asifma
Growing Asia's Markets

31 January 2018

Justice B.N. Srikrishna
Chairman, Committee of Experts
C/o Shri Rakesh Maheshwari
Scientist G&Group Co-ordinator, Cyber laws
Ministry of Electronics and Information Technology (MeitY),
ElectronicsNiketan, 6, CGO Complex,
Lodhi Road, New Delhi- 110003.

Dear Justice B.N. Srikrishna,

Re: ASIFMA response to the White Paper of the Committee of Experts on Data Protection Framework for India

The Asia Securities Industry & Financial Markets Association (ASIFMA) welcomes this White Paper and the opportunity to comment on the proposal for a new data protection regime for India. India 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. We have set out in this letter our comments in response to the proposals in the paper.

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

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

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

GENERAL COMMENTS

- ASIFMA welcomes this White Paper and the opportunity to comment on the proposal for a new data protection regime for India. India 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.

- The White Paper is accordingly comprehensive. As a result, and in order to ensure 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. In the meantime, we have set out the comments we were able to obtain from our members.

- 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 will therefore need to be carefully drafted to ensure harmonisation with existing rules, or existing rules will need to be harmonised or revoked to avoid inconsistencies. We suggest further consultations in this regard.

- Despite the highly cross-border nature of data flowing into India, the current data protection regulations (i.e. the SPDI rules) are silent on how requests for client information/data of India clients, or from regulators in other jurisdictions, are to be dealt with. Rule 6 states the client data (including SPDI) can be shared, without obtaining client consent, with Government agencies. ASIFMA is of the view that this exception should be carried over to the new proposed data protection law ("Proposed Law").

SCOPE AND EXEMPTIONS

1. Territorial and Personal Scope

1.1. What are your views on what the territorial scope and the extra-territorial application of a data protection law in India should be?

- The Proposed Law should apply to data processing activities conducted in India rather than to the personal data of Indian residents or citizens. This will afford consistent application of the law to all activities conducted in India. This would also ensure an adequate degree of protection, as the act of transferring such data out of India would then be subject to the data protection principle on third-country transfers, but third-country processors would not be subject to Indian laws.

1.2. To what extent should the law be applicable outside the territory of India in cases where data of Indian residents is processed by entities who do not have any presence in India?

- The Proposed Law should be territorial, i.e. limited to the processing (including collection) of personal information in the territory of India by entities that have a presence in India.
- The Proposed Law should specifically exempt application of any local law to data coming into India from a data controller located offshore for processing, subject to the processing of the foreign data being in compliance with the laws of the data controller's home jurisdiction. Further, the Proposed Law should exempt short-term visitors to India (such as visiting employees) from the scope of the Proposed Law.

1.3. While providing such protection, what kind of link or parameters or business activities should be considered?

Alternatives:
a. Cover cases where processing wholly or partly happens in India irrespective of the status of the entity.
b. Regulate entities which offer goods or services in India even though they may not have a presence in India (modelled on the EU GDPR)
c. Regulate entities that carry on business in India (modelled on Australian law), business meaning consistent and regular activity with the aim of profit.

- ASIFMA's view is that Alternative A (Cover cases where processing wholly or partly happens in India irrespective of the status of the entity) is most appropriate given India's status as a net data importer. Options B and C may create significant barriers to India's competitiveness as an outsourcing services provider. Regardless, any such decision could be revisited in the future (noting that the GDPR itself took effect almost 20 years after the original EU Data Protection Directive).

1.4. What measures should be incorporated in the law to ensure effective compliance by foreign entities inter alia when adverse orders (civil or criminal) are issued against them?

- If the Proposed Law is to apply only to activities conducted in India, this issue should be of secondary importance: any breaches would be conducted by entities already operating within the jurisdiction

of India's authorities. ASIFMA does not believe that the mandatory establishment of a representative office would be a proportionate response.

1.5. Are there any other views on the territorial scope and the extra-territorial application of a data protection law in India, other than the ones considered above?

2. Other Issues of Scope

2.1. What are your views on the issues relating to applicability of a data protection law in India in relation to: (i) natural/juristic person; (ii) public and private sector; and (iii) retrospective application of such law?

- The subject matter of the Proposed Law should be limited to data relating to individuals. Information concerning corporate entities is not "personal data," but may instead constitute confidential or otherwise protected information. We recommend such information be protected as appropriate under established legal rules on confidentiality, trade secrets, etc. (including any applicable regulations).
- ASIFMA recommends that the Proposed Law apply equally to the public and private sector, but that the scope of available exemptions and guidance on application of the data protection principles make appropriate distinctions. The Proposed Law should recognise both "data controller" and "data processor."

2.2. Should the law seek to protect data relating to juristic persons in addition to protecting personal data relating to individuals?

Alternatives:
a. The law could regulate personal data of natural persons alone.
b. The law could regulate data of natural persons and companies as in South Africa. However, this is rare as most data protection legislations protect data of natural persons alone.

- As noted above, we agree with Option A. Company data may be subject to contractual, common law, regulatory obligations of confidentiality, or otherwise subject to intellectual property protections (e.g. in the case of trade secrets). But ASIFMA does not consider it appropriate to conflate these protections into a personal data regime.

2.3. Should the law be applicable to government/public and private entities processing data equally? If not, should there be a separate law to regulate government/public entities collecting data?

Alternatives:
a. Have a common law imposing obligations on Government and private bodies as is the case in most jurisdictions. Legitimate interests of the State can be protected through relevant exemptions and other provisions.
b. Have different laws defining obligations on the government and the private sector.

- ASIFMA agrees with Option A. We recommend the Proposed Law apply equally to the public and private sector, but that the scope of available exemptions and guidance on application of the data protection principles make appropriate distinctions. This will provide comfort to banks that when data is provided to a government agency, that data will be protected to a certain standard.

2.4. Should the law provide protection retrospectively? If yes, what should be the extent of retrospective application? Should the law apply in respect of lawful and fair processing of data collected prior to the enactment of the law?

Alternatives:
a. The law should be applicable retrospectively in respect of all obligations.
b. The law will apply to processes such as storing, sharing, etc. irrespective of when data was collected while some requirements such as grounds of processing may be relaxed for data collected in the past.

- ASIFMA strongly recommends that the Proposed Law not have retrospective application to issues relating to consents, collection and outbound transfers, as it would be onerous for organisations to try and track down data subjects whose personal data was collected before the passage of the Proposed Law.
- The Proposed Law should provide a minimum period of two years to achieve compliance on all other issues, such as storage, information security, and ensuring that consents are obtained for processing all new data collected after the transition period, etc.

2.5. Should the law provide for a time period within which all regulated entities will have to comply with the provisions of the data protection law?

- ASIFMA recommends a minimum period of two years to ensure compliance (see response above).

2.6. Are there any other views relating to the above concepts?

3. Definition of Personal Data

3.1. What are your views on the contours of the definition of personal data or information?

- ASIFMA proposes that anonymised data be outside the definition of personal data. Issues regarding reversed engineering of anonymised data can be addressed in guidance to ensure easy adjustments as technology develops (with appropriate industry consultation).
- The Proposed Law should retain the existing classification of information as Personal Information and Sensitive Personal Data and Information ("SPDI"). Definitions under the Proposed Law should be very specific and the proposed exceptions should be included.
- Exemptions under various existing laws should be recognised and incorporated into the definitions of the Proposed Law to avoid conflicts.

3.2. For the purpose of a data protection law, should the term personal data or personal information be used?

Alternatives:
a. The SPDI Rules use the term sensitive personal information or data.
b. Adopt one term, personal data as in the EU GDPR or personal information as in Australia, Canada or South Africa.

- As long as the definitions are clear on what is and what is not personal data, ASIFMA does not believe the nomenclature is material.

3.3. What kind of data or information qualifies as personal data? Should it include any kind of information including facts, opinions or assessments irrespective of their accuracy?

- ASIFMA recommends the GDPR concept of data (see question immediately below).

3.4. Should the definition of personal data focus on identifiability of an individual? If yes, should it be limited to an identified, identifiable or reasonably identifiable individual?

- ASIFMA believes identifiability should be the focus of the definition of personal data. The definition should cover identified or reasonably identifiable individuals. Issues regarding reversed engineering or what constitutes "reasonably identifiable" can be addressed in guidance to ensure easy adjustments as technology develops (with appropriate industry consultation).

3.5. Should anonymised or pseudonymised data be outside the purview of personal data? Should the law recommend either anonymisation or pseudonymisation, for instance as the EU GDPR does?

[Anonymisation seeks to remove the identity of the individual from the data, while pseudonymisation seeks to disguise the identity of the individual from data. Anonymised data falls outside the scope of personal data in most data protection laws while pseudonymised data continues to be personal data. The EU GDPR actively recommends pseudonymisation of data.]

- Anonymised or pseudonymised data should not fall within the definition of personal data. Separately, where personal data is collected, the Proposed Law could recommend that such data be anonymised or pseudonymised by the data controller or data processer where reasonably practical. But this may not be possible in all circumstances and ASIFMA recommends that further guidance be issued.

3.6. Should there be a differentiated level of protection for data where an individual is identified when compared to data where an individual may be identifiable or reasonably identifiable? What would be the standards of determining whether a person may or may not be identified on the basis of certain data?

- ASIFMA recommends that issues such as this be dealt with by industry guidance following a separate consultation.

3.7. Are there any other views on the scope of the terms personal data and personal information, which have not been considered?

4. Definition of Sensitive Personal Data

4.1. What are your views on sensitive personal data?

- The current definition of "sensitive personal data or information" as provided in the SPDI rules is sufficiently wide to cover the data for which protection is required.

4.2. Should the law define a set of information as sensitive data? If yes, what category of data should be included in it? Eg. Financial Information / Health Information / Caste / Religion / Sexual Orientation. Should any other category be included?

[For instance, the EU GDPR incorporates racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life.]

- ASIFMA recommends aligning with the EU GPDR on defining sensitive data or information.
- Financial information should not be considered sensitive personal data for the following reasons:
    - Classifying financial information as sensitive personal data would be inconsistent with data protection laws in other jurisdictions and would lead to challenges in implementation as most organisations operate globally;
    - Financial information is already heavily regulated by industry-specific laws and regulations, so adding financial information to sensitive personal data would be cumbersome and unnecessary.

4.3. Are there any other views on sensitive personal data which have not been considered above?

- There should be appropriate legal basis and/or exemptions for processing personal data – and particularly sensitive personal data – in financial services, where certain personal data is necessary as part of anti-money laundering (AML), terrorist financing and fraud prevention, or as part of customer-screening processes.

5. Definition of Processing

5.1. What are your views on the nature and scope of data processing activities?

- There should be an inclusive definition for processing. ASIFMA proposes that all personal data processed should be included, however it is processed.

5.2. Should the definition of processing list only main operations of processing i.e. collection, use and disclosure of data, and inclusively cover all possible operations on data?

- There should be an inclusive definition for processing. ASIFMA proposes that all personal data processed should be included, however it is processed.

5.3. Should the scope of the law include both automated and manual processing? Should the law apply to manual processing only when such data is intended to be stored in a

filing system or in some similar structured format?

Alternatives:
a. All personal data processed must be included, howsoever it may be processed.
b. If data is collected manually, only filing systems should be covered as the risk of profiling is lower in other cases.
c. Limit the scope to automated or digital records only.

- Activities undertaken by the data controller, being the service provider, in line with the purpose for which the data is collected should be permissible.
- Scope of law should include both "automated" and "manual processing."

5.4. Are there any other issues relating to the processing of personal data which have not been considered?

6. Definition of Data Controller and Processor

6.1. What are your views on the obligations to be placed on various entities within the data ecosystem?

6.2. Should the law only define "data controller" or should it additionally define "data processor"?

Alternatives:
a. Do not use the concept of data controller/processor; all entities falling within the ambit of the law are equally accountable.
b. Use the concept of data controller (entity that determines the purpose of collection of information) and attribute primary responsibility for privacy to it.
c. Use the two concepts of data controller and data processor (entity that receives information) to distribute primary and secondary responsibility for privacy.

- ASIFMA proposes that the attribution of data controllers be aligned with the EU GDPR requirements. The law should define "data controller" and "data processor" to ensure that organisations are under clear and reasonable obligations to protect personal data. This is especially the case in India where, in the context of outsourced data services, India's operators are processors rather than controllers.
- There is a need to clearly define data controller and data processor as firms may have data processing centres in India that should be classified as data processors and not as data controllers. If there is no definition of a data processor, it may be possible that such data centres would be designated as data controllers. This would be incorrect as the data and the purpose of processing will be determined by an offshore data controller and therefore should be subject only to secondary obligations. If primary obligations are imposed on data centres as data controllers instead of data processors, such obligations may conflict with the obligations of the offshore data controller.
- Data processors are usually subject to lower requirements because the primary responsibility for protecting personal data resides with the data controller; for example, the headquarters of a foreign firm.

6.3. How should responsibility among different entities involved in the processing of data be distributed?

Alternatives:
a. Making data controllers key owner and making them accountable.
b. Clear bifurcation of roles and associated expectations from various entities.
c. Defining liability conditions for primary and secondary owners of personal data.
d. Dictating terms/clauses for data protection in the contracts signed between them.
e. Use of contractual law for providing protection to data subject from data processor.

- ASIFMA recommends further industry consultation on these issues. For instance, we agree with Alternative "a" above, but options "d" and "e" may be useful in the context of transferring information to and from India. We also suggest that adoption of GDPR-compliant terms and contractual obligations is more than sufficient for these purposes and that India's regime should avoid being overly prescriptive in this regard, as this may result in significant and unnecessary administrative burdens.

6.4. Are there any other views on data controllers or processors which have not been considered above?

- Controllers established in India should be primarily accountable, but the Proposed Law should require processors established in India to undertake contractually to the standards required under the law.

7. Exemptions

7.1. What are the categories of exemptions that can be incorporated in the data protection law?

7.2. What are the basic security safeguards/organisational measures which should be prescribed when processing is carried out on an exempted ground, if any?

Domestic /Household Processing

1. What are your views on including domestic/household processing as an exemption?

2. What are the scope of activities that will be included under this exemption?

3. Can terms such as domestic or household purpose be defined?

4. Are there any other views on this exemption?

Journalistic/Artistic/ Literary Purpose

1. What are your views on including journalistic/artistic/literary purpose as an exemption?

2. Should exemptions for journalistic purpose be included? If so, what should be their scope?

3. Can terms such as journalist and journalistic purpose be defined?

4. Would these activities also include publishing of information by non-media organisations?

5. What would be the scope of activities included for literary or artistic purpose? Should the terms be defined broadly?

6. Are there any other views on this exemption?

Research/Historical/Statistical Purpose

1. What are your views on including research/historical/statistical purpose as an exemption?

2. Can there be measures incorporated in the law to exclude activities under this head which are not being conducted for a bona fide purpose?

3. Will the exemption fail to operate if the research conducted in these areas is subsequently published/ or used for a commercial purpose?

4. Are there any other views on this exemption?

Investigation and Detection of Crime, National Security

1. What are your views on including investigation and detection of crimes and national security as exemptions?

2. What should be the width of the exemption provided for investigation and detection of crime? Should there be a prior judicial approval mechanism before invoking such a clause?

3. What constitutes a reasonable exemption on the basis of national security? Should other related grounds such as maintenance of public order or security of State be also grounds for exemptions under the law?

4. Should there be a review mechanism after processing information under this exemption? What should the review mechanism entail?

5. How can the enforcement mechanisms under the proposed law monitor/control processing of personal data under this exemption?

6. Do we need to define obligations of law enforcement agencies to protect personal data in their possession?

7. Can the Data Protection Authority or/and a third-party challenge processing covered under this exemption?

8. What other measures can be taken in order to ensure that this exemption is used for bona fide purposes?

9. Are there any other views on these exemptions?

Additional Exemptions

1. Should "prevention of crime" be separately included as ground for exemption?

- Yes, detection and prevention of crime should be included as grounds for exemption.

2. Should a separate exemption for assessment and collection of tax in accordance with the relevant statutes be included?

3. Are there any other categories of information which should be exempt from the ambit of a data protection law?

- Yes. As per the comment above. There should be appropriate legal basis and/or exemptions for processing personal data and sensitive personal data, particularly in the context of AML, terrorist financing and fraud prevention or otherwise as part of pre-screening processes in the context of providing financial services.

8. Cross Border Flow of Data

8.1. What are your views on cross-border transfer of data?

- The financial services industry has evolved to use information technology to enhance the quality, efficiency and security it offers investors and customers. Cross-border transfers of personal information are an inextricable part of today's digital economy. Therefore, data protection laws must facilitate, not discourage, the effective and lawful transfer of personal information, while preserving the economic benefits of an interconnected data ecosystem. Accordingly, we encourage India's policymakers to protect the financial services sector and its customers from rising digital protectionism.
- Transferring data across borders is crucial for the financial services industry to: (i) provide core products and services to customers, including executing trades in global markets; (ii) manage risk across affiliates and borders; and (iii) comply with financial regulatory requirements in various jurisdictions, including Know Your Customer (KYC) and AML regulations. In addition, cross-border data flows are necessary for supporting the development of financial technologies (fintech), including blockchain.
- ASIFMA supports an open global economy in which financial services can boost international trade, investment and economic growth. We recommend the Committee of Experts: (i) recognise the importance of cross-border data flows to international trade and investment; (ii) address the challenges posed by increasing data localisation policies; and (iii) reference the following principles to design policies that enable cross-border data flows while recognising security, privacy, and economic growth objectives:
    - **Recognise that the ability to transmit data across national boundaries and store data in different jurisdictions is fundamental to supporting a secure, innovative, and prosperous global financial system, as well as fostering global economic growth.** Policymakers have a

significant interest in reducing barriers to safe and efficient data flows to grow the digital economy. By recognising the impact that data privacy and security policies have on international trade and investment, policymakers can balance the goal of protecting investors and consumers with the need to bolster cybersecurity and promote economic growth. Policymakers should aim to develop data confidentiality and security frameworks that multinational financial institutions can implement in a global operating environment. Adopting international privacy and data security frameworks that enable safe and efficient cross-border data flow will improve international trade and investment, and promote digital trade.

- **Ensure consistency with existing international best practices.** ASIFMA encourages governments to adopt existing frameworks that protect citizens' privacy and data security while enabling cross-border data transfer. For instance, the Asia-Pacific Economic Cooperation forum's privacy framework provides a principles-based framework that balances the objectives of privacy and security while enabling the cross-border flow of data critical to digital trade. We also encourage further adoption of the International Principles for Cybersecurity, Data and Technology drafted by the Global Financial Markets Association (GFMA), the European Banking Federation (EBF) and the International Swaps and Derivatives Association (ISDA).
- **Recognise that cross-border data mobility supports information security.** While well-intentioned, overly restrictive privacy or information security rules may undermine the security of multinational networks and operating systems. Privacy cannot be protected without effective security. It is therefore important to address how data is shared and stored, not where. Processing and sharing consumer data with third parties and between countries is important, particularly in the context of cybersecurity, AML and the enforcement of sanctions. Limitations on cross-border data access inhibit firms' ability to monitor and prevent cyber-attacks, and hinder the sharing of information on cyber threats between firms and law enforcement. In addition, requirements to store data onshore create additional points of entry for bad actors to infiltrate networks. Regional data centres or IT hubs enable firms to dedicate resources to data and technology security, and have more robust protections in place to for data back-ups. In that way, data localisation jeopardises firms' business continuity and disaster recovery plans.
- **Enable targeted cross-border information-sharing.** Financial institutions must provide appropriate, timely data to regulators to fulfil their regulatory obligations in different jurisdictions. Restrictions on cross-border data flows introduce compliance risks, as privacy laws and blocking statutes introduce conflicts of law for multinational firms subject to multiple regulatory reporting regimes. Accordingly, data localisation policies can prevent financial regulators from having the data necessary to do their jobs effectively, and undermine firms' efforts to comply with regulatory requirements. For instance, financial institutions need to share information with their affiliates across borders to obtain information necessary to file suspicious activity reports under the US Bank Secrecy Act/Anti-Money Laundering framework. We call on policymakers to be mindful of the impact that data localisation policies have on firms' abilities to carry out important investor-protection protocols, including AML, KYC, financial crime investigations, etc. ASIFMA encourages data protection authorities to coordinate with other financial crime and cyber authorities when defining parameters for the use of data to allow targeted cross-border data transfer necessary to fulfil regulatory obligations and bolster investor protection.
- **Enable third-party outsourcing arrangements.** Outsourcing arrangements are critical to improving the efficiency of the financial services industry. Outsourcing enables firms to provide

stellar customer service, maintain competitiveness internationally, and reduce operational costs to boost investments in other areas that deepen local capital markets. Policies that limit or prohibit outsourcing arrangements in the financial services sector undermine these benefits to local economies. Outsourcing requirements should be principles-based and technology-neutral to allow financial institutions to deploy outsourcing arrangements according to their own business models and risks. ASIFMA encourages policymakers to adopt pragmatic policies that address potential risks from third-party service providers while enabling the efficiencies they provide. For instance, the adoption of vendor risk-management frameworks can encourage financial institutions to assess and mitigate potential risks from outsourcing exposures. We advise policymakers to consider the materiality of outsourced activities to firms' business practices and their ability to fulfil their regulatory obligations to ensure outsourcing guidelines are proportionate to potential risks.

8.2. Should the data protection law have specific provisions facilitating cross border transfer of data? If yes, should the adequacy standard be the threshold test for transfer of data?

- For the reasons detailed above, ASIFMA supports provisions that facilitate cross-border transfers of data. The Proposed Law should, as a minimum, allow the cross-border flow of data so long as the recipient is bound by written agreement to ensure that the transferred data is provided a standard of protection comparable to that in India. Additionally, when an Indian entity is acting as a data processor on behalf of a foreign data controller, the proposed Act should not prohibit such cross-border flow of data.

8.3. Should certain types of sensitive personal information be prohibited from being transferred outside India even if it fulfils the test for transfer?

- ASIFMA does not support provisions that prohibit certain types of sensitive personal information from being transferred outside India. Transferring data across borders is crucial for the financial services industry to: (i) provide core products and services to customers, including executing trades in global markets; (ii) manage risk across affiliates and borders; and (iii) comply with financial regulatory requirements in various jurisdictions, including KYC and AML.

8.4. Are there any other views which have not been considered?

9. Data Localisation

9.1. What are your views on data localisation?

- ASIFMA strongly opposes data localisation requirements for the storage of personal data within India. Multinational companies typically consolidate data-processing operations for security, operational effectiveness and economies of scale. Requiring that servers be physically located within India would not significantly advance the protection of personal data contained in those Indian servers – as that would require the setup of an India-specific server that may not be able to avail itself of the standards of protection afforded to a consolidated server. Additionally, this could be detrimental to India's outsourcing industry, as certain data controllers may not wish to have their data physically located in India.

- For commercial enterprises where personal information processed by such enterprises does not (or rarely) affects national security, data localisation disrupts communications between a company's India office and its other global operators, stifles cross-border innovation, raises equipment costs, and undermines firms' ability to service clients in India and abroad. Data localisation should therefore not be a requirement in these situations.
- In the previous section on Cross Border Flow of Data we have set out more detailed considerations regarding the need for, and benefits of, cross border data transfers and methods for doing this. Adoption of those principles should reduce the need for any data localisation requirements.

9.2. Should there be a data localisation requirement for the storage of personal data within the jurisdiction of India?

- ASIFMA strongly opposes data localisation requirements for the storage of personal data in India. Such provisions would impose a geographic restriction on data flows and raise costs without necessarily improving data security. Relevant financial institutions would bear responsibility for such data security and could be held liable for any material breach. This requirement would also fail to reduce the risk of network intrusions from outside of India, as modern data storage and retrieval technology render the location of data centres immaterial.
- Any requirement to outsource data storage services within India's borders would limit the ability of international companies to effectively run their business as part of their global platforms. This would hurt their operations and create security risks. Local IT solutions may not immediately be compatible with global information security regimes, which are often designed and maintained by company headquarters in their home markets. Using India-specific solutions that are out of sync with global security networks could also create serious security vulnerabilities for data specifically collected in India.
- As acknowledged on Page 72 of the White Paper, the outsourcing industry plays a pivotal role in India's economy, and the adoption of data localisation requirements could hurt the growth of global in-house centres (GICs). Any data localisation requirements would need to take into account, therefore, the maturity and effectiveness of data protection laws in other countries or jurisdictions. Such approaches should be aligned with global standards. Existing data protection laws around the world permit the transfer of personal data subject to the application of appropriate safeguards to protect the data. Transfer restrictions should also take into account the maturity of data protection laws in other countries that offer adequate levels of protection in relation to personal data from India.

9.3. If yes, what should be the scope of the localisation mandate? Should it include all personal information or only sensitive personal information?

- As stated above, ASIFMA strongly opposes adopting data localisation requirements.

9.4. If the data protection law calls for localisation, what would be impact on industry and other sectors?

- Data localisation requirements would have a considerable impact on India's outsourcing industry and GICs. As acknowledged on Page 72 of the White Paper, the outsourcing industry plays a pivotal role in India's economy, and the adoption of data localisation requirements could have a severe impact on the growth of GICs – particularly in India.

- Data localisation requirements also hamper financial services by: (1) disrupting communication between a company's local office and its global operations; (2) raising the cost of doing business; (3) preventing the company from providing seamless global service to Indian customers; and (3) putting Indian enterprises at a competitive disadvantage with other countries that embrace the digital economy. These types of measures are counterproductive, as they fragment the global operations of firms and both create and increase cybersecurity risks, thereby inhibiting cross-border trade and investment.
- Data localisation undermines the effectiveness of a financial institution's risk monitoring and surveillance programme. For example, compliance with AML laws and sanctions requires a comprehensive and holistic approach, whereby quantification of risk encompasses a customer's entire relationship across a financial institution. Aggregation of data on a clients' activity across borders allows a holistic assessment of the client's global activity for better informed decision making.
- The proliferation of data localisation requirements and policies hindering the free flow of data has not been supported by credible evidence that such rules enhance security, ensure access to data, or mitigate privacy concerns. These issues are best addressed through the rigorous and high-standard systems employed by financial institutions.
- The resources required for compliance with data localisation laws often deters firms from entering or expanding in a market, limiting job creation and investment. These costs are passed along to consumers, reducing their access to goods and services. The costs of data localisation policies ultimately constrain the rise of digital trade, as well as global economic growth.

9.5. Are there any other issues or concerns regarding data localisation which have not been considered above?

- ASIFMA believes that data localisation would have a detrimental effect on financial institutions, banks and their operating entities. Many financial services firms operating in India are global institutions offering services that are not necessarily limited to the jurisdiction of India – and their network infrastructure and data processing facilities may not be in the country.

10. Allied Laws

Comments are invited from stakeholders on how each of these laws may need to be reconciled with the obligations for data processing introduced under a new data protection law.

- ASIFMA recommends having one, consolidated, national data protection law governing data protection among various industries – namely the financial sector, health sector and the information technology sector. This Proposed Law should prevail over other general laws in case of conflict to avoid overlapping or duplicative regulations, subject to the caveats below.
- ASIFMA recommends that the Committee of Experts consider including sector-specific provisions to minimise overlapping conflicts with pre-existing national laws. In addition, the Committee should make clear what role the data protection authority would be expected to perform and how it would

coordinate with existing regulators. In our view, maintaining sectoral regulators as the primary co-ordinators on issues pertaining to data protection is the most business-friendly approach.

- The banking sector is already bound by the secrecy norms prescribed by the RBI, which are already likely on par with the proposed restrictions. The disclosures required to the Credit Information Bureau of India and other credit agencies – and also to the Information Utilities under the Insolvency and Bankruptcy Code 2016 – would be essential from the perspective of effective functioning of the banking sector. As such, we propose that no standards be prescribed by the data protection authority that might override these requirements. The determination of standards should instead be left to sectoral regulators.
- Any new data protection regime should ensure that it cannot be abused in such a way that interferes with the Insolvency and Bankruptcy Code, 2016 ("the Code") or impede the Code's effectiveness in order to avoid insolvency or complicate resolution in the guise of privacy. The Code has, for instance, already provided for the establishment of an information database by the National e-Governance Services to facilitate the collection of information by resolution professionals. Any new data protection regime will need to ensure that it does not interfere with the collection of data by this utility or its timely access in order to meet the time restrictions for resolution under the Code.

GROUNDS OF PROCESSING, OBLIGATION ON ENTITIES AND INDIVIDUAL RIGHTS

1. Consent

1.1. What are your views on relying on consent as a primary ground for processing personal data?

Alternatives:
a. Consent will be the primary ground for processing.
b. Consent will be treated at par with other grounds for processing.
c. Consent may not be a ground for processing.

- ASIFMA is in favour of Alternative B. However, consent may be impractical for institutions where there is no direct relationship with the individual. Consent may be more appropriate for situations such as AML. We strongly recommend that the Proposed Law cater for obtaining negative consent as, in many instances, clients and customers remain passive.
- Consent should not be considered a "primary ground," but rather an alternative ground for processing personal data for the following reasons:
    - Obtaining valid consent can be challenging in an employment context because employers may be deemed to be in a position of power and therefore consent obtained may not be freely given;
    - Consent may be impractical where dealing with institutions/corporations and where data is processed in relation to their underlying representatives, as there is no direct relationship;
    - Consent may be inappropriate, e.g. for processing data as part of monitoring money laundering or fraud;
    - In order to remain valid, consent would need to be refreshed periodically, imposing cumbersome burdens on industry and commerce;
    - Consent can be refused or withdrawn by the data subject, impeding the processing of personal data.
- "Client consent" in the banking sector is the result of an informed decision qua the customer because the decision to open a bank account and avail services is often made by the customer before approaching the bank. Therefore, the consent is free and not induced or forced.
- The Proposed Law should allow notice (not consent) for personal information.

1.2. What should be the conditions for valid consent? Should specific requirements such as "unambiguous", "freely given" etc. as in the EU GDPR be imposed? Would mandating such requirements be excessively onerous?

- The RBI regulations on KYC and AML regulations clearly prescribe the documents to be collected from a prospective customer and this is not left to the discretion of the banking organisation.
- There should be a tiered approach in relation to consent; implied consent should be sufficient in relation to non-sensitive personal data. The manner of evidencing consent should be at the

discretion of the data controller and so should not be prescriptive, as consent will be obtained in different ways.

1.3. How can consent fatigue and multiplicity of notices be avoided? Are there any legal or technology-driven solutions to this?

- The personal/sensitive personal data collected by the bank from the client meets the threefold scrutiny discussed during the Mumbai Public Consultation session on 23 Jan 2018, i.e. (i) collection of data is legal, (ii) it is necessary and (iii) it is proportionate.

1.4. Should different standards for consent be set out in law? Or should data controllers be allowed to make context-specific determinations?

- With the advent of artificial intelligence and "Big Data," it may not always be feasible to obtain consent at the onset of processing. For example, data controllers may initially use anonymised data sets. However, once the data has been merged with other data sets and processed by AI, the end result could be personal data.

1.5. Would having very stringent conditions for obtaining valid consent be detrimental to day-to-day business activities? How can this be avoided?

- In many instances customers and clients will neither actively consent nor actively object to any data protection notice. In such circumstances, continued use of a service should be deemed to be consent to any data protection notice adequately provided.

1.6. Are there any other views regarding consent which have not been explored above?

- Consent is a primary ground for processing personal data and should be treated on par with other grounds for processing. Various other grounds for processing personal data will be needed in addition to consent. For example, businesses should be allowed to use personal data if consent is not feasible and if there is a legitimate business purpose for the use of the personal data (e.g. employee related matters, legal proceedings etc.). For regulated sectors such as banking, where the regulator already plays a vital role in protecting the customer's interest and mandates the collection of certain personal data for KYC and AML purposes, no further changes on the consent aspect should be made on these topics.

2. Child's Consent

2.1. What are your views regarding the protection of a child's personal data?

2. Should the data protection law have a provision specifically tailored towards protecting children's personal data?

2.3. Should the law prescribe a certain age-bar, above which a child is considered to be capable of providing valid consent? If so, what would the cut-off age be?

2.4. Should the data protection law follow the South African approach and prohibit the processing of any personal data relating to a child, as long as she is below the age of 18, subject to narrow exceptions?

2.5. Should the data protection law follow the Australian approach, and the data controller be given the responsibility to determine whether the individual has the capacity to provide consent, on a case by case basis? Would this requirement be too onerous on the data controller? Would relying on the data controller to make this judgment sufficiently protect the child from the harm that could come from improper processing?

2.6. If a subjective test is used in determining whether a child is capable of providing valid consent, who would be responsible for conducting this test?

Alternatives:
a. The data protection authority
b. The entity which collects the information
c. This can be obviated by seeking parental consent

2.7. How can the requirement for parental consent be operationalised in practice? What are the safeguards which would be required?

2.8. Would a purpose-based restriction on the collection of personal data of a child be effective? For example, forbidding the collection of children's data for marketing, advertising and tracking purposes?

2.9. Should general websites, i.e. those that are not directed towards providing services to a child, be exempt from having additional safeguards protecting the collection, use and disclosure of children's data? What is the criteria for determining whether a website is intended for children or a general website?

2.10. Should data controllers have a higher onus of responsibility to demonstrate that they have obtained appropriate consent with respect to a child who is using their services? How will they have —actual knowledgeǁ of such use?

2.11. Are there any alternative views on the manner in which the personal data of children may be protected at the time of processing?

3. Notice

3.1. Should the law rely on the notice and choice mechanism for operationalising consent?

3.2. How can notices be made more comprehensible to individuals? Should government data controllers be obliged to post notices as to the manner in which they process personal data?

3.3. Should the effectiveness of notice be evaluated by incorporating mechanisms such as privacy impact assessments into the law?

3.4. Should the data protection law contain prescriptive provisions as to what information a privacy notice must contain and what it should look like?

Alternatives:
a. No form based requirement pertaining to a privacy notice should be prescribed by law.
b. Form based requirements may be prescribed by sectoral regulators or by the data protection authority in consultation with sectoral regulators.

- We propose Alternative "a:" No form based requirement pertaining to a privacy notice should be prescribed by law.

3.5. How can data controllers be incentivised to develop effective notices?

Alternatives:
a. Assigning a data trust score.
b. Providing limited safe harbour from enforcement if certain conditions are met.
If a data trust score is assigned, then who should be the body responsible for providing the score?

3.6. Would a consent dashboard be a feasible solution in order to allow individuals to easily gauge which data controllers have obtained their consent and where their personal data resides? Who would regulate the consent dashboard? Would it be maintained by a third party, or by a government entity?

3.7. Are there any other alternatives for making notice more effective, other than the ones considered above?

4. Other Grounds of Processing

4.1. What are your views on including other grounds under which processing may be done?

- There should be other grounds for processing – as stated above consent is often challenging and impractical.

4.2. What grounds of processing are necessary other than consent?

- Contract Performance
- Legal Obligation
- Legitimate Interest
- Establishment, exercise or defence of legal claims
- Public Information
- Public Interest

4.3. Should the data protection authority determine residuary grounds of collection and their lawfulness on a case-by-case basis? On what basis shall such determination take place?

Alternatives:

a. No residuary grounds need to be provided.
b. The data protection authority should lay down lawful purposes by means of a notification.
c. On a case-by-case basis, applications may be made to the data protection authority for determining lawfulness.
d. Determination of lawfulness may be done by the data controller subject to certain safeguards in the law.

4.4. Are there any alternative methods to be considered with respect to processing personal data without relying on consent?

- ASIFMA favours option "d." Please see comments above on parallel grounds of processing in addition to consent.

5. Purpose Specification and Use Limitation

5.1. What are your views on the relevance of purpose specification and use limitation principles?

- Purpose limitation is an important principle, but should not restrict processing where the proposed new processing is compatible with the original purpose.

5.2. How can the purpose specification and use limitation principles be modified to accommodate the advent of new technologies?

- The purpose specification and use limitation principles should be technology neutral; focus should be on the purpose and legal basis for the processing.

5.3. What is the test to determine whether a subsequent use of data is reasonably related to/ compatible with the initial purpose? Who is to make such determination?

- The data controller should make that determination.

5.4. What should the role of sectoral regulators be in the process of explicating standards for compliance with the law in relation to purpose specification and use limitation?

Alternatives:
a. The sectoral regulators may not be given any role and standards may be determined by the data protection authority.
b. Additional/ higher standards may be prescribed by sectoral regulators over and above baseline standards prescribed by such authority.
c. No baseline standards will be prescribed by the authority; the determination of standards is to be left to sectoral regulators.

- Please see comments in relation to AML, terrorist financing, cybersecurity and fraud.

5.5. Are there any other considerations with respect to purpose specification and use limitation principles which have not been explored above?

6. Processing of sensitive personal data

6.1. What are your views on how the processing of sensitive personal data should be done?

6.2. Given that countries within the EU have chosen specific categories of —sensitive personal datall, keeping in mind their unique socio-economic requirements, what categories of information should be included in India's data protection law in this category?

6.3. What additional safeguards should exist to prevent unlawful processing of sensitive personal data?

Alternatives:
a. Processing should be prohibited subject to narrow exceptions.
b. Processing should be permitted on grounds which are narrower than grounds for processing all personal data.
c. No general safeguards need to be prescribed. Such safeguards may be incorporated depending on context of collection, use and disclosure and possible harms that might ensue.
d. No specific safeguards need to be prescribed but more stringent punishments can be provided for in case of harm caused by processing of sensitive personal information.

6.4. Should there be a provision within the law to have sector specific protections for sensitive data, such as a set of rules for handling health and medical information, another for handling financial information and so on to allow contextual determination of sensitivity?

- There should be certain exemptions – see related comments on exemptions at Section 4: "Definition of Sensitive Personal Data" under "Scope and Exemptions."

6.5. Are there any alternative views on this which have not been discussed above?

7. Storage Limitation and Data Quality

7.1. What are your views on the principles of storage limitation and data quality?

7.2. On whom should the primary onus of ensuring accuracy of data lie especially when consent is the basis of collection?

Alternatives:
a. The individual
b. The entity collecting the data

7.3. How long should an organisation be permitted to store personal data? What happens upon completion of such time period?

Alternatives:
a. Data should be completely erased
b. Data may be retained in anonymised form

7.4. If there are alternatives to a one-size-fits-all model of regulation (same rules applying to all types of entities and data being collected by them) what might those alternatives be?

7.5. Are there any other views relating to the concepts of storage limitation and data quality which have not been considered above?

- Storage should take into account any applicable legal and regulatory retention requirements, in particular in relation to financial services.

8. Individual Participation Rights-1

8.1. What are your views in relation to the above?

- ASIFMA proposes that access and correction requests should be rejected if sectoral regulators have imposed confidentiality requirements.

8.2. Should there be a restriction on the categories of information that an individual should be entitled to when exercising their right to access?

8.3. What should be the scope of the right to rectification? Should it only extend to having inaccurate date rectified or should it include the right to move court to get an order to rectify, block, erase or destroy inaccurate data as is the case with the UK?

8.4. Should there be a fee imposed on exercising the right to access and rectify one's personal data?

Alternatives:
a. There should be no fee imposed.
b. The data controller should be allowed to impose a reasonable fee.
c. The data protection authority/sectoral regulators may prescribe a reasonable fee.

8.5. Should there be a fixed time period within which organisations must respond to such requests? If so, what should these be?

8.6. Is guaranteeing a right to access the logic behind automated decisions technically feasible? How should India approach this issue given the challenges associated with it?

8.7. What should be the exceptions to individual participation rights?

[For instance, in the UK, a right to access can be refused if compliance with such a request will be impossible or involve a disproportionate effort. In case of South Africa and Australia, the exceptions vary depending on whether the organisation is a private body or a public body.]

- Proportionality is important, as is the nature of the request. Such rights should not be permitted as an alternative to disclosures necessary for litigation or abused by individuals.

8.8. Are there any other views on this, which have not been considered above?

9. Individual Participation Rights-2

9.1. What are your views in relation on the above individual participation rights?

9.2. The EU GDPR introduces the right to restrict processing and the right to data portability. If India were to adopt these rights, what should be their scope?

- Portability should be appropriately limited as it is not appropriate in the employment context, but is more suited to utility providers.

9.3. Should there be a prohibition on evaluative decisions taken on the basis of automated decisions?

Alternatives:
a. There should be a right to object to automated decisions as is the case with the UK.
b. There should a prohibition on evaluative decisions based on automated decision-making.

9.4. Given the concerns related to automated decision making, including the feasibility of the right envisioned under the EU GDPR, how should India approach this issue in the law?

9.5. Should direct marketing be a discrete privacy principle, or should it be addressed via sector specific regulations?

9.6. Are there any alternative views in relation to the above which have not been considered?

10. Individual Participation Rights-3: Right to be forgotten

10.1. What are your views on the right to be forgotten having a place in India's data protection law?

- Organisations should be exempted from the right to be forgotten if there is a conflicting requirement on the organisation to store and retain data (for example, KYC requirements).
- The right to exercise such a right should only be triggered in limited circumstances, such as when data has been collected unlawfully, or the requirements to retain such data has expired and there is no other legitimate reason to retain the data.
- How organisations implement should not be prescriptive, as the ultimate effect can be achieved by other means, such as restriction of further processing.
- Such a right should be applied proportionately, e.g taking into account the technology available and the likely adverse impact on the individual.

10.2. Should the right to be forgotten be restricted to personal data that individuals have given out themselves?

10.3. Does a right to be forgotten add any additional protection to data subjects not already available in other individual participation rights?

10.4. Does a right to be forgotten entail prohibition on display/dissemination or the erasure of the information from the controller's possession?

10.5. Whether a case-to-case balancing of the data subject's rights with controller and public interests is a necessary approach for this right? Who should perform this balancing exercise? If the burden of balancing rests on the data controller as it does in the EU, is it fair to also impose large penalties if the said decision is deemed incorrect by a data protection authority or courts?

- Please see comments on the above question no. 1.

10.6. Whether special exemptions (such as the right to freedom of expression and information) are needed for this right? (over and above possible general exemptions such as national security, research purposes and journalistic or artistic expression)?

- Yes, please see comments above on the question no. 1.

10.7. Are there any alternative views to this.

REGULATION AND ENFORCEMENT

1. Enforcement Models

1.1. What are your views on the above described models of enforcement?

- ASIFMA recommends the following measures:
    - A "self-reporting" obligation for breach of SPDI, with the nature of the breach and time period for reporting specified;
    - The Proposed Law should apply to all data regardless of the medium, e.g. collected manually/physically or electronically;
    - The Data Protection Authority should specify objective governance standards or data protection models/requirements after taking into consideration recommendations from industry bodies, based on their subject matter expertise of industry models; and
    - No criminal liability for the Data Protection Officer if relevant governance standards have been adhered to.

1.2. Does co-regulation seem an appropriate approach for a data protection enforcement mechanism in India?

1.3. What are the specific obligations/areas which may be envisaged under a data protection law in India for a (i) "command and control" approach; (ii) self-regulation approach (if any); and (iii) co-regulation approach?

1.4. Are there any alternative views to this?

2. Accountability and Enforcement Tools

2.1. What are your views on the use of the principle of accountability as stated above for data protection?

2.2. What are the organisational measures that should be adopted and implemented in order to demonstrate accountability? Who will determine the standards which such measures have to meet?

2.3. Should the lack of organisational measures be linked to liability for harm resulting from processing of personal data?

2.4. Should all data controllers who were involved in the processing that ultimately caused harm to the individual be accountable jointly and severally or should they be allowed mechanisms of indemnity and contractual affixation of liability inter se?

2.5. Should there be strict liability on the data controller, either generally, or in any specific categories of processing, when well-defined harms are caused as a result of data processing?

2.6. Should the data controllers be required by law to take out insurance policies to meet their liability on account of any processing which results in harm to data subjects?

Should this be limited to certain data controllers or certain kinds of processing?

2.7. If the data protection law calls for accountability as a mechanism for protection of privacy, what would be impact on industry and other sectors?

2.8. Are there any other issues or concerns regarding accountability which have not been considered above?

Enforcement Tools

A. Codes of Practice

2.A.1. What are your views on this?

2.A.2. What are the subject matters for which codes of practice may be prepared?

2.A.3. What is the process by which such codes of conduct or practice may be prepared? Specifically, which stakeholders should be mandatorily consulted for issuing such a code of practice?

2.A.4. Who should issue such codes of conduct or practice?

2.A.5. How should such codes of conduct or practice be enforced?

2.A.6. What should be the consequences for violation of a code of conduct or practice?

2.A.7. Are there any alternative views?

B. Personal Data Breach Notification

2.B.1. What are your views in relation to the above?

- Proposed voluntary breach notification: ASIFMA strongly recommends a voluntary breach notification regime for the reasons stated below:
  - One of main purposes for breach notification is to allow individuals to take necessary steps to minimise or avoid harm, and for regulators to exercise adequate oversight and ultimately ensure an effective data protection regime that can promote a digital economy with strong consumer and investor confidence. To that end, we feel that a data protection framework with strong accountability and governance would achieve the desired objectives better than imposing mandatory reporting requirements, including mandatory breach notification.
  - A robust governance and accountability programme established by an organisation will both: (a) ensure that appropriate controls and decisions are made to protect data subjects' personal information; and (b) allow flexibility in security incident management responses and containment measures to mitigate the risk of harm from security incidents which may inadvertently occur.
  - More importantly, a mandatory breach notification is incompatible with numerous considerations highlighted in pp. 162-165 of the White Paper, in particular:
    - it is "*important to take into consideration the magnitude of the leak;*"

- "*the nature of notification required depends on the nature of the data involved in the breach*"; and
- "*the degree of harm and the sensitivity of the data*" must be considered – these are not absolute, but questions of extent and degree.

- Mandatory breach notification
  - If mandatory breach notification must be implemented, the breach notification requirement must take a risk-based approach requiring notifications of breaches that may result in serious harm.
  - ASIFMA supports the provisional view expressed in the White Paper (p. 165) that the law only requires individuals be notified of data breaches "*where there is a likelihood that they will suffer privacy harms as a result of data breaches*" – as opposed to situations where there is negligible harm or impact to the individual.
  - ASIFMA is of the view that requirements on organisations – particularly international businesses – to notify national regulators and data protection authorities are too onerous. Instead, if mandatory breach notification is required, reporting to sectoral regulators should be sufficient. It may also be impractical for organisations to contact individuals in instances where no direct relationship between them exists.
  - For the mandatory breach notification to work, materiality considerations and exemptions would need to be specified to avoid notification fatigue of both data subjects and regulators, which would defeat the purpose of notification.

- Notification deadlines
  - If mandatory notification must be implemented, ASIFMA strongly recommends avoiding hard and short deadlines (e.g. 72 hours), and instead proposes that notification of breaches be made "as soon as practicable," or that an approach be taken similar to Australia's Notifiable Data Breach Scheme, which comes into effect on 22 February, 2018.
  - Requiring hard and short deadlines is counterproductive to organisations' risk management and containment efforts in the immediate aftermath of data breaches.
  - In addition, a hard and short deadline is arbitrary, unrealistic and unconstructive. It is unrealistic because the aim of notification is to enable data subjects to understand what has happened and take necessary steps to protect themselves from harm. Serious incidents these days are usually the result of cyber-attacks or breaches involving hackers or other cyber-criminals. In such situations, the investigation might require following a complex digital trail, which inevitably require days or even weeks. Requiring the organisation to notify would unnecessarily divert much-needed resources on investigation and containment not constructive to mitigating risk. On the contrary, such a requirement could introduce additional risk.
  - This echoes some of the considerations stated in the White Paper (pp. 163 to 164):
    - "*It could take months, or even years to find and assess if the breach is in relation to personal data of an individual. The primary issue in relation to detection of breach is the large quantity of data that an organization has to comb through to find anomalies*"; and
    - mandatory breach notification at short notice has the potential to "*create a situation of panic, which might happen if the individual is informed right at the time of initial detection. At the stage of initial detection, the organisation itself is many times in the dark and won't*

have enough information to answer the individual's queries and may result in an atmosphere of panic and mistrust."

- Significantly, having a mandatory breach notification with a short deadline may lead to many instances of "technical" breaches, since (as mentioned above) it is impossible for large organisations to comb through large quantities of data. Many such "technical breaches" are unlikely to be prosecuted because of the large amount of resources required to do so. From the legislator's perspective, this creates an undesirable result as law and practice diverge. This weakens and undermines the authority of the law.

2.B.2. How should a personal data breach be defined?

- As mentioned above, we support the provisional view expressed in the White Paper (p. 165) that the law only requires individuals be notified of data breaches "*where there is a likelihood that they will suffer privacy harms as a result of data breaches*."

2.B.3. When should personal data breach be notified to the authority and to the affected individuals?

- We recommend taking a practical and risk-based approach, taking into account the nature of the breach and its likely impact on data subjects. Certain breaches may require quicker notification (as in breach of individuals' credit card or other sensitive information) so that individuals can take immediate steps to avoid or minimise harm, whereas other types of breaches (e.g. cyber breaches where the nature and extent of personal information leaked) may require more time to investigate in order to ascertain the measures needed.
- Therefore, as stated above, we strongly recommend avoiding hard and short deadlines (e.g. 72 hours), and instead propose for breaches to be notified "as soon as practicable," or adopt an approach similar to Australia's Notifiable Data Breach Scheme, which comes into effect on February 22, 2018.
- Moreover, the Proposed Law should recognise that some breaches may already require notification under existing regulations to sectoral regulators. As such, it should avoid requiring duplicate notification to the authority and a regulator. Instead, it should establish mechanisms for sharing such notifications to facilitate rapid awareness of new threats, minimise delays and reduce uncertainty and potentially costly miscommunication.

2.B.4. What are the circumstances in which data breaches must be informed to individuals?

- ASIFMA notes that, in some situations, the risk of impact or harm of a data breach to affected individuals may be minimal or insignificant: for example, if the nature of the breach itself is unlikely to result in actual access or use of the data by a third party (e.g., in a Ransomware attack) or if the data breach was discovered early and sufficient measures were put in place to minimise such risks. In such situations, it is unlikely that affected individuals would need to take steps to protect themselves from such risks. Notification may instead cause undue concern to such individuals.

- In taking a "materiality" approach, the likelihood of risk of harm to the individual should be a key factor in determining whether notification to affected data subject is appropriate or required. Consequently, a meaningful and effective mandatory notification regime should include exceptions or exemptions such as, but not limited, to the below:
  - Where the data breach is unlikely to give rise to risk of serious harm to the affected data subject;
  - Subsequent measures have been taken such that risk of serious harm to data subjects is adequately mitigated and unlikely to materialise;
  - Where adequate mitigating controls (before the fact) exist to reduce the risk of harm, e.g. where the breached data is encrypted to a reasonable standard;
  - Disclosure is subject to other secrecy provisions or laws prohibiting disclosures that are regulated by sectoral laws or regulations (e.g. financial sector regulations);
  - Necessary in national interest;
  - Necessary for the protection of the data subject or rights and freedoms of others;
  - Where notification is likely to impede law-enforcement investigations;
  - Where the data has been encrypted.
- In this regard, ASIFMA notes that the materiality approach is consistent with the EU GDPR's mandatory notification requirements for data subjects, which are based on whether the breach is likely to result in a "high risk" to the data subjects' rights and freedoms. ASIFMA further proposes that materiality be assessed in the context of a risk-based approach and that the data protection authority consider allowing organisations to take this into account when organisations conduct an overall risk and impact assessment, rather than designate specific types of personal data as material. This approach would be preferable in that it focuses on breaches that may result in actual harm and minimises notification fatigue on organisations, individuals and the data protection authority, and would not unduly and/or unnecessarily increase compliance costs.
- The national law should recognise any pre-existing overseas regulations to avoid duplication of additional data notification obligations. Any requirements would need to take into consideration the potential impact on outsourcing and processing of personal information related to overseas individuals.

2.B.5. What details should a breach notification addressed to an individual contain?

- ASIFMA is in favour of voluntary breach notification. Organisations should retain the discretion to determine the details to be notified to individuals, taking into account the interests of the individual and ability to mitigate adverse harm, the nature of the breach and other legal considerations (such as other local laws which may prohibit certain details being disclosed).
- ASIFMA recommends that the Committee of Experts abide by international best practises, as presented in the White Paper.

2.B.6. Are there any alternative views in relation to the above, others than the ones discussed above?

- Certain sectors are subject to extensive supervision by their sector regulator, including banks and other financial institutions. Therefore, in implementing a mandatory or voluntary breach

notification regime, ASIFMA strongly recommends imposing a single notification regime, and avoiding concurrent application of regulations that may require notification to multiple regulators.

- Concurrent application of multiple laws and regulations, i.e. both national and sectoral regulations, would increase the compliance burden on organisations.
- If concurrent application is, however, deemed necessary, ASIFMA proposes streamlining the notification and reporting process such that organisations deal with a single point of contact to fulfil such obligations.

C. Categorisation of Data Controllers

2.C.1. What are your views on the manner in which data controllers may be categorised?

2.C.2. Should a general classification of data controllers be made for the purposes of certain additional obligations facilitating compliance while mitigating risk?

2.C.3. Should data controllers be classified on the basis of the harm that they are likely to cause individuals through their data processing activities?

2.C.4. What are the factors on the basis of which such data controllers may be categorised?

2.C.5. What range of additional obligations can be considered for such data controllers?

2.C.6. Are there any alternative views other than the ones mentioned above?

Registration

1. Should there be a registration requirement for certain types of data controllers categorised on the basis of specified criteria as identified above? If yes, what should such criteria be; what should the registration process entail?

- There should be no registration requirement, as it would impose onerous requirements on organisations and might deter outsourcing of certain processing activities to India. It would raise costs with no corresponding increase in benefits to personal data protection. Even in jurisdictions where there are registration requirements, there seems to be no tangible or meaningful benefits.

2. Are there any alternative views in relation to registration?

- In lieu of registration, we feel that a data protection framework with strong accountability and governance is more effective in protecting data subjects' personal information than imposing specific actions. Consequently, we support data protection legislation that includes formal accountability and governance requirements.

Data Protection Impact Assessment

1. What are your views on data controllers requiring DPIAs or Data Protection Impact Assessments?

2. What are the circumstances when DPIAs should be made mandatory?

- ASIFMA believes there are no such circumstances. Organisations should have discretion to determine what warrants a DPIA.

3. Who should conduct the DPIA? In which circumstances should a DPIA be done (i) internally by the data controller; (ii) by an external professional qualified to do so; and (iii) by a data protection authority?

- Data controllers should conduct the DPIA.

4. What are the circumstances in which a DPIA report should be made public?

- A DPIA should not be required as this is an internal risk assessment and would be confidential and proprietary.

5. Are there any alternative views on this?

Data Protection Audit

1. What are your views on incorporating a requirement to conduct data protection audits, within a data protection law?

2. Is there a need to make data protection audits mandatory for certain types of data controllers?

3. What aspects may be evaluated in case of such data audits?

4. Should data audits be undertaken internally by the data controller, a third party (external person/agency), or by a data protection authority?

5. Should independent external auditors be registered / empanelled with a data protection authority to maintain oversight of their independence?

6. What should be the qualifications of such external persons/agencies carrying out data audits?

7. Are there any alternative views on this?

Data Protection Officer

1. What are your views on a data controller appointing a DPO?

- If required, this should not be prescriptive. A DPO should not have to be located in India, but should be reasonably accessible.

2. Should it be mandatory for certain categories of data controllers to designate particular officers as DPOs for the facilitation of compliance and coordination under a data protection legal framework?

- Please see the comment above on question no. 1 about DPO.

3. What should be the qualifications and expertise of such a DPO?

- An effective data protection law must cater to the variety of data controllers and data processes that exist in its jurisdiction. A data controller (or processor) may be a large, multinational with teams of legal, compliance and technology personnel, and operations in multiple states and countries. At the same time, it could also be a small- or medium-sized enterprise in a rural area with only a handful of employees.
- The legislation should not specify minimum qualifications, as these may impose unnecessary or unrealistic burdens on data controllers (or processers). The responsible person must be in a position of authority and have appropriate decision-making capabilities to ensure compliance with the data protection framework.
- Instead, the data protection regulator should provide regular training or awareness sessions to allow DPOs to adequately carry out their obligations.

4. What should be the functions and duties of a DPO?

5. Are there any alternative views?

D. Data Protection Authority

2.D.1. What are your views on the above?

2.D.2. Is a separate, independent data protection authority required to ensure compliance with data protection laws in India?

2.D.3. Is there a possibility of conferring the function and power of enforcement of a data protection law on an existing body such as the Central Information Commission set up under the RTI Act?

2.D.4. What should be the composition of a data protection authority, especially given the fact that a data protection law may also extend to public authorities/government? What should be the qualifications of such members?

2.D.5. What is the estimated capacity of members and officials of a data protection authority in order to fulfil its functions? What is the methodology of such estimation?

2.D.6. How should the members of the authority be appointed? If a selection committee is constituted, who should its members be?

2.D.7. Considering that a single, centralised data protection authority may soon be over-burdened by the sheer quantum of requests/ complaints it may receive, should additional state level data protection authorities be set up? What would their jurisdiction

be? What should be the constitution of such state level authorities?

2.D.8. How can the independence of the members of a data protection authority be ensured?

2.D.9. Can the data protection authority retain a proportion of the income from penalties/fines?

2.D.10. What should be the functions, duties and powers of a data protection authority?

2.D.11. With respect to standard-setting, who will set such standards? Will it be the data protection authority, in consultation with other entities, or should different sets of standards be set by different entities? Specifically, in this regard, what will be the interrelationship between the data protection authority and the government, if any?

2.D.12. Are there any alternative views other than the ones mentioned above?

3. Adjudication Process

3.1. What are your views in relation to an adjudication process envisaged under a data protection law in India?

3.2. Should the data protection authority have the power to hear and adjudicate complaints from individuals whose data protection rights have been violated?

3.3. Where the data protection authority is given the power to adjudicate complaints from individuals, what should be the qualifications and expertise of the adjudicating officer appointed by the data protection authority to hear such matters?

3.4. Should appeals from a decision of the adjudicating officer lie with an existing appellate forum, such as, the Appellate Tribunal (TDSAT)?

3.5. If not the Appellate Tribunal, then what should be the constitution of the appellate authority?

3.6. What are the instances where the appellate authority should be conferred with original jurisdiction? For instance, adjudication of disputes arising between two or more data controllers, or between a data controller and a group of individuals, or between two or more individuals.

3.7. How can digital mechanisms of adjudication and redressal (e.g. e-filing, video conferencing etc.) be incorporated in the proposed framework?

3.8. Should the data protection authority be given the power to grant compensation to an individual?

3.9. Should there be a cap (e.g. up to Rs. 5 crores) on the amount of compensation which may be granted by the data protection authority? What should be this cap?

3.10. Can an appeal from an order of the data protection authority granting compensation

lie with the National Consumer Disputes Redressal Commission?

3.11. Should any claim for compensation lie with the district commissions and/or the state commissions set under the COPRA at any stage?

3.12. In cases where compensation claimed by an individual exceeds the prescribed cap, should compensation claim lie directly with the National Consumer Disputes Redressal Commission?

3.13. Should class action suits be permitted?

3.14. How can judicial capacity be assessed? Would conducting judicial impact assessments be useful in this regard?

3.15. Are there any alternative views other than the ones mentioned above?

4. Remedies
A. Penalties

4.A.1. What are your views on the above?

- Calculation of civil penalties should be based on the discretion of the adjudicating body, subject to a fixed upper limit.

4.A.2. What are the different types of data protection violations for which a civil penalty may be prescribed?

4.A.3. Should the standard adopted by an adjudicating authority while determining liability of a data controller for a data protection breach be strict liability? Should strict liability of a data controller instead be stipulated only where data protection breach occurs while processing sensitive personal data?

4.A.4. In view of the above models, how should civil penalties be determined or calculated for a data protection framework?

4.A.5. Should civil penalties be linked to a certain percentage of the total worldwide turnover of the defaulting data controller (for the preceding financial year) or should it be a fixed upper limit prescribed under law?

4.A.6. Should the turnover (referred to in the above question) be the worldwide turnover (of preceding financial year) or the turnover linked to the processing activity pursuant to a data protection breach?

4.A.7. Where civil penalties are proposed to be linked to a percentage of the worldwide turnover (of the preceding financial year) of the defaulting data controller, what should be the value of such percentage? Should it be prescribed under the law or should it be determined by the adjudicating authority?

4.A.8. Should limit of civil penalty imposed vary for different categories of data

controllers (where such data controllers are categorised based on the volume of personal data processed, high turnover due to data processing operations, or use of new technology for processing)?

4.A.9. Depending on the civil penalty model proposed to be adopted, what type of factors should be considered by an adjudicating body while determining the quantum of civil penalty to be imposed?

4.A.10. Should there be a provision for blocking market access of a defaulting data controller in case of non-payment of penalty? What would be the implications of such a measure?

4.A.11. Are there any alternative views on penalties other than the ones mentioned above?

B. Compensation

4.B.1. What is the nature, type and extent of loss or damage suffered by an individual in relation to which she may seek compensation under a data protection legal regime?

- In the event that an organisation has put in place reasonable safeguards to protect personal data, but a breach occurs anyway (for instance, because of hacking), the fact that such reasonable safeguards had been put in place should be treated as a mitigating factor.

4.B.2. What are the factors and guidelines that may be considered while calculating compensation for breach of data protection obligations?

4.B.3. What are the mitigating circumstances (in relation to the defaulting party) that may be considered while calculating compensation for breach of data protection obligations?

4.B.4. Should there be an obligation cast upon a data controller to grant compensation on its own to an individual upon detection of significant harm caused to such individual due to data protection breach by such data controller (without the individual taking recourse to the adjudicatory mechanism)? What should constitute significant harm?

4.B.5. Are there any alternative views other than the ones mentioned above?

C. Offences

4.C.1. What are the types of acts relating to the processing of personal data which may be considered as offences for which criminal liability may be triggered?

- Acts performed by DPOs acting in good faith on behalf of their employer should be specifically treated as non-criminal in nature. This will encourage DPOs in India to act responsibly (rather than conservatively), and help promote the growth of India's data-protection industry.

4.C.2. What are the penalties for unauthorised sharing of personal data to be imposed on the data controller as well as on the recipient of the data?

4.C.3. What is the quantum of fines and imprisonment that may be imposed in all cases?

4.C.4. Should a higher quantum of fine and imprisonment be prescribed where the data involved is sensitive personal data?

4.C.5. Who will investigate such offences?

4.C.6. Should a data protection law itself set out all relevant offences in relation to which criminal liability may be imposed on a data controller or should the extant IT Act be amended to reflect this?

4.C.7. Are there any alternative views other than the ones mentioned above?