16 December 2022

To,

Ministry of Electronics and Information Technology
(Government of India)
Electronics Niketan, 6, CGO Complex,
Lodhi Road, New Delhi
110003.

Subject:

Comments on the Draft of Digital Personal Data Protection Bill, 2022

On behalf of its members, the Asia Securities Industry and Financial Markets Association ("**ASIFMA**")[1] ("**we**", "**our**" or "**us**") appreciates the opportunity to provide feedback on the Draft of Digital Personal Data Protection Bill, 2022 ("**Bill**") released by the Ministry of Electronics and Information Technology ("**MEITY**"), Government of India ("**Government**") on its website.[2]

We welcome the Government's initiative to introduce a new draft of the Bill that is simple and includes many welcome changes from the past iterations. The Bill is reflective of the Government's intent to promote digital industry and ease of doing business in India. We believe that the Bill is a positive first step that provides a business-friendly compliance regime while ensuring sufficient protection of the rights of data principals.

We are pleased to make our submissions and highlight some suggestions and concerns of the industry on certain provisions of the Bill. Our members include large responsible international organizations operating in the Banking Financial Services and Insurance sector, who along with handling large amounts of personal data are also responsible for ensuring security of financial transactions and framework by preventing frauds, money laundering, and assessing creditworthiness. Our members are also subject to sector specific regulations and oversight. Accordingly, our comments are reflective of certain practical difficulties that we, as a sector may face based on the current text of the Bill.

While we have provided chapter wise comments as required, which are enclosed as **Annexure A**, we have in this cover note set out the overall theme and highlights for your kind consideration:

---

[1] ASIFMA is an independent, regional trade association with over 160 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

[2] Available at: The Digital Personal Data Protection Bill, 2022.

ASIFMA Headquarters
Unit 3603, Tower 2, Lippo Centre
89 Queensway
Admiralty, Hong Kong
Tel: +852 2531 6500

ASIFMA Singapore Office
One Raffles Quay, North Tower
Level 49, Unit 51B
Singapore, 048583
Tel: +65 6622 5970

(i) Section 17- Transfer of Personal Data outside India

Recommendation: Since most of our members are a part of a global financial ecosystem and the ability to transfer data in a real-time manner is critical to their operations, including for purposes of fraud detection, anti-money laundering measures and similar activities, we submit that the mechanism for transfer is clearly spelt out and in the spirit of the overall Bill, it be simple. Section 17 as currently drafted, provides no objective criteria for determining which jurisdictions may appear on a list of countries to which personal data may be transferred and refers to "such factors as it may consider necessary". Given the need to ensure adequate data protection, our members suggest that key factors be set out in the Bill, namely the objective assessment that personal data can be held securely in the relevant third country jurisdiction. Along with a list of trusted jurisdictions, separate mechanisms may include express consent of the Data Principal, an independent security assessment, model contractual clauses, contracts incorporating prescribed principles, etc. Such mechanisms are well established in various other jurisdictions and avoid business disruption while also ensuring sufficient data protection. Multiple options for international data transfers also aligns with best practice elsewhere, for example in the United Kingdom where a data adequacy decision is one of several options for cross border data transfers.

(ii) Section 14- Right of Redressal

Recommendation: The timeline for redressal should be extended to 30 days to align with international standards, as 7 days is a very short period to adjudicate disputes.

(iii) Timeline for implementation

Recommendation: We submit that the Bill provides for a reasonable implementation timeline of twenty-four months from the date the key provisions are notified by the Central Government, or any delegated legislation is issued. This will be helpful to the industry at large, especially entities in the financial sector who may need to modify certain processes or implement additional measures. Given the high touch point with Data Principals who may be dispersed, financial institutions will need to take proactive measures to reach out to Data Principals. The substantial details needed for implementation will be contained in delegated legislation, and an implementation timeline that commences before key compliance requirements are finalised will create confusion and make it difficult to agree an implementation strategy.

(iv) Section 4(2) of the Bill states that it is applicable to processing outside India if such processing is in relation to offering of goods and services to Data Principals based in India.

Recommendation: We recommend that targeting criteria is included to determine whether Data Fiduciary has the intention of offering goods and services to Data Principals in India. De-identified data (e.g. pseudonymized data) and anonymized data should be explicitly excluded from the ambit of the Bill.

(v) Section 6(2)- Reissue of notice

Recommendation: We recommend that to the extent existing consent letters and privacy notices or policies already comply with the requirements under the Bill and same can be demonstrated, there should be no obligation to reissue notices. This will significantly reduce any unnecessary duplication of client outreach and "consent fatigue".

(vi) Section 8- Deemed Consent

Recommendation: We welcome the Government's initiative to provide grounds for processing where personal data may be processed without requiring consent of the Data Principal. However, we recommend the Government to consider rephrasing the Section as 'Legitimate Purpose' and including an express statement that Sections 6 and 7 of the Bill will not be applicable to processing under Section 8 to avoid any confusion on the rights of Data Principal to withdraw consent. Further, we also recommend that reasonable purpose exception under Section 8(8) should not be subject to an additional qualification of 'public interest' as it may lead to limiting the intent for inclusion of Section 8(8).

We also recommend that the exemption as provided under Section 8(2) is extended to Data Fiduciaries for their compliance with law.

(vii) Section 9(5)- Breach notification

Recommendation: Breach notification needs a harm threshold. International legislative norms and practicality concerns direct that only breaches likely to result in harm to the Data Principal should require notification to the Data Protection Board of India ("**Board**") and only those likely to have a material impact require notification to impacted individuals on direction of the Board. Further, in line with international data breach notification standards, the Data Fiduciary and not the Data Processor should be required to notify the Board and affected Data Principal. The Data Processor should instead be required to promptly notify the Data Fiduciary of any personal data breach.

(viii) Section 11- Additional Obligations of Significant Data Fiduciary

Recommendation: We submit that a Significant Data Fiduciary ("**SDF**") designation should only for such Data Fiduciaries whose existence is of critical national, economic, or social significance, and compromise of data processed by them would have significant effects that prejudice the national interests of India. Notification of such SDFs should be done in consultation with relevant sectorial regulators. This will ensure that entities with varying degrees of onshore presence will be proportionately categorized, and entities with a sparse presence or no retail operations will not be subject to higher obligations.

(ix) Section 20- Functions of the Board

Recommendation: The Bill has proposed set-up of the Board, which is meant to act as an adjudicating authority (Section 19). While the Board is meant to function as an independent body, the exact composition, qualifications of the members and other aspects of the Board are unknown and subject to be prescribed by the Central Government in the subordinated

legislation. To ensure the Board can act as an independent and transparent body, we seek greater clarity on the Board set-up, its powers, and responsibilities before the Bill is notified.

(x) General Recommendation

Recommendation: We recognise the importance of the subordinate legislations in implementing the Bill and welcome the consultative process that has been initiated to seek industry views. Since many of the operative elements of the Bill will materialise through rule making, we submit that a similar consultative process is also adopted as an express requirement for rulemaking, to allow the industry to submit its views and highlight any inconsistencies with existing requirements under sectoral laws and guidelines. It is also recommended that the translation requirements are reduced to include only English or any language specified in the Eighth Schedule of the Constitution of India in which Data Fiduciary offers products or services or otherwise issues marketing or other communications. This will substantially reduce the burden on the Data Fiduciary while ensuring ease of access to Data Principals.

As we understand the importance of such regulation for the business and economic environment, we would be pleased to engage in further discussions with MEITY. ASIFMA and our members stand ready to provide further details and to engage in constructive dialogue on the possible ways of implementation and further development of the proposed legal framework. Should you have any questions in relation to this submission or would like to obtain further industry input, please contact Diana Parusheva, Executive Director at ASIFMA, Head of Public Policy and Sustainable Finance at dparusheva@asifma.org.

Yours faithfully
Diana Parusheva
Executive Director, Head of Public Policy and Sustainable Finance at Asia Securities Industry and Financial Markets Association (ASIFMA)

RELEVANT PROVISION	RECOMMENDATIONS
Translation/Language Requirements 3. Interpretation (2) "the option to access … in English or any language specified in the Eighth Schedule to the Constitution of India" shall mean that the Data Principal may select either English or any one of the languages specified in the Eighth Schedule to the Constitution of India; 6. Notice (3) The Data Fiduciary shall give the Data Principal the option to access the information referred to in sub-sections (1) and (2) in English or any language specified in the Eighth Schedule to the Constitution of India. 7. Consent (3) Every request for consent under the provisions of this Act shall be presented to the Data Principal in a clear and plain language, along with the contact details of a Data Protection Officer, where applicable, or of any other person authorised by the Data Fiduciary to respond to any communication from the Data Principal for the purpose of exercise of her rights under the provisions of this Act. The	• This is a heavy translation burden. The government may consider limiting it to include only English or any language specified in the Eighth Schedule to the Constitution of India in which Data Fiduciary offers products or services or otherwise issues marketing or other communications.

Data Fiduciary shall give to the Data Principal the option to access such request for consent in English or any language specified in the Eighth Schedule to the Constitution of India.	
4. Application of the Act (2) The provisions of this Act shall also apply to processing of digital personal data outside the territory of India, if such processing is in connection with any profiling of, or activity of offering goods or services to Data Principals within the territory of India. For the purpose of this sub-section, "profiling" means any form of processing of personal data that analyses or predicts aspects concerning the behaviour, attributes or interests of a Data Principal. 4(3) The provisions of this Act shall not apply to: (b) offline personal data; …	• The provision should be clarified to qualify that the offering should be targeted in line with international standards. The targeting criterion should be built in to ensure that intention to solicit is a pre-requisite. • This would be in line with the use of the word "offering", which is an active verb indicating some degree of targeting of Indian Data Principals as opposed to merely inadvertent provision of goods/services to India based Data Principals. • There is lack of clarity on what amounts to "offline personal data", and whether it is subject to collection or storage of data, or both. • De-identified data (e.g. pseudonymized data) must be explicitly excluded from the ambit of the Bill. • Carve-out of personal data of deceased to be considered where no nominee has been selected. "Personal data" should be defined with reference to a living individual in line with international standards.
6. Notice 6(2) Where a Data Principal has given her consent to the processing of her personal data before the commencement of this Act, the Data Fiduciary must give to the Data Principal an itemized notice in clear and plain language containing a description of personal data of the Data Principal collected by the Data Fiduciary and the purpose for	• The word "itemized" should be deleted to align with international standards which rely on notices being clear and in plain language containing description. • To the extent existing consent letters and privacy notices already generally comply with the requirements under the Bill and same can be demonstrated, there should be no obligation to reissue notices.

which such personal data has been processed, as soon as it is reasonably practicable.	
8. Deemed Consent 8(1) A Data Principal is deemed to have given consent to the processing of her personal data if such processing is necessary: (1) in a situation where the Data Principal voluntarily provides her personal data to the Data Fiduciary and it is reasonably expected that she would provide such personal data; (2) for the performance of any function under any law, or the provision of any service or benefit to the Data Principal, or the issuance of any certificate, license, or permit for any action or activity of the Data Principal, by the State or any instrumentality of the State; (3) for compliance with any judgment or order issued under any law; … (7) for the purposes related to employment, including prevention of corporate espionage, maintenance of confidentiality of trade secrets, intellectual property, classified information, recruitment, termination of employment, provision of any service or benefit sought by a Data Principal who is an employee, verification of attendance and assessment of performance;	• The concept of "Deemed Consent" is confusing (when read together with the other clauses on consent) and should instead be revised to "other legitimate bases" in line with international standards (or to "legal and business purposes" as per other parts of this Bill). • Alternatively, since deemed consent as a concept is an exclusion to the requirement to obtain consent under Clause 7, it may be clarified that the requirements under Clause 6 (Notice) and Clause 7 (Consent) do not apply to Section 8 (Deemed Consent). Furthermore, an express statement that the right of withdrawal of consent does not apply to processing under Section 8 will clarify the intent of the provision. • Section 8 includes processing of personal data for performance of any function under any law by the State or any instrumentality of the State. This should be extended to cover processing conducted by Data Fiduciaries as well i.e., deemed consent provision should apply when any Data Fiduciary is processing data to comply with applicable law. This is consistent with existing SPDI rules where consent is not required to process SPDI to comply with applicable law. • Instances relating to prevention and detection of fraud, mergers and acquisitions, processing of publicly available data, search engine operations, network and information security, credit scoring, and recovery of debt may be removed from the mandatory requirement to prove "public interest". • The purposes for exemption for employment should be inclusive and include contractors within their ambit. Therefore, it is recommended to adopt the word "personnel" instead of "employment/employee".

(8) in public interest, including for: (a) prevention and detection of fraud; (b) mergers, acquisitions, any other similar combinations or corporate restructuring transactions in accordance with the provisions of applicable laws; (c) network and information security; (d) credit scoring; (e) operation of search engines for processing of publicly available personal data; (f) processing of publicly available personal data; and (g) recovery of debt;	
9. General obligations of Data Fiduciary (1) A Data Fiduciary shall, irrespective of any agreement to the contrary, or non-compliance of a Data Principal with her duties specified in this Act, be responsible for complying with the provisions of this Act in respect of any processing undertaken by it or on its behalf by a Data Processor or another Data Fiduciary. (2) A Data Fiduciary shall make <u>reasonable efforts</u> to ensure that personal data processed by or on behalf of the Data Fiduciary is accurate and complete, if the personal data: … (5) In the event of a personal data breach, the Data Fiduciary or Data Processor as the case may be, shall notify the Board	• To the extent that there are multiple Data Fiduciaries involved in the processing of the information, there should be a concept of joint liability as contemplated in EU General Data Protection Regulation ("**GDPR**") in relation to joint controllers. • The obligation on the Data Fiduciary to ensure accurate and complete information of the Data Principal should be restricted to personal data that can be independently verified by the Data Fiduciary. It should be the duty of the Data Principal to ensure that accurate and complete information is provided to the Data Fiduciary. • Breach notification needs a harm threshold. International legislative norms and practicality concerns direct that only breaches likely to result in harm to the Data Principal should require notification to the Data Protection Board of India ("**Board**") and only those likely to have a material impact require notification to impacted individuals on direction of the Board. Further, Data Fiduciary should not be required to notify the Data Principal

and each affected Data Principal, in such form and manner as may be prescribed. For the purpose of this section "affected Data Principal" means any Data Principal to whom any personal data affected by a personal data breach relates. (9) The Data Fiduciary may, where consent of the Data Principal has been obtained, share, transfer or transmit the personal data to any Data Fiduciary, or engage, appoint, use or involve a Data Processor to process personal data on its behalf, only under a valid contract. Such Data Processor may, if permitted under its contract with the Data Fiduciary, further engage, appoint, use, or involve another Data Processor in processing personal data only under a valid contract.	if it is able to take actions such that it is unlikely that the notifiable data breach will result in harm to the Data Principal concerned. Form and manner of reporting, and a workable reporting timeline should also be arrived at in close consultation with the industry. • In line with international data breach notification standards, it should be for the Data Fiduciary, not the Data Processor, to notify the Board and affected Data Principal. The Data Processor should instead be required to promptly notify the Data Fiduciary of any personal data breach. • In relation to Section 9(9), transfer of personal data should not purely based on the consent of the Data Principal, and should be allowed where transfer is necessary for: (a) performance of a contract with Data Principal; (b) compliance with Data Fiduciary's legal obligation; (c) protecting vital interests of the Data Principal; (d) performance of a task carried out in the public interest; or (e) purposes of the legitimate interest of the Data Fiduciary. • Engagement of Data Processor by Data Fiduciary should also be allowed under other modes than a valid contract, such as binding corporate rules. This would facilitate transfer of personal data of employees or clients by Data Fiduciaries with their group entities for administrative purposes.
11. Additional obligations of Significant Data Fiduciary 1. The Central Government may notify any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary, on the basis of an assessment of relevant factors, including: a. the volume and sensitivity of personal data processed;	• The designation of Significant Data Fiduciary should only be levied on Data Fiduciaries whose existence is of critical national, economic, or social significance, and whose compromise would have significant effects that prejudice the national interests of India. • Further, the notification of significant data fiduciaries should be done in consultation with relevant sectoral regulator.

b. risk of harm to the Data Principal; c. potential impact on the sovereignty and integrity of India; d. risk to electoral democracy; e. security of the State; f. public order; and g. such other factors as it may consider necessary; (2) The Significant Data Fiduciary shall: (a) appoint a Data Protection Officer who shall represent the Significant Data Fiduciary under the provisions of this Act and be based in India.	• Sensitivity of personal data should not be a key factor given that the Bill does not distinguish between sensitive and non-sensitive personal data. The sensitivity of personal data should only be relevant to the extent that its compromise would significantly prejudice India's national interests. • The current criteria for defining a Significant Data Fiduciary should further consider the fact that the volume threshold for data of Indian nationals is **sufficiently significant in size to impact India's national interests.** Further, employee data should be excluded from consideration while determining Significant Data Fiduciaries, given that employee data has minimal impact on India's national interests. • Regulated entities, particularly wholesale banks and others, that provide services to corporate clients are already under very stringent confidentiality and data protection requirements mandated by financial regulators. Further, as these regulated entities are not in the business of collecting and monetising data, they should not be treated as Significant Data Fiduciaries. • For Multinational Corporations ("**MNC**") having offices across the globe, the Data Protection Officer should be permitted to be based out of a foreign office of the MNC to allow agility in structuring and quick decision making.
12. Right to information about personal data The Data Principal shall have the right to obtain from the Data Fiduciary: …	• The term "in one place" is vague and should be replaced to shed more clarity on the means of sharing the information. • We recommended that only information relating to broad categories of Data Fiduciaries should be required to be made available to the Data Principal to the best of Data Fiduciary's ability.

(3) in one place, the identities of all the Data Fiduciaries with whom the personal data has been shared along with the categories of personal data so shared;	
13. Right to correction and erasure of personal data **…** (2) A Data Fiduciary shall, upon receiving a request for such correction and erasure from a Data Principal: **…** (d) erase the personal data of a Data Principal that is no longer necessary for the purpose for which it was processed unless retention is necessary for a legal purpose.	• Like in case of storage limitation obligation, erasure of personal data should be qualified with a right to retain data necessary for "business purposes" in addition to "legal purpose". Further, meaning and scope of "busines purpose" in the Bill may be clarified through illustrations.
14. Right of grievance redressal (2) A Data Principal who is not satisfied with the response of a Data Fiduciary to a grievance or receives no response within seven days or such shorter period as may be prescribed, may register a complaint with the Board in such manner as may be prescribed.	• The timeline for redressal should be extended to 30 days to align with international standards, as 7 days is a very short period of time to adjudicate disputes.
17. Transfer of personal data outside India. The Central Government may, after an assessment of such factors as it may consider necessary, notify such countries or territories outside India to which a Data Fiduciary may transfer personal data, in accordance with such terms and conditions as may be specified.	• Until the transfer mechanisms are finalized, Data Fiduciaries should be permitted to continue transfer of personal data as per their current procedures. • Adopting a single mechanism for cross-border data transfers would be very limiting and restrictive, particularly where the one and only mechanism is further subject to the Central Government having conducted an assessment and notifying such countries to which a Data Fiduciary may transfer personal data. Hence, consider enabling transfers by default, alternative mechanisms such as explicit consent, contracts incorporating prescribed principles, intra-group schemes, binding corporate rules, cross

	border transfer within affiliates, and other internationally accepted mechanisms on the lines of GDPR. • Regular changes to the whitelisted countries will significantly impact technology infrastructure for MNCs, and therefore, there should be a degree of transparency and certainty in the whitelisting and removal. For foreign entities/MNCs, the Government to consider the flexibility of allowing transfer, processing, and storage of personal data in any jurisdiction that has equally stringent data protection laws or has such reasonable safeguards for data protection as maybe prescribed. • Transfer requirements should be kept reasonably light touch to enable ease of doing business with deemed consent provisions, specifically for MNCs. An approach on the lines of jurisdictions such as Singapore, Japan, and the EU, may be considered.
18. Exemptions. (1) The provisions of Chapter 2 except sub-section (4) of section 9, Chapter 3 and Section 17 of this Act shall not apply where: … (c) personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law (d) personal data of Data Principals not within the territory of India is *processed pursuant to any contract entered into with any person outside the territory of India* by any person based in India.	• The words in italics in Section 18(1)(d) should be removed to ensure that data originating outside India which is processed in India is fully exempted. This would maintain India's competitive advantage as an outsourcing and data hub and ensure that the Act only applies in scenarios where there is a strong India nexus (i.e. impacting Data Principals within India). • This section should expressly cover (and exempt) processing of data for the purposes of complying with applicable laws in force (e.g. AML, KYC). • This could be done by amending Section 18(1)(c) as: "personal data is processed in the interest of prevention, detection, investigation or prosecution of any offence or contravention of any law, *as well as the compliance with applicable laws"*.

29. Consistency with other Laws.	• Given that the Bill is intended to provide for a general law that applies horizontally across sectors while allowing the scope for sector-specific legislations, there is a need for co-ordination with the sectoral regulators to ensure the standards under the Bill is aligned with sector regulations to avoid confusion and leading to triggering of the overriding provision in the Bill. Similar to clause 67 of the Personal Data Protection Bill, 2018 a formal consultation with other sectoral regulators should be made mandatory. Clarity on the role that the sectoral regulator will play in the rule making and implementation process will be critical for the smooth implementation of the privacy law across the sectors.
Regulatory Overlap **9. General obligations of Data Fiduciary** (5) In the event of a personal data breach, the Data Fiduciary or Data Processor as the case may be, shall notify the Board and each affected Data Principal, in such form and manner as may be prescribed. **20. Functions of the Board.** (3) The Board may, in the event of a personal data breach, direct the Data Fiduciary to adopt any urgent measures to remedy such personal data breach or mitigate any harm caused to Data Principals.	• There is a regulatory overlap in the powers of CERT-In and the Data Protection Board of India ("**Board**"), requiring reporting of data breaches to both bodies, and both are vested with the powers to prescribe measures in case of a data breach. • To consider that there is no overlap in terms of compliances prescribed by different regulators. E.g. RBI requirements for data localization, SEBI guidelines, etc. • The Bill has proposed set-up the Board which is meant to act as an adjudicating authority (Section 19). While the Board is meant to function as an independent body, the exact composition, qualifications of the members and other aspects of the Board are unknown and subject to rules to be prescribed by the Central Government. To ensure that the Board can act as an independent and transparent body, we seek greater clarity on the composition of the Board, its powers, and duties before the Bill is implemented.
Implementation Period	• Given the substantive overhaul required by companies dealing with personal data, there should be an implementation period of 24 months in

	line with the recommendation of Joint Parliamentary Committee to enable a smooth transition. Further, in case of delegated legislation, this timeline should commence from the date of notification of the relevant delegated legislation.
Consultation for subordinate legislation.	• Given that substantial details will primarily be covered in the rules issued under the Bill by the Central Government, it will be important for the rules proposed under the Bill to be subject to public consultation. It is recommended that it be required under the Bill that the rules and regulations issued thereunder would mandatorily be subject to public consultation process.