January 31 2021

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 revised Non-Personal Data Governance Framework, 2021

The Asia Securities Industry & Financial Markets Association (**ASIFMA**)[1] welcomes the opportunity to comment on the revised draft Non-Personal Data Governance Framework, 2021 (**Revised Framework**) as stakeholders from the financial services sector, and with the lens of improving 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 Revised Framework, prepared and submitted in collaboration across ASIFMA and its affiliates' members. Our response focuses on the potential impact of the Revised 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 membership.

Overview

The Revised Framework provides much-needed clarifications to the concepts set forth by the Committee in the Report on Non-Personal Data Governance Framework, 2020 (**2020 Framework**). It is clear that the Committee intends for the Revised Framework to culminate into legislation independent of the Personal Data Protection Bill, 2019 (**PDP Bill**), and govern all classes of data which are not classified as (i) personal data, (ii) reidentified anonymized data, and (iii) mixed data sets comprising of personal and non-personal data characteristics. We appreciate that the Committee has acknowledged the various ways in which the objectives set out in the 2020 Framework could fall under the ambit of the PDP Bill causing an overlap in the scope of the two legislations, as well as duplicity of compliance obligations.

The focus of the Revised Framework, as per our understanding, is mainly on high-value datasets which are intended to be the only datasets subject to data-sharing obligations in the interest of community welfare. Unlike the 2020 Framework, the Revised Framework does not delve into the various classifications of non-personal data or impose storage and transfer restrictions on such classes of data.

[1] ASIFMA is an independent, regional trade association with over 140 member firms comprising a diverse range of leading financial institutions from both the buy and sell side, including banks, asset managers, law firms and market infrastructure service providers. Together, we harness the shared interests of the financial industry to promote the development of liquid, deep and broad capital markets in Asia. ASIFMA advocates stable, innovative, competitive and efficient Asian capital markets that are necessary to support the region's economic growth. We drive consensus, advocate solutions and effect change around key issues through the collective strength and clarity of one industry voice. Our many initiatives include consultations with regulators and exchanges, development of uniform industry standards, advocacy for enhanced markets through policy papers, and lowering the cost of doing business in the region. Through the GFMA alliance with SIFMA in the United States and AFME in Europe, ASIFMA also provides insights on global best practices and standards to benefit the region.

The elimination of the categories of 'sensitive non-personal data' and 'critical non-personal data' while resorting to a single classification of a 'high-value dataset', would likely reduce the compliance burden on the data custodian, and relieve him from the need to adhere to varying obligations for different types of non-personal data.

The Committee also recognizes certain situations where high-value datasets may not be shared. In our recommendations below, we provide for specific categories of datasets which should benefit from this pre-existing exemption from data-sharing under the Revised Framework.

We also appreciate that the Committee has acknowledged that the implementation of the Revised Framework, as legislation governing non-personal data, may result in domestic and foreign entities incurring high transaction cost, which would discourage entities from entering into and/or continuing operations in the Indian market. We are happy to assist the Committee by providing global market trends and collated stakeholder views to improve the Revised Framework and help avoid burdening business entities with exorbitant compliance cost. We at ASIFMA are also of the collective opinion that certain changes, clarifications, and omissions need to be made to the Revised Framework to ensure unhindered business, ease of compliance and economic growth for all stakeholders.

Having closely followed global and regional policy developments around regulation of non-personal data and free flow of data across borders, ASIFMA would like to offer our members' views concerning the potential ramifications of the approach in the Revised Framework. We foresee challenges in the implementation of the Revised Framework, and potential unintended consequences caused by the lack of clarity on the registration and screening process of a data trustee, continued emphasis on obtaining consent for anonymised data and mandatory data sharing obligations on data custodians.

With the PDP Bill on the anvil, we understand that the Committee intends to convert the Revised Framework into an enforceable piece of legislation soon. We strongly believe that the Committee's approach in obtaining stakeholder feedback is commendable and will contribute to the making of a keystone non-personal data governance framework. We hope that the Committee will keep stakeholders, such as ASIFMA, updated on any developments in the promulgation of the non-personal data framework and provide ample time to review and provide feedback on its upcoming iterations. We request that the Committee and the Ministry of Electronics and Information Technology prescribe a timeline for such a consultation process and continue engaging with the public and other stakeholders. An open and transparent consultation process, including written feedback and face-to-face discussion with stakeholders and various regulators, will help mitigate any uncertainty or ambiguity in the structure and content of the Revised Framework.

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

Yours faithfully,

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

Recommendations for the Revised Framework

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

Our recommendations are divided into **Part A**, which deals with provisions and concepts which the Committee should provide a more comprehensive consideration of, and **Part B**, which highlights certain provisions of the Revised Framework which should be reconsidered for their ability to cause implementation challenges and contradict the global precedent on treatment and regulation of data.

PART A
Definitions and Scope

1. **Scope & Definitions**: The Revised Framework has amalgamated previously defined categories of non-personal data, and promotes the idea of mandatory data-sharing of high-value datasets which are reckoned to be beneficial to the community at large. The issue remains, however, that the definition of 'community' continues to be vast and ambiguous. The Committee has not defined the abstract concept of 'public good' either. This enables any set of people, for any vague reason, to request high-value datasets from data custodians. We recommend that the Committee disclaims the concept of community data altogether and restricts data-sharing to high-value datasets only. In addition to this, we also recommend that high-value datasets are clearly defined [*refer Part A Section 7(c)*] and only allowed to be shared if the benefits from obtaining such data incontestably outweigh the cost of producing it and making it available.

   We also note that inferred or derived data may also constitute a high-level dataset subject to mandatory data-sharing requirements under the Revised Framework. Owing to the possibility that a 'derived dataset' may be copyrightable or proprietary, and therefore exempted from data-sharing [*refer Part A Section 2 below*], the Committee should provide clarification regarding the types of derived datasets which will be expected to be shared as compulsory sharing, if misused, or excessively broad in its ambit could be value-erosive for data businesses.

2. **Carve-outs for Certain Types of Data**: Databases constitute literary works under the Copyrights Act, 1957, upon which copyright subsists. The current position in law remains that original literary works (including databases created on a computer, using a programme) is copyrightable. Despite the extant legal position the Revised Framework has carved out data extractions done on pre-set data fields, as not copyrightable because there is no unique way of applying creativity to the preparation of such databases. A similar position was also taken in certain judgments where the court held that unless a work has been prepared by one's own labour and skill, and there is originality and creativity in its generation, it will not be protected under copyright. However, such pre-set data fields which, despite being generated *without an added element of creativity*, may constitute proprietary and business-sensitive information even if not copyrightable. This includes, but is not limited to, email records, business plans, operational processes, contractually agreed upon confidential information, employee matters, tax matters, regulatory matters, data forming *proprietary information* (even if not copyrightable) under imminent Indian and extant foreign laws. The provisions of the Revised Framework must expressly carve out all types of *proprietary data* and *copyrighted data* from the ambit of those datasets for which data-sharing is mandatory. We recommend that in the interest of upholding legitimate privacy and confidentiality interests of data custodians and creating more confidence in the Revised Framework, that this provision be eliminated from the

Revised Framework to prevent it from being an enabling the misuse of proprietary data and mixed datasets which constitute trade secrets and are business sensitive even if not copyrightable.

3. **Mixed Data-Sets**: The Revised Framework provides that datasets that are made of 'inextricably linked' personal and non-personal data will be governed by the rights and obligations provided under the PDP Bill. However, the Revised Framework does not explain what the term '*inextricably linked'* indicates, and the treatment of mixed datasets in which the personal data and non-personal data elements are not 'inextricably linked'. In the absence of clarity, we have assumed that the requirement to be 'inextricably linked' was borrowed from Section 2.2 of the Guidance on the Regulation on a framework for the free flow of non-personal data in the European Union issued by the European Commission on May 29, 2019[2] (**EU Guidance**). The Committee should provide a clear classification of the term "inextricably linked". The EU Guidance on the related term clearly outlines that not all mixed data sets will be governed by the GDPR unless they are "inextricably linked datasets" and provides an illustrative list of examples. A similar clarification in the Revised Framework is necessary to address concerns regarding the possibility that mixed datasets may be partly regulated by the non-personal data legislation to be promulgated and partly by the PDP Bill should they not be inextricably linked.

4. **Meta-data**: We understand that meta-data has been defined as data that provides information about the data collected by data businesses/data custodians and must be shared with the NPDA mandatorily [*refer Part A Section 5(c)&(d) below*]. The Revised Framework contemplates the storage of all meta-data shared by the data businesses digitally, in meta-data directories managed by the NPDA. It is pertinent to note that the Revised Framework does not make any mention of "*data trusts*" which were defined in the 2020 Framework as "*institutional structures, comprising specific rules and protocols for containing and sharing a given dataset*". The Committee must clarify if a meta-data repository is the same as a data trust as defined in the 2020 Framework or if the concept of data trusts has been intentionally dropped from the Revised Report and is intended to be removed from the non-personal data legislation to be promulgated. The Committee must also provide a more comprehensive technology architecture plan for ensuring the security of the meta-data stored in directories.

   Additional clarification on whether the NPDA or government may transfer such meta-data outside India to third parties is needed. This could include instances where entities which are not registered in India, but planning to start operations in India, are permitted to access meta-data and request high-value datasets for a fair consideration (with a transparent valuation methodology prescribed by the NPDA). While we assume that this may be the case, given that the Committee has consistently expressed its intention to capitalize on non-personal data, remains necessary.

5. **Data Business**: The definition of a data business has been expanded in the Revised Framework to include all entities, whether government or private, which collect and manage personal and/or non-personal data. The Revised Framework also retains the registration obligations for such data businesses, which collect and manage data beyond a prescribed threshold. Such threshold will be prescribed by the Non-Personal Data Authority (**NPDA**) in the future. In our recommendations to the 2020 Framework, we had pointed out that the Committee has not established how a *data business* under the 2020 Framework is different from a *significant data fiduciary* under the PDP Bill. The Revised Draft clarifies this by *expanding* the scope of a data business to include an entity which not only collects non-personal data but also personal data.

[2] https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2019:250:FIN

To this end, the thresholds for registration of a data business under the Revised Framework, and the thresholds for a significant data fiduciary under the PDP Bill should be harmonized. The Revised Framework would likely give rise to multiple registration requirements as a consequence of including personal data within the definition of a data business. If this definition is adopted in the upcoming non-personal data legislation, any entity processing a prescribed threshold of personal data will need to register with the Data Protection Authority under the PDP Bill as well as the NPDA under the Revised Framework.

Other concerns and queries regarding the obligations on a data business under the Revised Framework include:

a. **Ongoing obligations**: Clarifications regarding any ongoing compliance obligations of data businesses under the Revised Framework are necessary to enable data custodians to analyse costs and business risks and prepare for compliance. The Revised Framework should include a description of all additional compliances following the one-time registration with the NPDA. This could include the requirement to undertake data protection impact assessments, maintenance of records, etc. akin to a significant data fiduciary under the PDP Bill. This ambiguity should be addressed by clearly prescribing an exhaustive list of duties of a data business.

b. **Multiple Registration and Disclosure Requirements**: Entities in the financial services sector, financial institutions, and banks (including GCCs in IT & ITES) are already heavily regulated and comply with not only local regulations but are also bound by contractual obligations through extra-territorial laws. The additional registration requirement contemplated in the Revised Framework will add to the regulatory burden and make operations complex. Furthermore, financial institutions routinely receive and process confidential and business-sensitive data. Accordingly, the disclosures required to be made for use of such data would be highly detrimental to market participants in the financial services industry. Thereby data businesses may register or report to the NPDA as a one-time registration/reporting and the periodic disclosures thereafter on the nature of data collected and processed, manner and standards adopted in the processing of data, storage of data and purposes should be made to the sectoral regulators.

   Financial institutions are also required to make disclosures to the sectoral regulatory body regarding their ownership, operations, capital adequacy, etc. Given the highly sensitive and proprietary nature of the operations of the financial sector, there are robust mechanisms already in place for new entrants into the financial services sector. Under extant law, financial institutions are required to adhere to ongoing security and audit compliances prescribed under applicable federal laws. Therefore, duplicitous obligations to share meta-data and register with a new authority are not only cumbersome but also add to the operational inefficiencies for global banks to operate and expand in India.

c. **Conflict with Sector-Specific Laws**: Mandatory data-sharing under the Revised Framework may result in conflict with existing legal obligations on data custodians. Considering the highly sensitive nature of financial data and the secrecy obligations typical of the financial sector, regulated financial institutions should be exempted from this requirement to share meta-data, unless specifically requested, and if shared voluntarily, then with the consent of the sectoral regulator. In December 2014, the

RBI released a Charter of Customer Rights for all banks including the right to privacy as a basic right of all bank customers. In November 2017, the Insurance Regulatory Development Authority of India ("**IRDAI**") issued the IRDAI (Outsourcing of Activities by Indian Insurers) Regulations, 2017 ("**Outsourcing Rules**") to ensure that insurers follow prudent practices on management of risks and effective oversight and adequate due diligence with regard to outsourcing activities by insurers. These Outsourcing Rules identify specific classes of data which is barred from outsourcing by insurers and includes investment-related data and NAV calculations. The Committee should note that while these types of datasets may classify as non-personal data under the Revised Framework, the same are highly proprietary and business-sensitive in nature and already regulated by sector-specific regulators. Any obligation contemplated under the Revised Framework should be put under advisement of the existing sectoral regulators to avoid clashes.

d. **Carve-outs for Financial Services Sector**: Under the Revised Framework meta-data about the data collected by a data business can be assessed by data trustees and relevant subsets of such data can be requested for sharing. It is our considered view that despite comprising of non-personal data, high-value datasets may include business-sensitive information which cannot be shared by a data business. A few examples of such datasets in the financial services sector which should be excluded from mandatory data-sharing include:

    i. **Unpublished price sensitive data and material non-public information**: High-value datasets may include 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 extant regulatory framework. Inclusion of such data within the definition of non-personal data could lead to unintended conflict between other regulatory frameworks and the Revised Framework leading to unintended consequences. Accordingly, such material non-public information and unpublished price sensitive information received by an entity should be exempted from data-sharing.

    ii. **Customer information**: The banking and financial services sector has an implicit duty of confidentiality towards its customers. Given the nature of its operations and information collected/received/managed, the information continues to be sensitive and critical in nature despite not being attributable to a person. Therefore, datasets pertaining to customer information should be identified by the NPDA, with assistance from regulators of the financial services sector and exempted from the data-sharing norms under the Revised Framework.

    iii. **Business/market-sensitive information**: Even without being attributable to an individual, significant amounts of data in the banking and capital markets sector may be business sensitive or confidential in nature (for instance, corporate client account information and trading positions). While such information needs to be available to financial institutions to supervise participation in global markets, it cannot be made subject to mandatory data-sharing with non-financial institutions.

iv. **Dynamic Datasets**: A comprehensive list of datasets, in line with existing sector-specific regulations, should be identified as exempted from the data-sharing norms of the Revised Framework and be subject to a hybrid sectoral regulation model which enables the NPDA to intervene only if the sectoral regulator calls upon it for such intervention. This list should contain not only those datasets which are explicitly confidential or business-sensitive in nature but also include those datasets which are regulated under extant Indian and foreign laws and would pose operational challenges and cause diminution of value if shared freely. For example, even including the location of where data is stored in our data registration could be a breach of business continuity and operational resilience requirements under both Indian law and third-country laws as well as good practice in terms of ensuring business continuity arrangements are kept confidential, in addition to being a breach of outsourcing contracts which may include confidentiality requirements.

Such excluded high-value datasets should be (i) notified prior to the implementation of the Revised Framework, and (ii) notified by the NPDA over time as needed

The recommendations under this Section 5 will also foster innovation and entrepreneurship within the financial services sector by reducing the registration and compliance burden on new entrants and allowing them to adapt business models based on the supervisory relationships with their respective regulators.

6. **High-Value Datasets**: The concept of high-value datasets has been elaborated upon to include all such datasets that are beneficial to the community at large, and will act as an institutionalised mechanism for data communities to exercise their rights over their non-personal data. We understand from the reading of the Revised Framework that the Committee has steered clear from the classification of non-personal data into sensitive and critical and emphasizes on the utility created by datasets when shared with the public at large. The idea of opting for high-value datasets appears to be borrowed from the European Commission's Directive of open data and reuse of public sector information dated June 20, 2019[3] (**Open Data Directive**). As per the Open Data Directive, depending on the GDPR and EU Guidelines, high-value datasets may include cover postcodes, national and local maps (geospatial), energy consumption and satellite images (earth observation and environment), in situ data from instruments and weather forecasts (meteorological), demographic and economic indicators (statistics), business registers and registration identifiers (companies and company ownership), road signs and inland waterways (mobility).

   We recommend that the Committee also adopts a similar approach by (i) formulating a specific list of high-value datasets, (ii) making procedural and regulatory arrangements for their use instead of relying on a blanket classification as any dataset which is beneficial to the public at large, and (iii) empower the NPDA and relevant sectoral regulators to make revisions to the list of high-value datasets, by public consultations, from time to time to ensure that the Revised Framework is meaningful and appropriate for governance of non-personal data.

7. **Data Trustee**: We note that the Committee has clarified that government organisations or non-profit organisations such as Section 8 companies under the Companies Act, 2013, a

[3] https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1561563110433&uri=CELEX:32019L1024

society or trust, which is responsible for the creation, maintenance and sharing of high-value datasets in India will classify as a data trustee under the Revised Framework. These data trustees are entrusted with the responsibility of handling non-personal data of such community, and are obligated to ensure that (i) they exercise a duty of care in ensuring that the high-value datasets which are requested from data custodians are used only in the interest of the community, and (ii) no harm is caused to any person of the community by the reidentification of their non-personal data. Some specific queries and concerns with respect to data trustees under the Revised Framework are as follows:

a. **Multiple Data Trustees/Communities**: A data trustee will be responsible for at least one high-value dataset, either created by its community or requested from a data-custodian. While we do not debate the idea that a single community may have multiple datasets, the Revised Framework continues to remain ambiguous regarding the possibility of a data trustee taking cognizance over high-value datasets of multiple communities. This could result in entrusting a single entity with large sets of granular high-value datasets of various fields. Without a robust mechanism in place for the regulation of data trustees, the chances of misuse of data and abuse of power by a data trustee are high and, therefore, clarification is sought on this subject from the Committee.

b. **Registration Process For Data Trustee**: While the Revised Draft does not explicitly specify this, we are of the considered view that a data trustee, by virtue of classifying as a data business, will be required to register with the NPDA. To this end, the Committee should provide a comprehensive process for registration as a data trustee, including the eligibility criteria and documents required to be submitted. Each data trustee should be screened by the NPDA (and applicable sectoral regulators, such as RBI in the case of financial data) before it is allowed to request data sharing. The Committee's attention is directed to the fact that while government and non-profit organisations may seem to be most suited to play this role, they are not free from bias or conflicts of interest and may not have resourcing or capability for cybersecurity or operational resilience expected of financial services institutions.

c. **Pre-Determination of High-Value Datasets**: We recommend that the Committee should include provisions enabling data trustees to pre-determine the type of high-value dataset they require based on engagement with the relevant data businesses. Additionally, the Committee may consider an ombudsman-based approach whereby an authorised member of the NPDA carries out a diligence or conflict check to ascertain that data-trustees cannot abuse their powers to harass data custodians who may have a conflict of interest with the data trustees, (unless such data sharing is expressly consented to by both parties).

d. **Duty of Care**: The Committee should also elaborate upon the 'duty of care' of data trustees. Apart from the obligation to prohibit the use of high-value datasets for any activity (other than the benefit of the community), the duty of care should include obligations such as:
    i. refraining from reidentification of non-personal data, further disclosure of high-value datasets obtained from data custodians to other data trustees, companies, government bodies, persons, etc.;
    ii. a mandatory periodic audit of the non-personal data held by the data trustee to ascertain whether such data is being used for the purpose for which it was obtained; and

iii. if any dataset in the possession of a data trustee which is not being used for the benefit of the community or has become redundant, then the data trustee must be obligated to destroy such dataset as per guidelines provided by the Committee;
iv. accountability to the Data Protection Authority under the PDP Bill, especially in the context of any mixed data sets or data which may be at risk of deanonymisation.

e. **Hybrid Sectoral Approach**: The Committee should consider amending the Revised Framework to make sectoral regulators the prescribed data trustees for financial institutions. A single regulator will help ensure that there are no conflicts between laws and provide a single point of contact for all financial services sector related issues. Sectoral regulators such as RBI, Securities Exchange Board of India, the IRDAI and the International Financial Services Centres Authority should be entrusted with the role of data trustees for the financial institutions which they already regulate under extant laws. This approach would help ensure that the rights over the high-value datasets derived from the financial services sector are not scattered across multiple bodies which may or may not have been conferred regulatory powers, or have well defined and distinct jurisdictional purviews under applicable law. We submit that a hybrid sectoral approach would enure effective implementation of the guidelines provided in the Revised Framework without compromising the integrity of the financial services sector.

PART B
Other specific concerns

This section deals with specific concerns our members have in relation to the Revised Framework which have been set out in brief detail:

1. **Data Anonymization**: The consent requirement for anonymisation has remained unchanged in the Revised Framework. The data fiduciary is required to obtain consent for anonymisation and end-use of the personal data collected from the data principal. 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. In addition to this consent requirement, the Revised Framework also imposes an obligation on data collectors to inform the data principal in advance about any intended anonymisation their data may be subject to and provide the data principal with an option to opt-out of such anonymisation.

   We find that the imposition of such obligations is *ultra vires* the object of the Revised Framework which provides for the regulation of non-personal to enable unlocking economic benefit. Chapter II of the PDP Bill prescribes the obligations of a data fiduciary including the details of all the requisite disclosures which need to be made by him at the time of collection of personal data. Any other obligations concerning further disclosures at the time of collection of personal data may *only* be prescribed by the PDP Bill and the Revised Framework does not have the power to impose excessive obligations for collection of personal data. Furthermore, the Revised Framework does not provide any guidance on how pre-existing anonymised data will be treated and whether such data will be rendered unusable for any specific end-use until valid consent is obtained for the proposed end-use.

We also submit that the requirement under the Revised Framework to revoke consent if personal data is not anonymised despite obtaining consent for anonymisation is vague and evokes confusion on account of: (i) who will have the right to exercise such revocation of consent, and (ii) whether the data fiduciary is supposed to be periodically notified the data principal about the status of his/her personal data under the Revised Framework. This is likely to be a very onerous obligation which is not only impractical to comply with, but also enforce. This also runs contrary to the requirements laid down in the PDP Bill, that merely requires the data fiduciary to provide a notice to the data principal, explaining the purpose of data collection. Practically speaking, consent to anonymization may also cause considerable confusion to the data principal, who, (i) under the PDP Bill, is being asked to consent to the collection and use of personal data (where anonymisation is generally seen as a positive step to increase privacy) and (ii) simultaneously being asked to consent to anonymization under the Revised Framework wherein opting out of anonymisation would be an additional right granted to him to ensure data protection (i.e. to avoid anonymised data being made public and possibly reverse-engineered)

Additionally, from an enforcement standpoint, verifying collection of such consents poses operational challenges when an entity receives data from another intermediate entity (and not directly from the data principal). If an entity is using anonymised data for its internal purposes, including for commercial purposes, without sharing it with others, it is unclear as to whether consent from the data principal would be necessary (as this information is not personally identifiable, and where personal information is anonymised, the data principal would be untraceable). The consequences of revocation of consent for anonymisation may then result in two likelihoods: (i) deletion of data pertaining to revoked consent being impossible if data has already been anonymised and cannot be traced back to the data principal or (ii) where it may be deleted in case of high-value or public datasets, it may theoretically increase the likelihood of de-anonymisation being possible. All entities using a public data set would then need to ensure that they, in turn, have deleted relevant data which is highly arduous and impractical.

The Committee's attention is drawn to the fact that anonymisation benefits data fiduciaries and data principals alike. It helps achieve the objectives of the Revised Framework through the creation of large high-value datasets comprised of non-personal data that can be shared and utilised by the government, public and private entities as a catalyst for economic development, innovation, social welfare and creation of opportunities. Mandating data collectors to obtain consent for anonymisation may lead to the creation of a comparatively smaller pool of aggregated data which limits the data collectors' and data trustees ability to infer more accurate forecasts, insights and trends. Therefore, we suggest that all excessive consent notice requirements, in addition to those specified in the PDP Bill, be omitted from the Revised Framework and not be carried forward to any upcoming legislation governing non-personal data. Instead, we recommend that data fiduciaries/data collectors are subject to certain minimum data protection standards for the handling of anonymised data to prevent re-identification under the PDP Bill rather than having the Revised Framework impose an onerous requirement of obtaining consent from data principals.

Lastly, there is an overlap between the data anonymisation techniques that the Revised Framework intends to prescribe to data custodians and the anonymisation standards contemplated in the PDP Bill. The PDP Bill defines anonymisation as an irreversible process of transforming or converting personal data to a form in which a data principal cannot be identified, which meets the standards of irreversibility specified by the Data Protection Authority. The Committee should clarify what types of standards and techniques of anonymisation will be governed by which legislation upon its enactment and the levels of

anonymisation contemplated under either/each legislation for different types of data processed by different types of data custodians.

2. **Undifferentiated Obligations**: The Committee has provided that data-sharing can be requested in such cases where the dataset serves either (i) a sovereign purpose, (ii) a public good purpose, or (iii) a business purpose. Data sharing for a business purpose indicates the sharing of data between two private entities for business development or any other objectives mutually agreed between the entities. On the other hand, when data sharing is mandated under a sovereign or public good purpose, the data custodian has no practical autonomy over the datasets it possesses. While data sharing for sovereign purposes is already required under several legislations; such as the Information Technology Act, 2000; for data sharing requests made for a public good purpose, the final say on whether the data custodian has to go through with the request rests with the NPDA.

   The Committee's attention is drawn to the fact that irrespective of the nature of the data-sharing request, certain data custodians are already governed by existing laws which set out various mandatory compliance obligations. Some sectors are more stringently regulated than others. We further submit that non-personal datasets of data custodians belonging to such highly regulated sectors (such as banking and healthcare) may continue to be business-sensitive and proprietary in nature and cannot be shared freely unlike datasets belonging to, for example, the agricultural sector.

   We suggest that the better approach for implementing data sharing for the public good purpose and making it less arbitrary is to study the severity of the compliance and security requirements imposed under extant laws in each sector and redefine the scope and process of data-sharing. This approach would also ensure that different types of regulated entities which collect and manage different types of non-personal data are not subjected to identical data sharing requests and obligations. Any data sharing framework should (i) impose voluntary obligations on members of the data-sharing ecosystem to share data after assessing the costs and associated factors connected with it, (ii) provide exhaustive definitions for and carve-out appropriate proprietary information, trade secrets, certain sensitive datasets determined in consultation with sectoral regulators, and (iii) have in place a well-charted adjudication and appeal procedure allowing the regulatory body to determine, without any ambiguity, what kind of datasets can be exempted from data sharing when the question arises in an appeal by the data custodian.

3. **Grievance redressal and appeal process**: A grievance redressal and appeal process would enable individuals forming the community, data trustees and data custodians to raise their grievances before the NPDA and have data sharing requests sanctioned or challenged. It is evident from the plain reading of the Revised Framework that a data trustee is given most autonomy and power to manage non-personal data. However, unlike the PDP Bill which contemplates heavy penalties on data fiduciaries for any data breach, the Revised Framework does not provide any penalties on data trustees contravention with their obligations. Accordingly, a clearly defined grievance redressal and appeal mechanism with the NPDA should be prescribed in the Revised Framework to avoid instances of abuse of power and provision of checks and balances.

4. **Cross-border datasets**: The Revised Framework is contemplated to be a single national-level legal framework in India to establish rights over non-personal data **collected and created in India**. However, the definition of private non-personal data includes data in a global dataset of non-residents which are collected in foreign jurisdictions. Clarification must be provided

regarding the scope of the Revised Framework and if it caters to data security interests of communities belonging to foreign jurisdictions. Given the strong competitive advantage that India has in the outsourcing sector, it would not be desirable to open itself to scrutiny by third-country enforcement agencies for any breach or excessive use of power in handling global datasets by the NPDA and data trustees under the Revised Framework.

Therefore, we recommend that cross border data sets, such as (i) data relating to business or clients outside India in addition to those inside India, (ii) services provided from India to entities outside India, (iii) services partly provided in India and partly provided outside etc. should be exempted from the data-sharing mandated under the Revised Framework. A clear exemption for datasets generated from outsourcing is needed to prevent global datasets of banks from becoming subject to the Revised Framework simply by having an outsourcing hub in India. Registration and data-sharing requirements could result in businesses operating outside India (e.g. global news sites) to firewall their websites and businesses from Indian users or access for fear of legal liability, thereby isolating India from the internet or digital innovation in general.

5. **Free flow of data across borders:** We submit that Committee should also provide clarification on whether the data storage and data transfer restrictions imposed on sensitive non-personal data and critical non-personal data in the 2020 Framework carry forward to the Revised Framework. We reiterate the position taken in our recommendation to the Committee on the 2020 Framework with regards to ensuring the free flow of data across borders. Ensuring that India has rights over Indian data does not mean that data should not flow freely across borders, especially in key sectors such as finance, which drive growth in other sectors of the Indian economy. Free flow of data is key in the creation of competitive digital economies, ensuring effective risk management and the facilitation of global participation in innovation and entrepreneurship in India. The underlying objective of the Revised Report to unlock the economic benefits of data cannot be actualized if unnecessary restrictions on cross border data transfers are imposed on the data custodians and data businesses. Any cross-border transfer restrictions are bound to create hurdles to the anti-money laundering and know your customer processes of financial institutions.

Furthermore, several national and multinational companies depend on outsourcing and cloud storage solutions to reduce costs, support operations and have access to up-to-date, decentralized technology which is borderless. Given the extant business practices, the imposition of local storage requirements and prohibition of data transfers outside India would result in unnecessary compliance burden on a company which will directly impact its operations and profitability and should be avoided at all costs. Cross-border movement and storage of non-personal data is essential for regulatory compliance obligations as well as unifying multi-jurisdictional services. The Committee should adopt an approach where the free flow of data is the rule and data localization is the exception, especially in sectors such as financial services which are already subject to stringent rules on information security, confidentiality, governance and conduct of business.

We submit that the Committee should devise a procedure for the management of inbound and outbound non-personal data which does not impose any excessive obligations on the data custodian. The purpose of such procedure shall be merely to track the inward and outward flow of data and ensure adequate data protection is provided in third countries.