asifma
Growing Asia's Markets

21 March 2025

To: Ministry of Electronics and Information
Technology (MEITY)
Government of India
Electronics Niketan, 6 CGO Complex
Lodhi Road, New Delhi 110003
Tele:011-24363071

Subject: The Draft Digital Personal Data Protection Rules, 2025- Operationalising India's Data Protection Law

Asia Securities Industry & Financial Markets Association ("**ASIFMA**")[1], on behalf of its members are pleased to submit this letter to India's Ministry of Electronics & Information Technology ("MEITY") on the proposed rules to the regulations under **the Draft Digital Personal Data Protection Rules, 2025**. We are grateful for the opportunity to submit our comments via the public consultation and appreciate MEITY's endeavours to collaborate with the industry to work towards an enabling legal and regulatory framework in India.

As requested, we have made our submission via the electronic portal, Innovate India. In this letter, we have consolidated our official response as **Annex 1** and expanded on the submission in **Annex 2** for further considerations on Significant Data Fiduciaries, which were not included in the official electronic submission due to word count restrictions.

We would like to note that ASIFMA's members comprise a combination of leading FIs from both the buy and sell side, who use financial data, including personal data, in their normal course of business following the laws of the country and in alignment with the rules stipulated by sector regulators like RBI and SEBI. In doing so we remain committed to protecting and preserving the integrity of personal laws while continuing our engagement with the Indian authorities for a strategic and holistic approach for data regulations including cross-border transfers, which are crucial for financial flows and international trade and cooperation to enhance the Indian economy.

Next steps

ASIFMA members would be happy to provide further information or clarification on this submission. Should you have any questions, please contact **Ms. Diana Parusheva-Lowery, Managing Director at ASIFMA**, Head of Public Policy and Sustainable Finance at dparusheva@asifma.org.This submission was prepared based on feedback from the wider ASIFMA membership with assistance

[1] ASIFMA is an independent, regional trade association with over 160 member firms comprising a diverse range of leading FIs 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.

from the legal firm, Trilegal.

Yours faithfully

Diana Parusheva - Lowery

Managing Director, Public Policy and Sustainable Finance

Asia Securities Industry & Financial Markets Association

M: +852 9822 2340

DParusheva@asifma.org

asifma
Growing Asia's Markets

Annex 1

Draft Rule	Comment
Rule 1 – Short title and commencement	
(2) Rules 3 to 15, rule 21 and rule 22 shall come into force with effect from _____. *(3) These rules, except rules 3 to 15 and rules 21 and 22, shall come into force on the date of their publication in the Official Gazette.*	**Introduction** We, Asia Securities Industry and Financial Markets Association (**ASIFMA**) are pleased to make our submissions on certain provisions of the Draft Digital Personal Data Protection Rules, 2025 (**Draft DPDP Rules**). Our members include large responsible international organizations operating in the regulated financial institution (**FI**) 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 may also be subject to sector specific regulations and oversight (for instance, in India, organizations are overseen by the Reserve Bank of India and the Securities and Exchange Board of India). We are grateful for the opportunity to submit our comments in response to the public consultation. **Effective Date** We submit that the Draft DPDP Rules should provide for a reasonable implementation timeline of 24 months from the date the key provisions are notified by the Central Government. This will be helpful to the industry at large, especially entities in the FI sector, which will need to dedicate significant time and resources to implementing the additional measures and processes required by the new law. Given the high touch point with Data Principals who may be dispersed, entities in this sector will need to take proactive measures to reach out to Data Principals. This would be aligned with the approach adopted with global privacy laws, including the European Union's General Data Protection Regulation (GDPR), which had a 2-year implementation timeline, and the laws of California (U.S.A.) and Brazil.
Rule 3 - Notice given by Data Fiduciary to Data Principal	

The notice given by the Data Fiduciary to the Data Principal shall— *(a) be presented and be understandable **independently of any other information** that has been, is or may be made available by such Data Fiduciary;*	Organizations operating in the FI sector are typically required by sectoral regulations to provide certain details to various stakeholders at the time of onboarding – for their own internal purposes as well as to obtain stakeholder consent. For instance, the Reserve Bank of India (**RBI**)'s Master Direction – Credit Card and Debit Card – Issuance and Conduct Directions, 2022 require the card issuer (i.e., the regulated banking entity) to provide cardholders a term sheet with the "Most Important Terms and Conditions" at the time of onboarding. Data Principals whose data is processed by such organizations may, therefore, prefer the privacy notice to be included along with other onboarding documents, to ensure that they can digest all relevant information in one go as well as avoid consent fatigue. The requirement in Rule 3(a) for the privacy notice to be "*presented independently of any other information*" could, if interpreted very strictly, mean that this practice may no longer be possible. Our members, therefore, suggest that this requirement be accordingly clarified to enable the notice to be provided as part of a combined onboarding document set. This would streamline the notification process for organisations that have aligned their practices with sectoral regulatory obligations and conventions, without disrupting well-established industry practices.
The notice given by the Data Fiduciary to the Data Principal shall— *(b) give, in clear and plain language, **a fair account** of the details necessary to enable the Data Principal to give specific and informed consent for the processing of her personal data, which shall include, at the minimum,—*	Further, the word "itemized" should be deleted to align with international standards which rely on notices being clear and in plain language.
The notice given by the Data Fiduciary to the Data Principal shall— *(c) the **particular communication link for accessing the website or app, or both**, of such Data Fiduciary, and a*	Rule 3(c) suggests that the Notice issued by the Data Fiduciary must mention the website or app of the Data Fiduciary. We respectfully recommend including the phrase "(if any)", to include entities that may not have a user-facing website or an app, as follows, along with the grammatical change to add the word "provide": "…***provide** the particular communication link for accessing the website or app **(if any)**, or both, of such Data Fiduciary…*"

description of other means, if any, using which such Data Principal may— (…)	
Rule 4 - Registration and obligations of Consent Manager	
(1) A person who fulfils the conditions for registration of Consent Managers set out in Part A of First Schedule may apply to the Board for registration as a Consent Manager by furnishing such particulars and such other information and documents as the Board may publish in this behalf on its website. *(a)* *(2) On receipt of such application, the Board may make such inquiry as it may deem fit to satisfy itself regarding fulfilment of the conditions set out in Part A of First Schedule, and if it—* *(b) (a) is satisfied, register the applicant as a Consent Manager, under intimation to the applicant, and publish on its website the particulars of such Consent Manager; or* *(c) (b) is not satisfied, reject the application and communicate the reasons for the rejection to the applicant.*	The concept of a consent manager is not common to other jurisdictions, so many FIs will be considering this issue for the first time. In this context the general concern may be regarding how to create and maintain interoperability with consent managers. The Draft DPDP Rules do not clarify whether data fiduciaries will have to mandatorily integrate with a consent manager (and if so, how many such consent managers), the allocations of costs for such integration and use, and do not provide operational details for implementation of the integrations similar to RBI's Account Aggregator Framework. The integration of consent manager should not be a mandatory requirement for a data fiduciary unless there is a seamless digital public infrastructure which may be integrated with, and suitable technical protocols laid down in that connection in consultation with the industry. We would also note that technical changes and build out for FIs will need to be subject to various internal governance and risk management mechanisms, many of which arise in response to various regulations and supervisory oversight. As a result, we request additional transition time, in comparison with other provisions, for the consent manager requirements to take effect to let the market develop and technical standards be formulated. Separately, Draft Rule 4 does not include any exemption for corporate groups to the extent that it may be beneficial and efficient for multiple group companies to have a single consent manager integration. Such an exemption will create additional flexibility – for instance, where a bank has an affiliate responsible for outsourced operational or technology functions across a corporate group. In such an instance, it may be more efficient for the bank's clients (and the client's consent manager if applicable) to liaise with the affiliate's consent manager in respect of their data management across the entire corporate group or to be able to choose the affiliate's consent manager as their consent manager for their broader banking relationship.
Rule 7 - Intimation of Personal Data Breach	

(1) ***On becoming aware of any personal data breach****, the Data Fiduciary shall, to the best of its knowledge, intimate to each affected Data Principal, in a concise, clear and plain manner and without delay,* ***through her user account or any mode of communication registered by her with the Data Fiduciary****,—* *(a) a description of the breach, including its nature,* ***extent and the timing and location of its occurrence****;* *(b) the* ***consequences relevant to her****, that are likely to arise from the breach;* *(c) the measures implemented and being implemented by the Data Fiduciary, if any, to mitigate risk;* *(d) the* ***safety measures that she may take to protect her interests****; and* *(e) business contact information of a person who is able to respond on behalf of the Data Fiduciary, to queries, if any, of the Data Principal*	Data breach incidents are often complex, international and anonymous events that can occur despite legally compliant security measures. Effective investigation and meaningful analysis of such incidents – and the identification of affected Data Principals, in some instances - can be time-consuming. Hence, data breach reporting requirements are an aspect of high priority for ASIFMA members. As a general matter, international legal norms and practicality concerns direct that only breaches likely to result in harm to the Data Principal should be notified. Therefore, we recommend that only those breaches that result in significant harm ought to be reported. A strict, combined reading of sub-rules 7(1) and (2) could lead to an interpretation that the phrase "without delay" in sub-rule (2) may refer to a period less than 72 hours from becoming aware of the same. Thus, Data Fiduciaries may not be able, in every instance of a personal data breach, to intimate every potentially affected Data Principal within such a short period, since whether or not a Data Principal was affected is a detailed and forensic exercise, and moreover may become known in a phased manner. Therefore, our members suggest that Rule 7 be clarified to avoid a potential interpretation that the 72-hour rule applies to the obligation to intimate affected Data Principals. Further, even once affected Data Principals are identified and can be notified, Data Fiduciaries may not often be able to provide certain information like timing and location of occurrence. Therefore, our members suggest modifying Rule 7(1) to limit the details to be notified to preliminary information. Rule 7(2) indicates that there must be 2 urgent notifications within 72 hours of a breach, including detailed information to be provided within 72 hours. Given the time and resources involved in analysing a breach, and the complexity involved in data breaches, we respectfully submit that these timelines may not practicable. Additionally, given that breach reporting is a regulatory requirement, organizations would need to allocate significant technical resources to prioritise this obligation, which may delay immediate on-ground risk mitigation efforts. Instead, our members suggest a single urgent notification, and the timeline may be aligned with leading international norms which generally require notification without undue delay and "where feasible" not later than 72 hours after having become aware of it.
(2) ***On becoming aware of any personal data breach****, the Data Fiduciary shall intimate to the Board,—* *(a)* ***without delay****, a description of the breach, including its nature,* ***extent, timing and location of occurrence and the likely impact****;*	

(b) ***within seventy-two hours of becoming aware of the same****, or within such longer period as the Board may allow on a request made in writing in this behalf,—* *(i) updated and detailed information in respect of such description;* *(ii) the broad facts related to the events,* ***circumstances and reasons leading to the breach****;* *(iii) measures implemented or proposed, if any, to mitigate risk;* *(iv)* ***any findings regarding the person who caused the breach****;* *(v) remedial measures taken to prevent recurrence of such breach; and* *(vi) a report regarding the intimations given to affected Data Principals*	
Rule 8 - Time period for specified purpose to be deemed as no longer being served	
(2) At least forty-eight hours before completion of the time period for erasure of personal data under this rule, the Data Fiduciary shall inform the Data Principal that such personal data shall be erased upon completion of such period, unless she logs into her user account or otherwise initiates contact with the Data Fiduciary for the performance of the specified purpose or exercises her rights in relation to the processing of such personal data.	While noting that Rule 8 does not apply to FIs in and of themselves, we respectfully submit that Rule 8(2) should be deleted as it creates an onerous obligation on Data Fiduciaries to notify Data Principals prior to the routine deletion of their data, the terms of which would already be agreed under the user agreement in accordance with consent principles. It also bears noting that a similar obligation does not appear to exist under data protection laws of other jurisdictions.

asifma
Growing Asia's Markets

Rule 9 - Contact information of person to answer questions about processing	
Every Data Fiduciary shall prominently publish on its website or app or make known via any other electronic means, and mention in every response to a communication for the exercise of the rights of a Data Principal under the Act, the business contact information of the Data Protection Officer, if applicable, or a person who is able to answer on behalf of the Data Fiduciary the questions of the Data Principal about the processing of her personal data.	Rule 9 suggests that details about the Data Protection Officer must be mentioned on a website or an app. We respectfully recommend including the phrase "*or make known via any other electronic means*", to include entities that may not have a user-facing website or an app, as follows: "*shall prominently publish on its website or app,* ***or make known via any other electronic means****, and mention in every response…*"
Rule 10 - Verifiable consent for processing of personal data of child or of person with disability who has lawful guardian	
(1) *A Data Fiduciary shall adopt appropriate technical and organisational measures to ensure that verifiable consent of the parent is obtained before the processing of any personal data of a child and* ***shall observe due diligence****, for checking that the individual identifying herself as the parent is an adult who is identifiable if required in connection with compliance with any law for the time being in force in India, by reference to—* *(a)* ***reliable details*** *of identity and age available with the Data Fiduciary; or* *(b) voluntarily provided details of identity and age or a virtual token mapped to the same, which is issued by*	We recommend that Part A of the Fourth Schedule to the Draft DPDP Rules should be amended to include platforms and services that are not directed at children. The obligation to verify the age of a user prior to their personal data being collected can become quite onerous and should not be mandated where the risk of a child's data being collected is typically low. For instance, the target audience of entities in the FI sector is fundamentally different from those of typical consumer Internet platforms. Further, we recommend that Part B of the Fourth Schedule to the Draft DPDP Rules should be amended to include processing for undertaking know-your-customer verification and processing for the benefit of the child, since these are reasonable bases for which an organization ought to collect and process the personal data of a child with limited risk (if any) of harm to the child.

an entity entrusted by law or the Central Government or a State Government with the maintenance of such details or a person appointed or permitted by such entity for such issuance, and includes such details or token verified and made available by a Digital Locker service provider.	
Rule 12 - Additional obligations of Significant Data Fiduciary	
(2) A Significant Data Fiduciary shall ***cause the person carrying out the Data Protection Impact Assessment and audit*** *to furnish to the Board a report containing significant observations in the Data Protection Impact Assessment and audit.*	FIs that do not serve retail clients should not be subject to additional obligations under the DPDP Act as SDFs as they process low volumes of personal data and are already subject to stringent sectoral regulations on data security and confidentiality. We recommend a DPIA obligation only if there is a change in the risk of processing, instead of an annual requirement. SDF categorization criteria should be objective and transparent with sufficient notice and clear compliance timelines. Further, Rule 12(2) suggests that a DPIA will need to be conducted by a third-party and not the Data Fiduciary. Since Section 10(2)(b) of the DPDP Act already provides for the appointment of an external auditor to conduct periodic audits, and to align with the global practice, we recommend that this Rule clarify that the DPIA may be conducted by the Data Fiduciary.
(4) A Significant Data Fiduciary shall undertake measures to ensure that personal data specified by the Central Government on the basis of the recommendations of a committee constituted by it is processed subject to	The data localization requirement in Rule 12(4) is not envisaged under the DPDP Act. Section 16 of the DPDP Act only contemplates a negative list of jurisdictions to which transfers of personal data may be restricted and does not contemplate localization. Section 10(2)(c)(iii) (from which Rule 12(4) appears to seek basis) requires that prescriptions under this section must be "consistent" with the provisions of the DPDP Act. This localization requirement is not consistent with the scheme of the DPDP Act to permit cross-border transfers. Data localization in principle can undermine innovation, cross border trade, and

the restriction that ***the personal data and the traffic data pertaining to its flow is not transferred outside the territory of India.***	investment. Many of the objectives sought to be achieved can be achieved without localization, especially in the context of regulated entities such as FIs. Data localization may lead to a setback for the digital economy and adoption of emerging technologies, such as AI, which India is eager to advance. Further, it appears that this requirement may apply to certain types of personal data, which would pose unique challenges since it may be impracticable to differentiate the location of storage based on the types of personal data, particularly in the case of intertwined datasets containing different heads of personal information. Additionally, the rule does not specify the composition and working rules of the proposed committee. Rule 12(4) would require Significant Data Fiduciaries to fundamentally modify the manner in which they process data, which would also result in them incurring significant cost without a corresponding public benefit. Hence, this requirement should not apply to regulated FIs.
Rule 13 – Rights of Data Principals	

(1) For enabling Data Principals to exercise their rights under the Act, the Data Fiduciary and, where applicable, the Consent Manager, ***shall publish on its website or app, or both, as the case may be…*** *(d)…* (3) *Every Data Fiduciary and Consent Manager* ***shall publish on its website or app, or both, as the case may be,*** *the period under its grievance redressal system for responding to the grievances of Data Principals and shall, for ensuring the effectiveness of the system in responding within such period, implement appropriate technical and organisational measures.*	Rule 13(1) and 13(3) suggests that a website or an app is required for enabling the rights of the Data Principals. We respectfully suggest including the phrases "if any" and "or via any other electronic means", to include entities that may not have a website or an app, as follows: "*shall publish on its website or app* ***(if any)****, or both,* ***or via any other electronic means,*** *as the case may be...*"
Rule 14 - Processing of personal data outside India	
Transfer to any country or territory outside India of personal data processed by a Data Fiduciary— *(a) within the territory of India; or* *(b) outside the territory of India in connection with any activity related to offering of goods or services to Data Principals within the territory of India, is subject to the restriction that the Data Fiduciary shall meet such requirements as the Central Government may, by*	The Draft DPDP Rules empower the Central Government to notify cross-border transfer restrictions, where foreign states or state-controlled enterprises can be restricted from being allowed access to personal data. However, the basis on which territories will be considered as restricted territories is unclear. Therefore, we recommend that further clarity is provided on this. It is also unclear as to what requirements may be so specified, leading to uncertainty and ambiguity for global enterprises such as our members. This requirement may create hurdles to personal data processing activities carried out in foreign locations by regulated entities. For instance, such requirements might conflict with foreign laws that allow access to such data by foreign regulators and require members to share personal data with them on certain grounds, such as criminal investigations and others.

general or special order, specify in respect of making such personal data available to any foreign State, or to any person or entity under the control of or any agency of such a State.	It is important for ASIFMA members that the free flow of data should be allowed as any limitations on the cross-border movement on data could hinder innovation and firms' ability to leverage global resources and expertise in technology development leading to a trade-off between the growth of India's digital economy and the potential benefits of emerging technologies. An exemption for regulated financial services such as banking and capital markets and related activity can strike the appropriate balancing between cross border investment and financing for economic growth. We would like to highlight that this is the approach taken in the US, while the UK, EU, Singapore, Hong Kong, Japan, Australia do not have such localisation requirements that members are aware of.
Rule 22 - Calling for information from Data Fiduciary or intermediary	
(1) The Central Government may, for such purposes of the Act as are specified in specified in Seventh Schedule, acting through the corresponding authorised person specified in the said Schedule, ***require any Data Fiduciary or intermediary to furnish such information as may be called for****, specify the time period within which the same shall be furnished and,* ***where disclosure in this regard is likely to prejudicially affect the sovereignty and integrity of India or security of the State, require the Data Fiduciary or intermediary to not disclose the same except with the previous permission in writing of the authorised person****.* *(2) Provision of information called for under this rule shall be by way of*	We recommend that the grounds under the Seventh Schedule of the Draft DPDP Rules should be more narrowly scoped and specific, rather than the current widely worded grounds, in order to reduce discretion and ambiguity. To mitigate the risk of misuse, we also recommend that the purposes for which the authorised persons may process any information disclosed to them should be limited to those necessary for the specific law enforcement grounds for which such personal data was requested. For instance, where information is called for the investigation of a criminal offence, it should only be processed for the limited purpose of such investigation. We also request that the powers of the Government to call for information from Data Fiduciaries do not extend to any personal data of foreign nationals or Data Principals not within the territory of India that may be covered under Section 17(1)(d) of the DPDP Act. This will ensure that members continue to seamlessly leverage global capability centres in India without being in conflict with confidentiality or other legal requirements in other countries, specifically with respect to the processing of personal data of foreign nationals. More specifically, as India remains an outsourcing hub and global servicing centre for many financial institutions, personal data relating to non-Indian clients and customers may be stored and processed within India. An exemption that such information as it relates to non-Indian businesses is outside the scope of Rule 22 and Section 36 and other similar information gathering powers will create certainty for international financial institutions that they can continue to house global data operations in India without risk of forcible disclosures that may place them in breach of laws elsewhere.

fulfilment of obligation under section 36 of the Act. [Purposes under the Seventh Schedule: (a) Use by the State or any of its instrumentalities, of personal data of a Data Principal in the interest of sovereignty and integrity of India or security of the State (b) Use by the State or any of its instrumentalities for the following purposes, namely:— (i) Performance of any function under any law for the time being in force in India; or (ii) Disclosure of any information for fulfilling any obligation under any law for the time being in force in India (c) Carrying out assessment for notifying any Data Fiduciary or class of Data Fiduciaries as Significant Data Fiduciary.]	

asifma
Growing Asia's Markets

Annex 2

Submissions on certain aspects under the Digital Personal Data Protection Act, 2023

Please see below for further consideration on the **Digital Personal Data Protection Act, 2023 (DPDP Act**) which are not covered by the Draft DPDP Rules, namely: **(i)** the classification of Significant Data Fiduciaries (**SDFs**) and the time period for SDFs to comply with the additional obligations; and **(ii)** scope of the exception under Section **3(c)(ii)** of the DPDP Act on 'data being made publicly available.'

(i) ***Classification of SDFs*****:** Pursuant to Section 10(1) of the DPDP Act, the central government may notify any data fiduciary or class of data fiduciaries as SDFs based on factors including: (a) the volume and sensitivity of personal data processed; (b) risk to the rights of Data Principal; (c) potential impact on the sovereignty and integrity of India; (d) risk to electoral democracy; (e) security of the State; and (f) public order. However, the Draft DPDP Rules do not elaborate on the parameters for classifying SDFs. We understand that notifications will be issued by the Central Government to classify certain entities as SDFs pursuant to Section 10(1) of the DPDP Act. Given this, our members humbly submit that there should be no automatic classification of FIs as SDFs, and that the government should classify FIs as SDFs only if they serve a substantial number of retail clients i.e., individual end-customers. Accordingly, FIs that primarily cater to corporate clients should not be included, as the volume and sensitivity of personal data processed, and risks to the rights of data principals, are significantly lower. Further, establishing clear, objective thresholds for classification, rather than subjective criteria, will ensure consistency and transparency in regulatory enforcement. Given that India is a data hub serving global organisations from which foreign data flows into India, such clarity on the classification of SDFs would better facilitate data flows, and hence, have a positive impact on inbound business into India. In this regard, the threshold for classification of entities as "Significant Social Media Intermediaries" under the Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, i.e., entities with more than 50 lakh / 5 million registered users, is instructive, and a similar threshold may be considered while classifying SDFs.

- Additionally, our members recommend that any notification of SDFs under Section 10(1) of the DPDP Act provide an adequate timeframe for organizations to implement the compliance measures required by Section 10 of the DPDP Act and the corresponding rules. Given the nature of additional obligations for SDFs, organisations would require time and resources to incorporate processes and procedures for effective compliance with these obligations. A defined timeframe set out in advance will result in more effective compliance across the industry.

(ii) ***Exception on 'data being made publicly available':*** The provisions of the DPDP Act do not apply to 'personal data that is made publicly available.' Section 3(c)(ii) exempts personal data that is made publicly available by the data principal themselves, or by any other person who is under an obligation under applicable laws. Some of our members are service providers that process publicly available personal data for purposes such as Know Your Customer (**KYC**) / Anti-Money Laundering (**AML**) and Combating the Financing of

Terrorism (**CFT**) verification as part of client due diligence. Such publicly available personal data may not specifically be made available by the individual themselves or made available pursuant to applicable laws. Hence, such processing may not be exempt under the language of the current provision. KYC/AML and CFT checks are integral in the FI sector in order to fight financial crime and fraud, as stipulated under the Prevention of Money Laundering Act, 2002, the Reserve Bank of India's Know Your Customer Master Direction, 2016, the Securities and Exchange Board of India's Master Circular on Know Your Client norms for the securities market, and global best practices and regulations including The Financial Action Task Force's recommendations. Further, global data protection laws, including the General Data Protection Regulation set out "prevention of fraud" as a lawful basis for processing personal data (Recital 47 states "*The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned*"). We, therefore, urge that initiatives by FIs and their service providers to fight financial crime and prevent money laundering and financial fraud be supported by including an exemption for all publicly available data processed for this purpose.

<End>