11 September 2020

By online submission and mail

To:
Mr. Kris Gopalakrishnan
Committee of Experts on Non-Personal Data Governance Framework
Ministry of Electronics and Information Technology

Dear Sir / Madam,

Consultation on the Non-Personal Data Governance Framework, 2020

The Global Financial Markets Association ("**GFMA**")[1] welcomes the opportunity to comment on the draft Non-Personal Data Governance Framework, 2020 (**"Framework"**) from the perspective of the financial services sector, and the ease of doing business in India. We appreciate the Committee of Experts' (**"Committee"**) efforts to solicit industry feedback and are making this submission on behalf of our members.

We enclose our response to the Framework, prepared and submitted in collaboration across GFMA and its affiliates' members. Our response focuses on the potential impact of the proposed Framework on the financial services sector. While our comments are thematic, we look forward to further opportunities to discuss sector-specific issues as we move forward with this consultation process. In the meantime, if you have any questions, please do not hesitate to contact Matthew Chan, ASIFMA Head of Policy and Regulatory Affairs, at mchan@asifma.org or +852 2531 6560.

This submission was prepared with the assistance of the Law Offices of Panag & Babu, based on feedback from the wider ASIFMA and SIFMA membership.

Overview

The Framework signals a policy statement with an intent to categorise non-personal data ("**Non-Personal Data**") as a resource, and in some instances, as a public asset which contributes to India's economic advancement and in furthering sovereign and public interests. The Framework appears to be the first step towards drafting of legislation that not only defines ownership of non-personal data collected about Indians, or collected within India, but also prescribes mandatory sharing on grounds which will be subsequently defined.

The overall scope of the proposed framework, the proposed definitions, and categorisations, as well as the proposals on data businesses, anonymisation, mandatory data sharing and localisation, are all deeply concerning from the industry's standpoint. Any framework for non-personal data should recognise, and not undermine, or cut across requirements that already exist in law/regulation, in areas

[1] The Global Financial Markets Association ("**GFMA**") brings together three of the world's leading financial trade associations to address the increasingly important global regulatory agenda and to promote coordinated advocacy efforts. The Association for Financial Markets in Europe (AFME) in London and Brussels, the Asia Securities Industry & Financial Markets Association (ASIFMA) in Hong Kong and the Securities Industry and Financial Markets Association (SIFMA) in New York and Washington are, respectively, the European, Asian and North American members of GFMA. For more information, please visit http://www.gfma.org .

such as intellectual property, competition and bank secrecy. Without a radical recasting of the proposals, we do not believe they are workable from the perspective of the financial services sector.

To date, organisations and institutions, including private companies, have voluntarily, and in many instances in collaboration with regulatory partners, shared large volumes of data available for processing and use by the public without intervention or compulsion from the State, with the intent of facilitating innovation while ensuring equality of opportunity. Such sharing of data has been predicated on three key principles, which are as follows:

Principle I: Sector Specific Rulemaking and Use Cases. The first principle is that data portability initiatives are sector specific and driven by particular use cases or objectives. Having a well-defined scope enables smooth implementation and promotes consumer and market confidence and certainty while also reducing the risk of unintended outcomes or incentives. The Framework is sector-agnostic, which creates much ambiguity in terms of its application to financial services. It also means that there is a missed opportunity for the industry to focus on use cases that may have the most impact, such as the ability to make Anti-Money Laundering (**"AML"**), Know-Your-Customer (**"KYC"**) and anti-fraud data sharing processes more efficient, or to look at maximising consumer portability and choice in retail banking, or to reduce risks regarding unjustified bias or inadvertent discrimination in data processing that can affect consumer credit decisions.

Principle II: Regulator – Private Stakeholder Engagement on Rulemaking. The second principle is that once a well-defined and sector specific use case is identified (e.g. those identified above), implementation can be led by private organisations in collaboration with each other, and in partnership with appropriate sectoral regulators to drive innovation. Ensuring that private organisations lead in implementation promotes more detailed technical standards and protocols, leading to more efficient projects that are more likely to achieve their targeted outcome. Such collaboration also ensures the relevant regulator, with sectoral expertise, is able to weigh in with its own views and evolve its own know-how, while ensuring implementation is conducted on a timescale suitable for all parties and without raising cybersecurity or other operational risk profiles.

Principle III: Safeguards to Protect Private Ownership. The third principle is that data portability sets clear parameters on the scope of data such that proprietary data, trade secrets and sensitive or confidential business information (including regulatory confidential information) is clearly excluded. Such data projects, if primarily aimed at ensuring innovation in consumer facing businesses, will typically need to ensure that data relevant to consumer choice and consumer portability is in scope while all other data remains out of scope. Clear guardrails and safeguards are essential to ensure private businesses are able to maintain confidence in the ownership of their own data. The Framework does not elucidate on such guardrails, but these will need to be much more clearly defined going forward. Given the difficulties in creating such certainty on a sector-agnostic level, guardrails and market confidence is better maintained in project or sector specific rule sets.

An example of these principles in action is the open banking framework established in the UK for the retail banking sector. In 2016, the UK Competition Authority identified a lack of competition in retail banking and proposed a number of remedies including "Open Banking", which enables customers and small and medium-sized businesses to share their current account information securely with other third party providers from January 2018 onwards. Such a project required a detailed set of standards both technological and regulatory in nature, coupled with almost two years of industry collaboration

prior to launch, in addition to ongoing collaboration on subsequent improvements[2]. The Open Banking project was defined with a clear objective and set of use cases, targeted a specific sector and was led by a joint effort of the regulator of that sector along with the industry participants themselves. The scope of data being shared was also clearly defined as data relating to the particular consumer, who would give rolling consent for participation in such portability initiatives. It would be relevant to point out that even now, the Open Banking initiative is not mandatory for smaller banks given the time and cost involved in implementation.

Another example of these principles in action is the emerging field of governance principles over the use of artificial intelligence. The Framework notes that even Non-Personal Data, including anonymised Personal Data, could provide collective insights that could open the way for collective harms (exploitative or discriminatory harms) against communities. However, the Framework provides for no clear approach in reducing this risk, which would not be addressed through the data sharing proposal. Other jurisdictions have focused on the need for governance principles for the ethical use of artificial intelligence in decision making that can affect consumer outcomes. Notably, such proposals are led by industry regulators for financial services, such as the UK Financial Conduct Authority (**"FCA"**) or the Monetary Authority of Singapore (**"MAS"**)[3] again in collaboration with financial service providers[4]. This enables governance principles to be better targeted at financial service firms for better outcomes for consumers.

In addition to the above principles, our members would also like to highlight certain issues in particular for the Indian market, which are summarised as follows:

A. Given the decentralised nature of global businesses today, and in particular the strong competitive advantage that India has in the outsourcing sector, a proposed framework regulating Non-Personal Data collected or processed by companies in India, or from Indians by companies offshore, needs to protect private ownership (and treatment of data processed in India under outsourcing models) in order to further the ease of doing business in India, and retain India's strong position as a global data processing hub.

B. Mandatory sharing of any data, whether proprietary or not, would inherently be value-erosive and will be viewed adversely by companies (and where applicable, by home country governments and regulators) assessing India as a jurisdiction to conduct business in or from. Mandatory sharing of data also poses significant practical challenges and creates risks relating to the protection of proprietary information and should accordingly be removed. Accordingly, any policy which encourages data sharing should be predicated on voluntary and free-market principles, including the right of ownership of data, which is an important factor for companies investing significant amounts of capital and resources to collect and create commercially valuable data sets.

C. As governments globally assess the need to implement governance standards over the data ecosystem, it is important to acknowledge that the regulatory architecture for such standards already exist for sectors such as financial services. Such pre-existing arrangements and sector

[2] See timeline of the UK Open Banking project showing steps taken: https://www.openbanking.org.uk/about-us/; the various standards: https://standards.openbanking.org.uk/

[3] See the MAS announcement: https://www.mas.gov.sg/publications/monographs-or-information-paper/2018/FEAT

[4] See the terms of reference for the FCA's Financial Services Artificial Intelligence Public-Private Forum: https://www.fca.org.uk/publication/corporate/financial-services-artificial-intelligence-public-private-forum-terms-of-reference.pdf

expertise should not be overridden by sectoral agnostic authorities as this could create considerable uncertainty and potential conflicts over rulemaking, to very little benefit for the industry, clients and consumers as a whole. In this context we note a proposed Non-Personal Data Protection Authority could have rule making powers over banks who already have a working relationship with the Reserve Bank of India ("**RBI**") (which is pursuing its own policies over data), in addition to a proposed Personal Data Protection Authority, which has not yet been established. It is important to ensure consistency and certainty and minimise risks of conflicts over policymaking and we suggest that there be clear and public cooperation arrangements between all such authorities to ensure a single set of policies apply to banks. This can leverage the expertise of data authorities with the know-how of the financial sector regulators to create a level playing field for all service providers in financial markets and payments. This will create a firm platform for the Indian authorities to respond to future developments as boundaries between sectors in the data space may increasingly overlap.

D. Banks and other financial institutions and entities, which are already registered with and comprehensively regulated by RBI or the Securities Exchange Board of India (**"SEBI"**) under an existing statutory framework, should be exempted from registration as a *'Data Business'* and also from regulation under the Framework. Separate registration for financial institutions and banks as '*Data Business*' may not be in line with the regulatory framework under which financial institutions and banks in India are currently regulated. Any additional regulations which are required to address the issues in the Framework should be dealt with through rules/guidelines issued by the relevant sectoral regulators who are best placed to assess and understand the value of the Non-Personal Data generated in the relevant sector. The introduction of a competing and overlapping regulatory framework for financial institutions or banks could cause fragmentation, and potentially disrupt the stability of the financial system.

Having closely followed global and regional policy developments around regulation of non-personal data and free flow of data across borders, GFMA would like to offer our members' views in relation to the potential ramifications of the approach in the Framework. We foresee challenges in implementation, and potential unintended consequences by the inclusion of derivative data (based on intellectual property), foreign data, and lack of clarity on the pricing for data sharing as contemplated by the Framework.

The industry believes it would be useful for the Committee to establish working groups with both onshore and offshore trade associations, and authorities such as RBI and SEBI, to ensure a holistic policymaking environment for financial services.

We would be pleased to further engage in constructive dialogue with the Committee and the Ministry of Electronics and Information Technology on the Framework and its potential impact on the financial services industry in India.

Yours faithfully,

Kenneth E. Bentsen, Jr.
CEO, Global Financial Markets Association and
CEO and President, Securities Industry and Financial Markets Association

ANNEX 1

Recommendations and Suggestions for the Draft Framework

Following internal deliberations with our members, we set out below our viewpoints on the Framework, practical difficulties financial institutions may face with respect to implementation of the Framework as proposed, and our recommendations and requests for clarification on certain areas of the Framework.

Our recommendations are divided into **Part A**, which contains thematic aspects in relation to the Framework, and **Part B,** which contains brief descriptions of specific issues.

PART A

1. Definitions and Scope

We understand that the Framework defines Non-Personal Data as:

> "*any data that is not related to an identified or identifiable natural person, or is personal data that has been anonymised*"

i.e. data that cannot be attributed to an identified or identifiable natural person, or data which initially was personal data but has become Non-Personal Data due to anonymisation and removal of identifiers which can associate such data to a person. Non-Personal Data is further classified as public, community and private. The Framework also considers anonymised personal data to belong to the individual(s) to whom the data relates, despite anonymisation and declassification as personal data. In this regard our comments are as follows:

A. Definition of non-personal data: The definition of Non-Personal Data is extremely wide and may cover even unpublished price sensitive information received by an entity which carries out merchant banking/banking activity under the regulatory framework set out by SEBI or the RBI or potentially even such information that is processed in India and is subject to similar regulation in other jurisdictions. Such unpublished price sensitive information is extremely confidential and regulated under the relevant regulatory framework. Inclusion of such data within the definition of Non-Personal Data could lead to unintended conflict between other regulatory frameworks and the Framework leading to unintended consequences. Accordingly, such material non-public information or unpublished price sensitive information received by an entity should not be considered as Non-Personal Data. Further, all Non-Personal Data that has been specifically accorded confidentiality under applicable law (whether Indian law or the laws of other countries) or contractually should be excluded from the definition of public, private or community Non-Personal Data

Additionally, in the ordinary course of business, foreign entities receive large volumes of material non-public information or unpublished price sensitive information, which is required to be kept confidential under the law of their home jurisdictions. The definition of Non-Personal Data as currently framed, is wide enough to cover such material non-public information or unpublished price sensitive information and any obligation to disclose the same would have unintended consequences. It may also lead to a breach on part of foreign entities under existing confidentiality obligations towards their client or towards other global group entities.

B. **Overlapping Definitions**: We note that the definitions of new categories of Non-Personal Data are extremely broad. Without clearly demarcated 'litmus tests' for classification, these definitions have a high possibility of overlap. An instance of Private Non-Personal Data under the Framework includes '*inferred data*'. The inclusion of '*inferred data'* as Private Non-Personal Data could come in conflict with the Personal Data Protection Bill, 2019, wherein inferred data is included within the definition of personal data. This is likely to lead to competing claims for classification amongst these categories of data. Where an overlap exists, either due to ambiguity in definition or variance in interpretation, the data would be subject to multiple thresholds and be capable of misclassification, resulting in litigation, interpretative uncertainty, and inadvertent non-compliance. As an example, the Committee should address the fact that significant amounts of unstructured data are regularly generated and might not necessarily be used for any form of analytics, and are not clearly identifiable or distinguishable from other personal data or proprietary data. In such a scenario, it is unclear as to which category of Non-Personal Data such unstructured data will fall under and if the data sharing norms will apply to such Non-Personal Data which is unstructured, and inextricably mixed with other classes of data including personal data. Additionally, the focus of comparable legislation in other jurisdictions has hitherto been the regulation of the flow of Non-Personal Data between jurisdictions (and a prohibition on data localisation among EU Member States), rather than governing the collection/processing of Non-Personal Data within a country, which appears to be the primary focus of the Framework.

C. **Competing Ownership of Community Data**: The Framework contemplates that data that pertains to a community of natural persons and is collected in India is "*beneficially owned*" by the related community. At the same time, the rights over such data vest with the data trustee of that community, such as data collected by municipal corporations and public utility companies. This is likely to cause a duplicity of rights (and a duplicity of communities) over the same resource and create an inconsistent and conflicting framework for ownership of such data. While data is not finite, given that the Framework contemplates delineating rights over a body of data, such delineation is likely to create a conflict in several instances. For example, where community data is collected by a private company, which is often involved in the supply of utilities, e-commerce, food delivery, or infrastructure such data is unstructured. Since the definition of the data trustee is indicative and states "*such as*" within the definition, it appears to loosely define who would be the data trustee in the form of an inclusionary definition. For companies operating in regulated sectors, given the presence of a sectoral regulator, the inclusive definition may either be interpreted as conferring implicit rights over such data, which are likely to conflict with the relevant sectoral regulator, or if a separate data fiduciary exists alongside the sectoral regulator, they may exercise their rights in a manner contrary to the directions of the other.

The inclusion of virtual community data within the ambit of Community Non-Personal Data implies that the Framework would also include virtual communities which are internal to private entities (e.g. communities on social media, or an organisation when it has certain internal portals or virtual communities which are created solely for the purposes of development of knowledge resource or talent development specific to the needs of that organisation). The data generated from such internal virtual communities are proprietary to the organisation. Hence, the definition of Community should be narrowed to exclude virtual communities which are internal to an organisation.

D. **Sensitive Non-Personal Data**: Data is further segmented as sensitive Non-Personal Data i.e. Non-Personal Data that (i) relates to national security or strategic interest, (ii) bears the risk of collective harm to a group, (iii) is business sensitive or confidential information, and/or (iv) is data which bears the risk of re-identification.

The Framework contemplates that any Non-Personal Data that is derived from sensitive personal data will inherit its sensitive characteristic and anonymised and aggregated data from sensitive personal data will yield sensitive non-personal data. We submit that the view that personal data carries forward its sensitive nature even after anonymisation or aggregation is predicated on the incorrect assumption that the sensitive nature of such data survives anonymisation or aggregation. We submit that such data cannot be viewed as retaining sensitive characteristics after anonymisation since it is no longer attributable to the person to whom it belonged and, after aggregation, is not able to pinpoint a data principal or singular source of data. If Non-Personal Data were to be classified as sensitive, it would be incumbent upon the Committee to clarify whether sensitive Non-Personal Data shall also be subject to additional safeguards similar to those applicable to sensitive personal data under the Personal Data Protection Bill. Additionally, the Framework states that one of the determinants of sensitive Non-Personal Data, is that when it is re-identified, it would be re-classified as sensitive personal data or personal data. If derivative data can be traced to its source which is personal information, it would imply that such data falls under the regulatory ambit of the Personal Data Protection Bill. Sensitive Non-Personal Data cannot be treated analogously to sensitive personal data under the Personal Data Protection Bill and so needs to be treated separately. Another infirmity with the current definition of sensitive Non-Personal Data is that even without being attributable to an individual, significant amounts of non-personal data in the banking and capital markets sector may be Non-Personal Data, but still be business sensitive or confidential in nature and since such sensitive data does not relate to individuals, the definition of sensitive Non-Personal Data should be de-linked from the concept of personal sensitive data, as in many circumstances, an analogous comparison would not be possible. Accordingly, while the element of re-identification may be a factor which determines the sensitivity of Non-Personal Data if the re-identification cloaks such information with the colour of personal information, it still remains that the concepts of sensitivity operate in very different ways for personal and non-personal data.

The legislative treatment of sensitive Non-Personal Data would also need to be different as the primary risk of misuse of sensitive personal data is the unauthorised use of personal data in a manner violative of the individual's privacy, etc. However, for sensitive Non-Personal Data, the risks of harm are more likely to be in respect of data security and community harm, a risk that is much broader and needs more bespoke policymaking. As an example, in the European Union and elsewhere, much work has been done on ensuring use of data (e.g. through artificial intelligence etc.) does not create unjustifiable discrimination or contain bias. These are broader concepts dealing with principles of use and prevention of abuse of non-personal data that we believe should be addressed and the focus should pivot away from the comparison between "sensitive non-personal data" and sensitive personal data.

E. **Unstructured Data**: It is important to recognise that certain other types of data that are collected and stored with entities may be unstructured (i.e. data that does not have a pre-defined data model or is not organised in a pre-defined manner). It's not clear from the proposed framework whether the scope of data sharing includes all forms of Non-Personal Data, including unstructured data, and if in order to be in compliance with this proposed framework, a business entity or government agency possessing unstructured data will be

required to convert it into structured data in a format which is ubiquitous, so as to be used as a national resource for economic purposes. Such inclusion would be counter-productive to the ease of doing business norms in India and may act as a deterrent to foreign investment in (i) companies which are subject to this compliance obligation as well as (ii) greenfield projects in sectors likely to be impacted by such mandatory information sharing, since a significant amount of capital and resources would be dedicated to the generation of data valuable to the investor, which would risk being appropriated for public use as contemplated by the Framework

F. Classification & Exemption Norms: We are of the view that the wide scope of application and broad classification of types of data would lead to the imposition of compliance obligations which are unduly onerous and also restrictive to data custodians dealing with data. This may also result in differential standards being applied without such differential treatment meeting the touchstone of "*intelligible differentia"*. Without cogent exemptions from disclosure requirements, the extent of government intervention envisaged in the proposed Framework, in our view, is disproportionate to the need for such intervention and potentially discriminatory towards foreign companies. Accordingly, such legislation could be viewed as being in contravention of the principles laid down in the judgement of *Justice K.S. Puttaswamy v. Union of India* [(*2017)10 SCC 1*] which set out the principle of proportionality and legitimacy, and stated that the possibility of the State infringing the right to privacy can be met by the test suggested for limiting the discretion of the State, which is (i) the action must be sanctioned by law; (ii) the proposed action must be necessary in a democratic society for a legitimate aim; (iii) the extent of such interference must be proportionate to the need for such interference; and (iv) there must be procedural guarantees against abuse of such interference. We highly recommend laws and regulations adhere to these principles when proposing an interventionist approach to mandatory data sharing.

If Non-Personal Data is viewed as being sensitive irrespective of anonymisation, access to such Non-Personal Data would certainly be viewed as a breach of privacy, and would need to meet the aforesaid thresholds or be susceptible to challenge on the grounds of being unconstitutional.

G. Exclusions & Exemptions: In accordance with well-established principles of intellectual property rights, any data generated by employees of a company during the course of their employment, or by using the resources of the company should be owned by the employer. Consequently, such data cannot be owned by the community, or the employees of the company and ownership of those property rights solely vests with the employer.

The Framework should not view such data as community data as 'works for hire' are proprietary to an employer who has commissioned such 'work for hire'. The economic and statutory rights over data generated during the course of employment by employees and contractors cannot be reallocated in a manner that allows for co-existent and overlapping rights and privileges by virtue of reclassification as community data. This would disincentivise innovation and deployment of resources for generation of proprietary data by companies in India.

The Framework should also recognise that data being anonymised solely for the purposes of maintaining the confidentiality of the information and which will not be used for processing (as is a common practice in the financial services industry) should be excluded from the scope of Non-Personal Data.

2. Non-Personal Data Ecosystem

While we understand that stakeholders in the Non-Personal Data ecosystem have been classified as data principals, data custodians, data trustees and data trusts, we are unsure as to how a data principal is to be identified in respect of Non-Personal Data which, in essence, is devoid of any identifiers and personal data characteristics. In this scenario, the Framework creates an assumption that a data principal does not, and cannot find avenues to ensure his rights are not breached with respect to Non-Personal Data. Further, where Non-Personal Data is shared between two data custodians, it is unclear which data custodian needs to bear the obligation of adhering to the relevant consent requirements with respect to the data principals. Associated concerns are highlighted below:

A. Powers of data trustee:

The Framework places the responsibility of enforcing safeguards on sharing community Non-Personal Data, and implementing decisions that are in the interest of the data principals (to whom the Non-Personal Data relates), on data trustees and grants them powers to do so. These powers need to be narrowly defined as opposed to being inclusively defined, as is currently the case. Since the powers of a data trustee include having data custodians abide by certain obligations that the data trustee deems fit in the interest of the community data, this is a discretionary power which can be misused or misapplied. What has not been clarified is how data trustees will be identified, what objective criteria are to be met to ensure that the powers exercised by them do not prejudice the data principal, and measures to avoid conflicts of interest arising between the data trustee, the community and the data custodian. The exercise of powers by a data trustee must not be exploitative or arbitrary, and this will need to be factored into the legislation by adequate checks and measures being prescribed, along with appeal and redressal mechanisms.

For instance, a data trustee may impose unreasonable and arbitrary obligations on a particular class or category of entities without giving them any recourse since a data trustee is the delegated authority to decide how its community data is to be handled. The powers of a data trustee are seemingly arbitrary and pervasive in nature and appear to exceed the constitutionally permissible standards of delegated authority under the Indian legal regime. If adopted in their current form, they risk being challenged as defying procedural and substantive due process guarantees embodied in the Constitution of India.

B. Data Trusts & Custodians:

Data trusts are defined as institutional structures, comprising of specific rules and protocols for containing and sharing a given set of data. We seek to clarify whether public authorities managing data trusts will be subject to the duties and obligations of a data custodian, and where a public authority discharges such a function, what rights, obligations and liabilities of a data custodian would need to be discharged by such a public authority.

Separately, data custodians should not be treated on the same footing as data fiduciaries, or be burdened with the obligation to act in the "*best interest*" of the data principal, as this is (i) a fiduciary duty and (ii) is subjective in nature, without guiding principles outlining what constitutes "*best interest*" having been defined. Specifically, when dealing with community Non-Personal Data where there could be multiple communities involved, positing a fiduciary

obligation on data custodians would unfairly burden them, and such a practice would be a significant departure from international data protection practices and standards. We accordingly recommend that the requirement for establishing a fiduciary relationship between the data principal and data fiduciary should be deleted from the Framework.

3. Rights over Non-Personal Data

While the Framework provides an assurance that in case of private Non-Personal Data, algorithms or proprietary knowledge would not be considered for data sharing and only raw factual data that is related to the community would be compulsorily shared, the draft e-commerce policy seeks to give the government access to algorithms to check for biases. The Committee accordingly needs to clarify its stance on sharing of, and access to, proprietary data and preservation of intellectual property rights and align this with extant and imminent law. Foreign financial institutions in India use significant investments in algorithmic analysis of current trends in consumer analytics (for both domestic and offshore consumers).

A. While the Framework contemplates that data collected should be made available through a data exchange for stakeholders and that a data exchange should be able to accept data in any form, and produce output that is standardised and usable by all stakeholders, there are practical implementation challenges which we foresee. First, entities may maintain data in formats which, if compelled to be shared, would have no commercial value. Entities which inherently collect, or deal with structured data may also be disincentivised from disclosing the possession of such valuable data, or refrain from de-identifying, anonymising or segregating non-personal data from personal data (or performing any value additive processing of data which is subject to compulsory sharing). On the other hand, one situation that would justify compulsory data sharing is mandating Non-Personal Data generated by the government or government-funded activities, given that such activities are publicly funded and for the benefit of the people of India. However, private entities should be incentivised to share data on a voluntary or commercial basis.

B. While the Framework provides that benefits of data sharing should accrue to the data principal, responsibilities of the government as a data custodian and rights of the data principal over data collected by the government have not been defined.

4. Consent for Anonymisation

A. The Framework suggests that a data principal should also provide consent for anonymisation and end-use of such anonymised personal data at the time of collecting the personal data. This runs contrary to the rationale for anonymisation, which is to declassify data as personal data, and use it for purposes which the data principal does not need to consent to, or for purposes that have not been envisaged at the time of collecting such data. While the Personal Data Protection Bill prescribes the need to seek consent to anonymise data, while providing his/her consent for collection and usage of the personal data, we believe that excessive requirements to obtain consent at each stage for personal data or Non-Personal Data, are likely to render such anonymised data already collected unusable.

B. Additionally, from an enforcement standpoint, verifying collection of such consents poses operational challenges wherever an entity receives data from another entity and not directly from the data principal. If an entity is using anonymised data for its internal purposes and economic gain, and not sharing it with others, it is unclear as to whether consent from the

data principal could be argued to be necessary as this information is not personally identifiable information, and for information already anonymised, the data principal would be untraceable. The question of how personally identifiable information which is anonymised is treated would be better addressed in the Personal Data Protection Bill, since data derived from personal information would fall under the scope of the Personal Data Protection Bill. Additional Consent requirements in any non-personal data framework are, therefore, not necessary. Additionally, in cases where Non-Personal Data is shared between two data custodians, the Framework should clarify which data custodian needs to bear the obligation of adhering to the relevant consent requirements with respect to the data principals.

C. For Non-Personal Data that is collected from intermediaries, such intermediaries may not, or cannot identify which data principals are required to provide consent if data is anonymised and then transferred. Accordingly, recipients of data should be exempted from ensuring that intermediary entities have duly obtained consent. We recommend that the Committee reconsider the proposal mandating consent for anonymisation and consider introducing accountability based on a risk-based approach that focuses on developing best practices, policies, governance, risk assessment and management tools (such as data protection impact assessment and legitimate interest assessment).

5. Definition of Data Business

We understand that a new category of business called 'Data Business' has been introduced. Any entity which derives new or additional economic value from data, either by collecting, storage, processing, or managing such data upon reaching predetermined data-related threshold may be classified as a data business. The following clarificatory changes are required with respect to data businesses:

A. **Multiple Registration Requirements**: We understand that a 'Data Business' in the Framework has similar registration requirements as a 'significant data fiduciary' under the Personal Data Protection Bill wherein a data business must register with the Non-Personal Data Authority if it meets a certain data threshold. We would like to point out that several business entities which operate in India or operate from offshore but service the Indian market, are highly likely to be classified as a significant data fiduciary and a data business. The requirement of multiple registration, in this case, will create a complex environment for carrying on business.

B. **Mandatory Disclosures**: The Framework contemplates that a data business is required to share metadata which would be available for Indian citizens and Indian entities. After looking at such metadata, data requests can be made for the detailed underlying data held by such data business. If such a request is not serviced, then the Non-Personal Data Authority would evaluate such a request from various dimensions (including economic benefit perspective) and request the data business to share such data. We are opposed to this recommendation as such data being proprietary in nature and deriving independent economic value by virtue of it not being publicly disclosed, and being available only for data business's internal purposes. The disclosure of all data which belongs to a business (and not just Non-Personal Data) should be left to the discretion of that data business, and while incentives for disclosure may be provided by the government, we are opposed to legislation compelling private entities to disclose data. Mandatory disclosures may not be a sound practice in terms of competition law as well, as a competitor is not restricted from requesting such data of the

data business. We suggest that similar to the approach adopted in the Personal Data Protection Bill, the respective sectoral regulator must be consulted while framing the compliance requirements applicable to such entities. Also, considering the highly sensitive nature of financial data and secrecy obligations typical of the financial sector, regulated financial institutions should be exempted from this requirement to share either meta-data, unless specifically permitted on a reasonable basis in consultation with the sectoral regulator. Financial institutions routinely receive and process confidential and business-sensitive data, and disclosure of associated brand names, number of users, cumulative data, etc. at the time of registration and thereafter periodic disclosures on nature of data collected and processed, manner of processing and purposes for use of such data would be akin to the disclosure of confidential and business-sensitive data. This would be highly detrimental to market participants in the financial services industry.

6. Data Sharing

A. We are concerned that a blanket obligation is envisaged to be imposed on all entities dealing in Non-Personal Data to share data with the government if it falls under a sovereign, public good or economic purpose. The conditions for such compelled disclosures, as well as unambiguous conditions which would trigger such disclosures, require clarification. An established protocol for such disclosure is also required, including with respect to the method and process adopted for sharing of such data, appeal against such requests, and redressal mechanisms. The Framework proposes that data sharing practices are not only limited to meta-data but also the analytical data derived from the refinement or processing of such data and application of artificial intelligence to the Non-Personal Data. It could be argued that while the relevant Non-Personal Data itself might not be copyrightable, when it is processed through patented data processing technologies, it acquires a novel expression in itself and, therefore, conflicts with applicable intellectual property law. The proposal as currently stands may go against its own objective of a level playing field and supporting innovation. For example, data shared by large firms with smaller firms without any financial compensation or metadata which will have to be shared by firms who have financially invested in artificial intelligence or machine learning tools without any compensation is likely to eventually discourage investments in innovation. Global firms may accordingly exclude India from their innovation projects if there are concerns with regard to having to share their intellectual property or the derived data based on such intellectual property. Disclosures pertaining to what data elements are collected, where the data is stored, standards adopted to store and secure data, nature of data processing, etc. if publicly made, also pose a significant security risk. Any upload of metadata (which provides an idea of the nature of data stored and processed by the data business, underlying data principal base, classification, schema etc.) to a public registry by entity pose potential security and/or confidentiality risks.

B. The compulsory data sharing provision as currently framed, may be unconstitutional unless it clearly defines the specific instances where such data sharing with the government is necessary in the interest of public welfare and also provides exceptions to such data sharing requirements. Given the highly litigated definition of public policy under Indian arbitral law, and previous precedent of protracted litigation surrounding widely defined legislative definitions and the potential for misuse, this provision is likely to be contested.

C. More broadly, the implementation of this Framework could prove to be counterproductive to foreign investments and business innovation. Indian companies and start-ups might also

prefer taking their innovations abroad to avoid having to comply with the mandatory data-sharing norms. As for foreign entities which have invested in the Indian market and have spent a significant amount of time developing their businesses in India, they could exit the market. While foreign entities operating in India are required to share metadata, they would not have the ability to access this metadata, as this access has been restricted to Indian companies. This approach will likely operate adversely against foreign companies which would not be treated on par with their Indian counterparts, and consequentially discourage foreign entities from setting up business operations in India. Though the Framework appears to favour access for India based start-ups, there is nothing preventing a competing business concern (regardless of whether Indian or foreign-owned) from raising a similar request for underlying data held by a foreign financial institution to share its customer base/products. This would also be detrimental to foreign entities from a competitiveperspective. While "*fair, reasonable and non-discriminatory based remuneration*" is the intended principle used for determining the valuation of data which is mandated to be shared "for reasons of overriding public interest", even where the value-added by private enterprise is valuable, the definitions of these terms are elastic and subject to interpretation. While our members are not opposed to the concept of data sharing, mandating sharing of data on the basis of the idea that 'economic privileges will be considered inherent to the data itself' and attempting to define parameters to determine valuation, are commercially infeasible and fetters free trade. When attempting to mandate sharing of data between a foreign and Indian enterprise or between competitors, the principle of non-discriminatory pricing in practice, would be difficult to adhere to, and accordingly should be removed from the Framework.

D. The Framework contemplates the creation of multiple adjudicatory bodies which have potentially overlapping jurisdictions for handling data-sharing issues. This is likely to have an adverse impact on innovation and the start-ups and also the ease of doing business in India, which is contrary to the intent of the Non-Personal Data Regulations.

E. Any requirements in this area should not impose onerous or repetitive obligations on private companies that incur compliance costs associated with the transfer of large quantities of Non-Personal Data. There is also an imminent requirement to create a safe harbour to exempt data businesses against any liability that may arise as a consequence of sharingNon-Personal Data, which should extend beyond the indemnification against vulnerabilities that the Framework contemplates for adhering to standards.

7. Data Localisation

A. The Framework provides that "any Sensitive Non-Personal Data may be transferred outside India, but shall continue to be stored in India". However, this language read with other references in the Framework is ambiguous with respect to whether the mirroring requirement allows for such data to be processed offshore and then returned to India which, if adopted, would attempt to impose obligations on data processed extraterritorially and would be impractical in terms of enforcement. The ensuing local storage and processing requirements under the Framework for sensitive Non-Personal Data and critical Non-Personal Data (which will be defined when the Government defines critical personal data) would be contradictory to the intent of the Framework of driving innovation and societal welfare. In the financial sector as well as the EU's Regulation on a framework for the free flow of non-personal data, it is well recognised that borderless flow and use of data is paramount in ensuring effective risk management. The data localisation restriction would

also affect AML and KYC processes, very vital to both of which is access by financial institutions and financial regulators of relevant information. The movement and storage of Non-Personal Data across national borders is essential for regulatory compliance purposes, devising new products and improving overall customer service. The restrictions contemplated in the current Framework on cross-border data flow for sensitive and critical Non-Personal Data would accordingly cause compliance hurdles for multinational companies doing business in India.

B. Many firms, including local start-ups, rely on cloud storage for data storage purposes to reduce costs and have access to up-to-date technology which is innately borderless. Firms which operate in multiple jurisdictions also find it easier to support their operation around data by storing it in one place. The localisation requirement contemplated under the Framework places an unnecessary compliance burden and cost on such entities.

C. Therefore, we suggest, that the Government reconsider restrictive legislations with respect to storage and processing of data.

D. The provisions of the Framework in its current form transgresses permissible limitations that can be imposed on the exercise of constitutionally guaranteed freedoms enumerated under the Constitution of India. We are also concerned that imposing obligations on entities to mandatorily share data for policymaking, economic and other purposes would fall foul of reasonable restrictions that can be lawfully imposed on the exercise of free trade, occupation, or business.

8. Rationalisation of Cross Border Flows

A. The movement and storage of data across national borders is fundamental to manage risks across affiliates and comply with financial regulatory requirements across jurisdictions. Data localisation, which restricts the free flow of data, creates barriers to data sharing, whereas such sharing is essential for consumers and institutions to function seamlessly across jurisdictions. The recently published World Economic Forum's report on Data Free Flow with Trust[5] includes a matrix mapping existing international regulatory tools to build openness for data flows alongside trust to ensure that domestic legitimate public policy objectives are met – even among countries with different legal systems. The report includes a set of policy recommendations for advancing the Data Free Flow with Trust architecture. It is also worth noting other international practices in this regard – for example, the EU Legislation on free flow of non-personal data[6] and the GFMA Data Mobility principles[7], which could inform the Framework and ensure that policies do not add barriers to trade or impede the functioning of cross-jurisdictional banking and commerce.

9. Non-Personal Data Authority

[5] See WEF Data Free Flow with Trust (DFFT) Report: http://www3.weforum.org/docs/WEF_Paths_Towards_Free_and_Trusted_Data%20_Flows_2020.pdf

[6] See European Commission Free flow of non-personal data: https://ec.europa.eu/digital-single-market/en/news/free-flow-non-personal-data

[7] See GFMA International Principles to Improve Data Security and Mobility to Support Global Growth: https://www.gfma.org/wp-content/uploads/2019/05/international-principles-to-improve-data-mobility-privacy-and-security-website-final.pdf

A. In addition to a Data Protection Authority (**"DPA"**) under the Data Protection Bill, the Framework wishes to set up a separate regulator for governing Non-Personal Data. It is crucial to avoid duplicative and potentially conflicting regulations, standards, rules, and guidelines. While Non-Personal Data would need to be treated very differently from personal data owing to its inherently different characteristics, there should be a single regulatory authority for data within India, which can be the DPA. This would ensure that jurisdiction determination and overlap between multiple regulators and a fragmented regulatory approach is avoided. Multiplicity of regulatory authorities coupled with definition capable of broad and overlapping interpretation creates lack of clarity, difficulties with implementation, drives up costs of compliance, slows the pace of business, and frustrates the good objectives of a simpler, principle-based, light-touch approach to regulate data and protect data principals, in conjunction with sectoral regulators.

B. We observe that the Framework does not contemplate situations use of mixed datasets (i.e. banking sector datasets which comprise of community Non-Personal Data and Non-Personal Data which is business sensitive). It needs to be clarified how the Data Protection Authority, the Competition Commission of India and the Non-Personal Data Authority will regulate such a data set. The Framework also leaves out sectoral regulators, such as RBI, from regulating such data sharing activities.

C. We recommend that the Committee adopt the EU Regulation's concept of free flow of non-personal data and approach to appointing a single point of contact for each regulatory authority responsible to not only deliberate and decide on the ways to regulate such mixed data sets but also monitor worldwide development to build interoperability and favourable policy environment for the data economy.

D. From an implementation point of view and in order to maximise the efficiency of the Framework to achieve the objectives outlined by the Committee, a sectoral approach is recommended where RBI, SEBI, the Insurance Regulatory and Development Authority (**"IRDA"**) and the International Financial Services Centres Authority could be the nodal authorities for their respective industries, and frame industry-specific regulations, instead of setting up a separate Non-Personal Data authority. The creation of a separate authority adds complexities in terms of defining regulatory purview, and a simpler approach would be to delegate powers to sectoral regulators who are already familiar with their sectors. Depending on the need to regulate Non-Personal Data in a particular sector, the existing sectoral regulators, if any, or the relevant government department or ministry can issue appropriate rules and regulations. The government can consider releasing an overarching policy on voluntary Non-Personal Data sharing, which can be used as a common minimum guideline for relevant sectoral regulators around the sharing of certain kinds of data. In any event, financial data or private data of financial institutions or associated entities, including global service centres, on which such financial institutions or entities have proprietary rights should be exempted from the purview of this Framework. To this end, it would be immensely beneficial for existing sectoral regulators to be consulted by the Committee before the next consultation is published.

E. The Framework also needs to acknowledge that the banking and financial sector has an implicit duty of confidentiality towards its customers and as information is highly confidential and highly business-sensitive even where it does not relate to an individual, this does not make such information less sensitive. Such data should not be in the public domain

and needs more consideration in terms of use cases which are tacitly accorded approval by law, such as for portability in the financial services context (e.g. potentially sharing information for purposes of know your customer or anti-money laundering solutions or more accurate credit risk monitoring and use of credit rating data).

PART B

II. Other Specific Concerns

This section deals with specific concerns our members have in relation to the Non-Personal Data which have been set out in brief detail:

1. **Existing Avenues for Data Collection**: The government and various law enforcement agencies are already empowered under various internet, telecom, interception, banking, and securities laws to access data for various reasons. The Information Technology (Amendment) Act, 2008 allows authorised agencies to access personal information held by the private sector for investigations. Banking laws also require proactive/systematic disclosure of private sector activities and information, for instance, the RBI can require financial institutions, non-banking companies and corporations to furnish information on a regular basis as may be specified by RBI through a general or specific order. The Securities Exchange Board of India Act, 1992 also allows access to information by the government through SEBI, which is empowered to access private-sector data related to securities market. It even contains provisions to penalise persons who fail to furnish the required information. In light of such powers being available by the government under existing laws, we do not see the need for having such overreaching data sharing obligations in the Framework as specific laws exist to cater to information being sought for investigative processes.

2. **Treatment of Foreign Data**: Certain sections of the Framework suggest that the Framework intends to govern and regulate data present in a global dataset that pertains to individuals who are not Indian nationals and may be collected in foreign jurisdictions. The rationale of inclusion of data that pertains to non-Indian nationals and which is collected in foreign jurisdictions (other than India) as a category of private Non-Personal Data is unclear. It is important to recognise that there may be corresponding data governance frameworks in place in the jurisdiction from which the data has originated which could result in a conflict of laws. This underscores the importance of recognising the data principal as the owner of the data and not the data custodian, of which there may be many, which are present in different jurisdictions. Any implication that foreign data will not benefit from the protections accorded in its home jurisdiction and may also be mandated to be shared in India without any incentives or protections, may deter foreign data principals from wanting their data being present in India. This may also disrupt India's current status as a global service centre for multinational companies. Similar to the suggestions made with respect to the Data Protection Bill, we recommend that clear carve-outs be put in place for foreign data, which is likely to be subject to foreign data protection laws. The Framework would need to provide for recognition of, and compliance with applicable compliance obligations under foreign laws, in accordance with conflict of laws principles. The inclusion of foreign data within the purview of the Framework does not align with the stated objectives of the Framework and should be reconsidered by the Committee. With a view to encouraging data processing businesses to continue in India, specific carve-outs and exemptions should be considered for international financial institutions which have, or will set up global service centres located in India. The Committee should also consider the feasibility of enforcement of obligations imposed under the Framework against foreign data custodians and ideally limit the purview of the Framework.

3. **Best Interests of Data Principals & End Use:** The Framework suggests that personal data that is anonymised should continue to be treated as Non-Personal Data of the data principal. This is guided by the principle that where Non-Personal Data is derived from personal data of an individual, the data principal for personal data will continue to be the data principal for the Non-Personal Data, which should be utilised in the best interest of that data principal. While the principle of "*beneficial ownership*" is intended to ensure that a data principal benefits from the end-use(s) of its data, the Framework needs to provide for parameters which determine what the legislative objective of this data sharing are expected to accrue to the data principal and implement such mechanisms to enable such benefits accruing to the data principal. Without such parameters, the concept would likely not be translated into legislatively prescribed obligations, either as a positive list or negative list.

4. **Phased Implementation:** To ensure a stable implementation of the Framework, a phased approach for cross-sector data sharing could be considered by the Committee similar to the manner of implementation contemplated in the EU-General Data Protection Regulation and the Personal Data Protection Bill, in the 2018 iteration. Mandatory data sharing in the financial sector has been implemented via Open Banking regulations in Europe, the UK and Hong Kong as well and guidance on the implementation process can be obtained from the issues in implementation in other jurisdictions. The current proposal does not contemplate a phased implementation and implies directly engaging in cross-sectoral sharing without having considered safeguards and experience from other jurisdictions. Australia's Consumer Data Right explicitly recognised this concern and has taken a deliberately phased, sectoral approach.