deal with the specific risks at hand regardless of the nature of the technology or business practice. Such a balancing test ensures the security of privacy rights for individuals. Having the regulator produce such guidelines rather than hardwiring them into primary legislation will also permit protections where they are most needed (e.g. in respect of consumers) while providing flexibility in B2B scenarios. Finally, in line with global developments around privacy frameworks, ASIFMA recommends that *reasonable purposes* be renamed with the nomenclature *legitimate interests*.

3.5 *Expanding the grounds for processing sensitive personal data*: Generally speaking, the grounds for processing sensitive personal data under the PDPB are extremely restrictive, and would potentially impact the ability of businesses to innovate and create solutions in the best interest of the data principal. The PDPB may, therefore, be amended to expand the scope of processing sensitive personal data on grounds and in a manner similar to that which is permissible for personal data. Specifically, processing of sensitive personal data for reasonable purposes (as is the case for personal data under Section 17 of the PDPB) with the modifications recommended above) and employment should be permissible. We understand that MEITY may have concerns in this area and we would be willing to engage further on this matter to ensure a reasonable outcome for both MEITY and the financial services industry.

3.6 *Notice and consent*: ASIFMA recommends that the PDPB not mandate notice and consent requirements in instances where the source of data is not the data principal herself. A blanket

requirement of notice and consent to all data principals, when they are not the sources of data, would be impractical (and in many instances impossible) when dealing with institutions/ corporations/ trusts as there is no direct relationship with the underlying representatives. This will also pose logistical and practical challenges around administration, tracking and monitoring of such notice and consent. This blanket requirement may also result in stifling India's growing artificial intelligence (AI) and big data industry for the same reasons stated above.

4. Data Principal Right – Right to Data Portability

4.1 ASIFMA applauds the PDPB in having the foresight to proactively create a rights-based framework for data principals to have the ability to port their data seamlessly. However, the language suggested in Section 26 (1) (a) (iii) of the PDPB, where this right extends to personal data "*which the data fiduciary has otherwise obtained*" is extremely broad, and leaves the provision without guidance or a harness. We, therefore, recommend deleting this portion from the provision.

4.2 Additionally, the purpose of a data portability provision is to ensure convenience and utility for data principals when, for instance, switching service providers. Therefore, to the list of exemptions, it would be prudent to add employee and contingent labour data or other instances where the data fiduciary is not acting as a service provider.

4.3 Finally, we recommend that the PDPB creates a specific exemption for data processed for *reasonable purposes*. The PDPB, under Section 17, recognises reasonable purposes to include *inter alia* fraud detection and prevention, and network and information security. Enabling portability of such data could have a significant adverse impact, and would weaken, internal processes concerning the above-mentioned activities.

5. Data Protection Impact Assessment

5.1 Section 33 of the PDPB requires that any processing that involves new technologies or large-scale profiling of sensitive personal data (such as biometric or genetic data) or any other processing which carries a risk of significant harm to data principals, should be preceded by an impact assessment by the data fiduciary.

5.2 This provision is found excessive, especially where the use of new technologies requires an impact assessment. A clear and defined determination in law, of what constitutes a new technology, is impossible. Therefore, the requirement of an impact assessment is disproportionate to the potential innovation and business interests.

5.3 Any impact assessment, it is recommended, should solely be on the basis of the link between the processing activity, the specific risk of harm and benefit to the data principals, and not based on the activity itself. This is important because any mitigations and controls for the identified risk might also reduce or remove the benefits. There should be acknowledgement of the

relevance of benefit assessment in the context of risk assessment. The language in the provision should therefore be updated accordingly. Regulated entities already incorporate risk assessments as part of new product approvals and so do not need additional rules which may require even more compliance resources to satisfy.

5.4 The requirement to submit every data protection impact assessment to the proposed Data Protection Authority ("**DPA**") appears to have the potential of creating a logistical challenge with the DPA inundated unnecessarily with such impact assessments. We, therefore, recommend that any submission of a data protection impact assessment to the DPA should be done on a case-by-case basis where the assessment determined a high level of residual risk to data principals, i.e. instances where the risk to the data principals remains high after the application of controls to mitigate those risks are considered. This approach appears to be consistent with the global practice, including that under the GDPR. Recital 89 of the GDPR particularly calls out the financial and administrative burdens of past general reporting requirements, without improving the level of protection, as regards the processing of personal data.

6. Data Audits

Data fiduciaries, under Section 11, are responsible for compliance with the provisions of PDPB. While this principle is laudable, the requirement and process of data audits under Section 35 is extremely prescriptive. It is important that the data fiduciary exhibits and evidences compliance – the means and method of illustrating compliance should be at the discretion of the data fiduciary itself, at least for regulated entities who have existing auditing processes and should not suffer the regulatory limitations of a prescriptive independent annual audit. ASIFMA also suggests that audits needs not be annual but could be bi-annual or triggered where there is a material change to applicable laws.

7. Data Protection Officer

Section 36 of the PDPB requires that data fiduciaries appoint a Data Protection Officer ("**DPO**"), and that such DPO should be physically located in India. Given the multinational nature of businesses, it may not always be feasible for the DPO to be located in India. Instead, the provision may require that the DPO be accessible for the purposes identified in the PDPB, regardless of her location.

8. Significant Data Fiduciaries

8.1 Section 38 of the PDPB empowers the DPA to notify certain data fiduciaries, or classes of data fiduciaries, as significant. Significant data fiduciaries may be determined as being significant based on the volume and sensitivity of personal data processed, turnover of data fiduciary, risk of harm that may result from processing activities, use of new technologies, and any other factor that harm data principals as a result of processing.

8.2 This provision is another example of the high level of discretionary powers allotted to the DPA, which in itself is a brand-new regulatory body that will be constituted upon the PDPB being notified as binding legislation. Additionally, the scope of what may be a significant data fiduciary is extremely broad and open-ended. We draw specific attention to the provision whereby the use of new technologies may, *inter alia*, be the enabling reason to be designated a significant data fiduciary, which would further increase the burdens of compliance requirements on such data fiduciary. The intent of this provision is unclear, and ASIFMA recommends that this nomenclature of significant data fiduciaries be considered for deletion from the PDPB at least in respect of regulated entities. There is little benefit to entities that are regulated financial institutions and already subject to extensive supervisory oversight in India from being subject to additional requirements with a DPA.

9. Data Localisation and Cross-Border Data Transfers

9.1 Sections 40 and 41 of the PDPB outline restrictions and requirements around the location and transfer of personal and sensitive personal data. We note that the position propounded by the PDPB, as well as the recent RBI circular (on local storage of payments systems data), is rather draconian in requiring copies or originals of certain categories of data to be maintained on servers physically located within India. Research suggests no causal link between local storage of data and data protection imperatives.[3] However, data localisation may result in significant costs and unintended consequences, like loss of time and resources in setting up new data centres, tweaking network architecture, or using local cloud vendors. As noted in the "APEC Roadmap for a New Financial Services Data Ecosystem"[4], there is a substantial negative impact in jurisdictions such as Indonesia, South Korea and China that have enacted or proposed data localisation of an average of -0.7 percent of GDP. The concerns regarding data localization are real and legitimate. For India, instead of requiring data localisation, any underlying policy concerns should be addressed through a regional and global network that allows for the exchange of information, cross-border enforcement and cooperation among jurisdictions. It may be prudent to bear in mind that any data located overseas will be protected under the conditions of Section 41 of the PDPB and standard contractual clauses.

9.2 From the perspective of business interests, it must be remembered that India has a burgeoning outsourcing industry which handles, *inter alia*, data from global sources. Given that India is home to such outsourcing offices, which require that data be transferred to *and subsequently*

[3] Analysys Mason. "Data-driven innovation for emerging Asia-Pacific: supporting economic transformation, protecting consumers." 6 September 2016.
http://report.analysysmason.com/DDI_Emerging_APAC/DDI%20in%20emerging%20APAC%20-%20Final%20report%20-%202016%2008%2006%20-%20FINAL.pdf

[4] Asia-Pacific Economic Cooperation (APEC) and APEC Business Advisory Council. "Financing Asia-Pacific Integration in the Digital Age: An APEC Roadmap for a New Financial Services Data Ecosystem (2018 Progress Report)." Page 19.
https://www2.abaconline.org/assets/2018/AGFSCB_Key_Documents/Attachment_A_An_APEC_Roadmap_for_a_New_Financial_Services_Data_Ecosystem.pdf

from India, it may not be logistically and legally possible for overseas entities to locate data within India due to logistic and legal impediments of then extracting such data. Localisation requirements could also create challenges for Indian start-ups going global to leverage global storage platforms. There is likely to be a negative impact on the growth of new technologies such as cloud computing, which will likely be stunted in a restrictive regulatory environment.

9.3 Data localisation has globally been known to hamper business growth. Particularly within the context of the financial sector, data localisation may inhibit sectoral growth and development for the following reasons:

- It would disrupt communication between a company's local office and its global operations;
- It would raise the cost of doing business significantly;
- It would prevent the company from providing seamless global service to Indian customers; and
- It would put Indian enterprises at a competitive disadvantage with other countries that embrace the digital economy.

Measures like localisation norms are counterproductive, as they fragment the global operations of firms. They not only create, but also increase cybersecurity risks, while inhibiting cross-border trade and investment. Without prejudice to the significant harm caused by localisation requirements generally, such measures are especially counterproductive where the data principals themselves are located outside India (see our earlier comment regarding the approach taken in the Philippines). Data replication also poses significant operational challenges and creates legal uncertainty on many issues.

9.4 We recommend that in this era of globalisation, and given that irrespective of data being stored overseas, the PDPB allows the regulator to enforce a data privacy breach if it has nexus to India, the businesses should have the ability to select local or global centres for data storage and processing. As a reasonable middle ground, if localisation is insisted upon, mirroring possibilities should be considered by the regulator, and undertakings may be made for the provision of data to authorities within a specified timeframe (e.g. 72 hours) as part of an ongoing investigation and pursuant to a valid legal order. Specifically, from the perspective of the financial sector, ASIFMA recommends –

- Financial services sector companies have specified regulators (RBI, SEBI, IRDA). Such regulated entities may be permitted to inform such regulator of the location of data, and specify availability of inspection/ audit rights of such regulator over such location.
- The DPA, as contemplated, may also be kept informed of the regulatory intimation/ permission, and provided details of data storage location.

- The regulators can adopt a differentiated approach whereby all data stored in 'approved' locations (say USA, EU, UK, Singapore etc.) is exempted from these provisions as compared to high risk locations (to be specified) where it would not be permitted.
- The regulators can allow data to be stored in countries where they have unfettered access under inter-regulator protocols that are in place and apply the provision of the PDPB only to the locations where such protocols don't exist.

9.5 We note another concern with localisation imperatives – data localisation undermines the effectiveness of a financial institution's international risk monitoring programme. For example, compliance with anti-money laundering laws and sanctions requires a comprehensive and holistic approach, whereby quantification of risk encompasses a customer's entire relationship across a financial institution in a location agnostic manner. Aggregation of data on a clients' activity across borders allows a holistic assessment of the client's global activity for better informed decision making, and creation of national silos of information prevents the seamlessness of such programmes, while, at the same time, negatively impacting seamlessness of user experience.

9.6 The PDPB, it is recommended, should permit transfers of all kinds of data, without the proposed limitations on categories of sensitive or critical personal data. The movement and storage of data across national borders is essential to providing cross-jurisdictional and core products and services to customers, including executing trades in global markets. It is also fundamental to manage risks across affiliates and borders, and comply with financial regulatory requirements across jurisdictions (including those related to Know-Your-Customer and anti-money laundering laws). Transfer of data is also uniquely important to India, as illustrated above in para 9.2, from an outsourcing perspective.

9.7 Section 41 of the PDPB particularly states that transfers may be made subject to (1) standard contractual clauses, or (2) intra-group schemes, or (3) to permitted countries or international organisations, or (4) where transfers are specifically permitted on grounds of necessity. However, the provision also requires that standard contractual clauses, intra-group schemes, or permitted countries/ international organisations, in addition to requiring DPA approval, should be accompanied by the data principal's consent (for personal data) and explicit consent (for sensitive personal data). Regulatory approval and data principal's consent, and the requirement of both together, appear excessive. Furthermore, with respect to (a) standard contractual clauses, we recommend against the use of non-modifiable standard clauses and the DPA pre-approval requirement because data flows occur within varying and specific business context and hence, parties to a transaction must remain free to use contractual language that suits their specific business needs and information flows (e.g. financial services will have different requirements to other industries for instance) while also imposing the appropriate data privacy and security obligations applicable to the data; and (b) intra-group schemes, we recommend not be subject to regulatory approval, since these processes are limited to transfers within the affiliates of local or multinational data fiduciaries, and should therefore not require specific approval from the DPA.

9.8 It is unclear from the language of Section 41 of the PDPB if the content of standard contractual clauses shall be prescribed by the DPA/ delegated legislation, or guidance on the contours of what may constitute approved contractual clauses. With no clarity on what the basis of granting approval would be, there remains uncertainty within the industry, and ASIFMA recommends that the PDPB appropriately address this issue. Direction around the applicability of Section 41 to data fiduciaries and data processors, and what requirements apply to which, would be useful as well.

10. Additional concerns

10.1 Data Fiduciary versus Data Controller: Unlike other jurisdictions, the PDPB refers to a 'data fiduciary' where in other jurisdictions the term "data controller" is almost exclusively used. This departure from standard nomenclature may create undefined fiduciary obligations and liabilities on the data controllers, which may cause contractual uncertainty. ASIFMA, therefore, recommends that all reference to *data fiduciaries* be changed to identify with the global standard term *data controllers*.

10.2 Penalties: For penalising non-compliance with Indian data protection and privacy laws, it is unreasonable to link global turnovers to domestic violations. Such a regulation would distort global economic flows and commercial imperatives. We recommend specifying monetary amounts and caps with a direct correlation with the harm done/ violation, as opposed to global turnovers and financial capabilities. While such an approach has been adopted in the EU under the GDPR, ASIFMA notes that the EU has benefitted from 20 years of data protection regulation with penalties that were much lower than those proposed under the PDPB. Legislation as far reaching as the PDPB will inevitably result in a high number of initial breaches as a culture of compliance develops in India. Rather than setting turnover-based penalties, MEITY and the DPA should consider alternative processes such as private (and eventually public warnings, and other fines) with a view to more robust penalties at a later stage once the DPA is a more established entity.

10.3 Consent: The PDPB requires that data be processed pursuant to appropriate consent. The validity of consent is dependent upon a wide variety of conditions (free, informed, specific, clear, capable of being withdrawn – with varied degrees for processing personal and sensitive personal data separately). To fulfil the requirements elucidated in, and to ensure compliance with, the PDPB, the data controllers/ fiduciaries/ processors will necessarily need to invest heavily in adequate and expensive infrastructure. Despite these costs, the burden to prove valid consent has been placed on the controllers/ fiduciaries/ processors. This provision has the potential of being widely misused. ASIFMA recommends that the discharging the burden of proof, as is a fundamental principle in law, should be on the shoulders of she who contests the consent and its validity.