SFLC.IN
K-9, Second Floor, Birbal Road,
Jangpura Extension,
New Delhi-110014
(tel): +91-11-43587126
www.sflc.in

SFLC.IN's COMMENTS ON NON-PERSONAL DATA GOVERNANCE FRAMEWORK

- ## EXECUTIVE SUMMARY

The Committee has undertaken the laudable task of trying to address the issue of big data amassed by huge corporations like Google, Facebook and Amazon and allowing smaller players to access this. However, it is debatable whether this framework is the right approach for it. The framework is replete with abstract concepts and ideas and it lays out a very shaky platform to draft a legislation which aspires to be a model for the world.

The Report fails to clarify what sort of an institutional structure would be beneficial in regulating non-personal data, ensuring that data principals receive their fair share of benefit from the processing of their data or how misuse can be thwarted. The focus of the report seems to be finding ways to monetise data and citizen's rights are more of an afterthought.

The Non-Personal Data Governance Framework lacks architectural clarity and legal coherence. Its definitions and categorizations are notably vague. Its analysis of the relations between its proposals and existing legal rights is non-existent. The Report assumes that data has an intrinsic value but it does not explain what this intrinsic value is and how this will be beneficial to the citizens, government and the private sector,.

The Report does not define rigorously the links between personal and non-personal data. Its examples and illustration, which are chosen apparently at random throughout the report, suggest that any personal data can be reclassified as non-personal data by applying ineffective

anonymization techniques that scholars in the field have repeatedly shown do not work. The Report proposes to treat hospitals and other health care deliverers, for example, as "data businesses" who can be compelled to publish meta-data and satisfy third party commercial requests on terms to be fixed by the government authorities. But the data involved is derived from individual health records, among the most sensitive and personal forms of personal data. These and other similar passages imply that "deriving" data from personal data extinguishes individual rights of privacy.

The Report imagines a new domain of community data. It anticipates granting government authority complete discretion to identify and set the boundaries of "communities", and to empower individuals to act as the "guardians" or "beneficial owners" of this community data, at government discretion. This "corporatism", in which government defines communities possessing new legal rights and arbitrarily determines the community's legal leadership, is explicitly anti-democratic, though dresses in "will of the people" populist grab.

The Report in Paragraph 2.1 states that the Committee had met with experts and representatives of various companies in the preparation of this Report However, the list of representatives and experts consulted has not been made public. Throughout the Report, terms like "data philanthropy" and "national security" have been used but no definition has been provided. Though the Report has considered economic, social and public value of data, it has failed to consider the individual value of non-personal data and therefore has missed talking about data from an individual's perspective. It has not discussed the rights of a data principal in consonance with the principles of data protection. The Report has done little to address the privacy principles of transparency, accountability and purpose limitation. The Report has empowered the government to get access to non-personal data of citizens for a multitude reasons with no safeguards whatsoever against misuse of such data by the government or private players.

The Report makes a lot of assumptions, which have not been tested even on a pilot basis. It has relied on a one-size-fits-all approach, which is not the case. For instance, the use case of weather data or road data will not be similar to the use case of data categorized as sensitive or critical non-personal data. Most importantly, the report builds on the problematic parts of the Personal Data Protection Bill, 2019 (the "PDP Bill, 2019"). For instance, the PDP Bill, 2019 does not define what all falls within the ambit of critical personal data. This has to be decided by the government from time to time. This categorization and definition of critical personal data is problematic in itself and the Report has gone further with this fallacious categorization.

The Report imagines a public data authority empowered to enforce sharing of non-public data by private parties who have collected or generated it, with the power to order unwilling parties to share if the requests are "genuine". No substantive provisions of law, or process for judicial review are proposed to qualify this extra-constitutional discretion, which threatens to infringe on both the fundamental rights of privacy and free expression.

The Report has not explored the interface of non-personal data governance framework with other legal frameworks including the competition law regime, and its interaction with broad compulsory licensing regime and existing legal protected by patent, copyright and trade secret law.

Our key recommendations include:

i. The phrases such as "national interest", "strategic interest", "core public interest" etc. must be precisely defined.
ii. There should be transparency about the role and mode of selection of a data trustee. In case of a dispute between two or more contending data trustees, the non-personal data protection authority must have the jurisdiction to adjudicate upon such disputes.

iii. The rights of community to control its data and to determine how it is used should be specified.

iv. The restriction of sharing non-personal data with only Indian entities could prove meaningless if these companies are acquired in future by multinaltional corporations. It is restrictive in nature and requires reconsideration. It should be made clear as to what all falls within the ambit of an "Indian company".

v. Meta-data collected by data businesses should be restricted to non-personal meta-data and that data shared beyond a certain threshold requires certain checks and balances.

vi. The interaction with the intellectual property laws like Copyright and Trade Secrets, and the Competition Law should be clearly spelled out.

vii. The Non-Personal Data Authority must act in a quasi judicial capacity and adhere to principles of natural justice while adjudicating on refusal of a data custodian to share data.

viii. It should be specifically mentioned that if personal and non personal data are inextricably linked, which Authority (Non Personal Data Authority or Data Protection Authority) will adjudicate on such cases.

ix. The Non Personal Data Authority's constitution should be clear and diverse. There should be one or two judicial members and a member from civil society. There should at least be one woman member and a member from marginalized communities.

x. The Framework must provide for robustness in order to maintain the trust and confidence of individuals in the rules designed to protect their data.

We sincerely hope that through this round of consultation, the Committee will consider the points raised by various stakeholders and will come up with a robust framework for non-personal data governance.

About SFLC.IN

SFLC.in is the first Indian legal services organization that works exclusively on technology, law, and policy. As a not-for-profit organization engaged in the empowerment of Indian citizens about their digital freedom and rights, it operates as a collective bringing together different stakeholders to a common platform to further the cause of digital rights. SFLC.in promotes innovation and open access to knowledge by helping policy makers make informed and just decisions regarding the use and adoption of technology. As of 2020 SFLC.in is the only Indian organization to be inducted as a member of the IFEX, a global network to defend the right to freedom of expression and information.

RECOMMENDATIONS

1. Defining Non-Personal Data

1.1. Wide definition of non-personal data

The definition of non-personal data in the Report has a very wide ambit. It includes anonymised personal data, data related to weather conditions, from sensors installed on industrial machines, public infrastructures etc. There should be proper demarcation between what constitutes the public non personal data, community non personal data and the private data. Instead, the definition of non-personal data must be laid down exhaustively. Though the European Union's framework for the free flow of non-personal data in the European Union defines "Data" as *"data means data other than personal data as defined in point (1) of Article 4 of Regulation (EU) 2016/679"*, the framework only regulates the cross border flow of data and not the data sharing, economic uses of data etc. The European Framework on free flow of non-personal data has also laid down the scope of the regulations to the processing of personal data in the Union. It is only through an exhaustive definition that rights and harms[i] to a data principal can be laid down and it will also lead to avoidance of unnecessary litigation after the legislationon non-personal data sees light of the day.

For any legislation, the rights and obligations of the parties should be laid down in precise and coherent manner.

1.2. Use of vague phrases like "national security" and "strategic interests"

In its recommendation 1, the Report describes the grounds on which non-personal data may be considered as "sensitive non personal data"[ii]. It includes grounds such as "national security" and "strategic interests". However, the Report does not mention what exactly is meant by these phrases

and what all will be covered under "strategic interests" or "national security". Such phrases must not be loosely used and require an exhaustive definition.

Similarly, in *Kartar Singh v. State of Punjab*[iii], it was observed that *"It is the basic principle of legal jurisprudence that an enactment is void for vagueness if its prohibitions are not clearly defined. Vague laws offend several important values. It is insisted or emphasized that laws should give the person of ordinary intelligence a reasonable opportunity to know what is prohibited, so that he may act accordingly. Vague laws may trap the innocent by not providing fair warning. Such a law impermissibly delegates basic policy matters to policemen and also judges for resolution on an ad hoc and subjective basis, with the attendant dangers of arbitrary and discriminatory application. More so uncertain and undefined words deployed inevitably lead citizens to "steer far wider of the unlawful zone ... than if the boundaries of the forbidden areas were clearly marked".*

1.3. Consent by a community

It is unclear as to how consent works towards community rights since harms to specific communities cannot always be identified at the collection stage, and might become apparent only at the processing stage.

In addition to this, the data principal should be aware of the fact that anonymised data could be shared with third parties and the consent given for anonymisation should be an explicit consent allowing for third party transfer of anonymised data.

1.4. Public Non-Personal Data: What constitutes "publicly funded works"?

Clause 4.2 of the Report provides for "public non-personal data". It states that data collected in the course of "*includes data collected or generated in the course of execution of all publicly funded*

works". There should be clarity as to what all will be included in publicly funded works. For example, will crowd-funded projects be considered as "publicly funded works"? It is important to address if "publicly funded works" means funds charged upon the consolidated fund, contingency fund, or budget earmarked for various governmental schemes.

The definitions must also lend some clarity to the classification of data collected in the course of public-private partnerships and joint ventures between the government and private players. It is currently unclear if this data will be classified as public non-personal data, community non-personal data or private non-personal data.

1.5. When personal and non-personal data are inextricably linked

There should be clarity as to what will happen when personal and non-personal data are inextricably linked to each other. For instance, in the European Union, when personal and non-personal data is inextricably linked, it is treated as the personal data and therefore, the relevant Data Protection Authority can take action.[iv] The Report does not delve into the fact that most of data-sets are mixed data-sets.

There are scenarios also possible wherein legislation dealing with personal data and with the Non Personal Data Governance Framework are applied in parallel, with each undermining the other.

The Report has not addressed this scenario except for mentioning the GDPR's position on inextricably mixed data-sets in the Appendix.

- **Key Recommendations**

1. The phrases such as "national interest", "strategic interest" should be precisely defined

2. It should be stated in clear terms in the terms of service of every government and non-government service that a data principal will not be denied any service in case it decides against sharing and processing of its non- personal as well as anonymised data.
3. There should be specifications as to what all will be included in "publicly funded works".
4. If the data is collected through the joint venture of the Government and private players, who will have the ownership over such data must be specifically stated.
5. In case the personal and non-personal data are inextricably linked, such data should be considered as personal data and fall within the ambit of the Personal Data Protection legislation.

2. Defining Non-Personal Data Roles

2.1. Concerns with the role of data trustee

The report has introduced the concept of data trustee which will have the authority to exercise rights on behalf of the data principal group or community. Such data trustee will be the closest and most appropriate representative body for the community. This is vague in nature because there is no clarity as to how such data trustee will be selected, who will be selecting them and exactly what will be their role. This clarity is necessary for the community to be able to hold the data trustees accountable.

For example, the Report refers to an instance where "*a public university in Hyderabad is collecting data on the state of roads in Hyderabad as part of research project can be a trustee of the data it has collected"*. However, the Ministry of Road, Highway and Transport of the Central Government or the Public Works Department of the State government will be a more appropriate data trustee of data on roads.

Another relevant consideration could be that there might be multiple groups having stake in that data, and therefore, could be more appropriate data trustees than a public university.

2.2. Potential conflicts between the data trustee and data community

In one of the examples, the Report states that the data trustee of diabetic patients in India will be the Ministry of Health and Family Welfare.[v] It is not specified however, as to what will happen in case there is a conflict between the community and the data trustee. For instance, the Ministry of Road Transport and Highways sold *Vahan* and *Sarathi* databases for ₹65 crores without due consent from the data holders i.e. a community. The report does not envisage such potential conflicts, which may arise in the future.

2.3. Situations where data trustee will also be data custodian

This also means that some data trustees will also be data custodians. For example, the Ministry of Health and Family Welfare can be the custodian as well as data trustee of the health data of diabetes patients. According to the report, data trustees can also recommend to the data regulator, the enforcement of soft obligations on data custodians, which may lead to conflict of interest[vi].

Therefore, there should be clarity on the roles and functions of the data custodian and data trustee, as well as a clause that a data custodian cannot be a data trustee and vice-versa.

2.4. Data Trustee

While it is appreciable that in seeking and enforcing data sharing, the data trustee and data regulator will collaborate, it is necessary to leave room for concerns raised by individuals of the community whose concerns may not be voiced by the data trustees.

The data trusts envisaged in the Report should be covered under the Right to Information Act, 2005 as they will be repositories of public data[vii] and maybe managed by public authorities or industry associations.

Clause 4.9 (iii) states that *"in certain cases, mandatory data sharing will be required to open up competition in any concerned sector enabling startups, or for other community/public interest purposes discussed in this report. The data trustee may seek enforcement of safguards on the sharing of community non-personal data of which it is the trustee, before the data regulator".*However, the Report does not envisage that this could take away all the effort put in by the first-mover in that specific domain which could also be a start-up. In such a situation, a well-funded start-up could get access to data collected by first mover in that area, thereby negating the competitive advantage of the innovative startup...

2.5. Role and rights of communities as data principal

At one point in the report[viii], it is stated that the benefits accruing from the processing of community data will also be shared with the community. However, it is not clear how such benefits will be shared with the community and in what form.

This clause also provides that such data may be shared on certain grounds or purposes with Indian citizens, start-ups, companies, universities etc. Firstly, the grounds or purposes of sharing of data should be clearly stated. Secondly, the restriction of sharing non-personal data with only Indian entities is restrictive in nature and requires reconsideration. It should be made clear that what all constitutes an "Indian company" i.e. if a company having its operations and office in India will be considered an Indian company or a company just doing business in India will meet the threshold of an Indian company. Thirdly, there should be clarity on the procedure adopted to seek consent

before sharing of community non-personal data. Fourthly, it should be clarified if such sharing of non-personal data will be limited to raw data or processed data.

- **Key Recommendations**

1. There should be transparency about the role and mode of selection of a data trustee. In case of a dispute between two or more contending data trustees, the non-personal data protection authority must have the jurisdiction to adjudicate upon such disputes.
2. Individuals from a community must have recourse available in case they are aggrieved by the actions of the data trustee.
3. In order to avoid conflict of interest, the functions of data trustee and data custodian should be properly demarcated. A data trustee should not be a data custodian and vice-versa.
4. The data trusts must be covered under the Right to Information Act, 2005.
5. The data infrastructure should be open source and open for third party audit.
6. The grievance redressal mechanisms available to the Authority in case of unauthorized data sharing should be made available to the communities.
7. The benefits to be accrued upon the communities from the processing of the community data requires to be clarified. It is not clear how the community will benefit by a commercial entity using/gaining access to their data.

3. Articulating a Legal Basis for Establishing Rights Over Non-Personal Data

The intended effect of the Report's proposals in an immense social subsidy to Indian commercial power pursuing large-scale data mining. All other parties in the economy collecting significant non-public data could

3.1. Interaction of raw data with the intellectual property rights

The report does not envisage how the raw data, which also requires some minimum threshold of originality for collection and then segregation, will interact with copyright law. The interaction of the intellectual property rights regime must be harmonized with the principle of community ownership of non-personal data. In India, "minimum level of creativity threshold" is allowed under the Copyright law and the process of raw data collection and segregation qualifies that threshold because there is creativity involved in data collection as well as in transforming it into usable data sets.

3.2. Rights of a community over its data

While the report provides for giving a right to the community to ascertain and control how much of its data is used, there is no mention of how a community shall be able to exercise these rights over its non-personal data.

The report does not envisage a situation where there may be a conflict between the community or an individual belonging to the community and the data trustee, and the rights available to individuals in such cases.

3.3. Harms caused

The Report has not envisaged a situation where non-personal data, apart from the anonymised data, of a data principal maybe misused but will not specifically fall within any of the offences in the Personal Data Protection Bill or the non-personal governance framework.

For example: location data of users, which forms part of non-personal data, close to a site of protests could be used to target them during investigations.

- **Key Recommendations**

1. The rights of community to control its data and determine how it is used should be specified.
2. The situations where there may a conflict between the community and the data trustee should be envisaged.
3. Individuals must be vested with the rights to exercise control over their own non-personal data.
4. The interaction of raw data with the copyright law, licensing regime and trade secrets must be clarified.
5. In clause 5.1(iv) of the Report:
   a. the grounds or purposes of sharing of data should be specified. .
   b. the restriction of sharing non-personal data with only Indian entities could prove meaningless if these companies are acquired in future by multinaltional corporations. It is restrictive in nature and requires reconsideration. It should be made clear as to what all falls within the ambit of an "Indian company".
   c. there should be clarity on the procedure adopted to seek consent before sharing of community non personal data.
   d. it should be clarified whether such sharing of non personal data will be limited to raw data or processed data.

4. Defining a Data Business

4.1. Open Access to Metadata

First and foremost, the report proposes that the data businesses shall provide open access to meta-data, however, it is not clarified if this will include all meta-data or non-personal meta-data.

Metadata when shared with Government agencies could provide a wealth of information for surveillance purposes and law enforcement agencies could then demand data from various data custodians. It needs to be noted that such data sharing with the Government for "national security or strategic interest" cannot be refused.All other parties in the economy collecting significant non-public data could be required to publish indexes of their collections (called "metadata" by the Report) and to furnish those collections to requesting businesses, potentially on government order, on government-established terms. No analysis is offered as to the likely effect on competition, presumably to avoid emphasizing the enormous transfer of wealth to the largest Indian data miners that would result.

4.2. Categorisation of Data Businesses

The Report envisages that based on a threshold of data collected or processed, businesses may be classified as data businesses. Firstly, it should be clarified if collected data or processed data or both will be included in determining the threshold level of the data businesses. The Report does not clarify if data processors will be treated on par with data controllers. This could create a burden on data processors who are only processing the data provided by the data controllers..The idea that data business will provide open access to meta-data within India[ix] is vague in nature- does this mean that metadata will have to be stored within the territory of India or will only be accessible to Indian companies?In the data disclosures section of the Report, there is a clause on open access to meta-data directories of data businesses. Meta-data forms a crucial part of various services rolled out by data businesses and open access to meta-data may lead to stifling of innovation and will eliminate the competitive edge companies will have.

This mandate also raises questions about the need for having a "data business" for data sharing transactions, when companies can enter into agreements themselves.

- **Key Recommendations**

1. Meta-data collected by data businesses should be restricted to non-personal meta-data.
2. The nature of data shared with data businesses should be clarified - if it will be raw non-personal data or processed non-personal data or both.
3. The requirement of sharing non-personal data beyond a certain threshold require checks and balances.

5. Defining Data Sharing Purpose

5.1. Core Public Interest Purpose

The data sharing will be undertaken for "sovereign purposes" like national security, legal purposes etc. These terms should be exhaustively defined to avoid misuse of non-personal data.

Similarly, phrases like "core public interest purpose" require an exhaustive definition and should be enshrined in the primary legislation on Non-Personal Data. The list of high-value datasets should be made clear, and it should specifically list the sets of data will be considered as high value, and in order to avoid arbitrary decisions by the executive, the mechanism through which such datasets will be listed must be transparent. Instead, in the age when "data is the new oil", proportionate remuneration could be offered to companies for sharing such "high value data sets". The Report has not discussed the economic characteristic of non-personal data. The economic aspect of data must form the preface of high value datasets.

5.2. Data Sharing for Economic Purposes

In the data sharing for economic purposes section[x], the Report states that in case of a dispute arising from data sharing requests[xi], the data regulatory authority will ascertain the genuineness of such requests. Instead, this should be left to the will of the company. Freedom must be provided to the

company to decide if it wants to share its data or not. The current form of the Report does not specify the constitution of the Non-Personal Data Authority and therefore the proposed constitution of the Authority may have conflict of interest with companies involved in such disputes.

At one point, the Report stipulates that pre-identified "important community data" will have to be made available to all relevant parties.[xii]

Firstly "important community data" is vague in nature and must be defined exhaustively. Secondly, this may not only stifle innovation but will also be problematic in the sense that such data maybe a trade secret/copyright of a company. The Report does not list out in clearer terms, how the non-personal data framework will interact with intellectual property laws like the Copyright and Trade Secret laws, and with Competition laws.

5.3. Cost of Compliance and Ease of Doing Business

One of the areas which the Report has not delved into is the compliance cost and ease of doing business. The Report proposes several compliance requirements for companies while at the same time dis-incentivising data collection for them. The Report has not done a cost benefit analysis of this infrastructure.

- **Key Recommendations**

1. Terms like "sovereign purposes", "national security", "legal purpose", "important community data" and "core public interest" should be exhaustively and precisely defined.
2. These should be specifically mentioned in the primary legislation on Non-Personal Data.
3. Any data sharing for "core public interest" purposes and "pre-identified community data" should have sufficient safeguards .

4. The interaction with the intellectual property laws like Copyright and Trade Secrets, and the Competition Law should be clearly spelled out.

6. Defining Data-Sharing Mechanisms and Checks and Balances

Regarding the sharing of private data, the companies should not have to share even their raw community data unless their consent has been sought for the same and proportionate remuneration must be paid for the same.

The Report gives merely vague examples that pretend to force all kind of data sharing between Business to Government (B2G) and Business to Business (B2B) without giving specific examples. It only states that certain data held by private sector may be useful for science, healthcare etc.

The refusal of data sharing request by data custodian should be evaluated by the Non-Personal Data Protection Authority keeping in mind the principles of natural justice.[xiii.] The data custodian must have the option to approach other appropriate judicial forums in case of a grievance.

- **Key Recommendations**

1. Companies should not be forced to share their raw "community data" without proper checks and balances.
2. The Non-Personal Data Authority must act in a quasi judicial capacity and adhere to principles of natural justice while adjudicating on refusal of a data custodian to share data.
3. The data custodian must have the option to approach other appropriate judicial forums in case of a grievance.

7. Establishing a Non-Personal Data Authority

The Report proposes to create a separate non-personal data authority because non-personal data in India is still an emerging area. At one point in the report, it has been stated that the main focus of the Non-Personal Data Authority (hereinafter "the Authority) will be to unlock the value of non-personal data in India and not to prevent personal harm. This blurs the demarcation of the role of a corporate or government and a regulator. Instead, a regulator's role should not be to promote innovation but to safeguard interests of all stakeholders involved. The Authority should be vested with powers to hear complaints of individuals as well. The report, however, restricts the mandate of the Authority to work on data sharing, competition, re-identification and collective privacy.

Under its enabling role, the report empowers the Authority to ensure that the data is shared for sovereign, social welfare, economic welfare and regulatory and competition purposes. However, terms like "sovereign", "social welfare" and "competition purposes" should be more precisely defined to reduce instances of misuse by the government or private players.

The enforcing role of the Non-Personal Data Protection Authority has been limited to ensure that all stakeholders follow the rules laid down and adhere to data sharing requests. The role of the Authority should be expanded to adjudication and grievance redressal.

In addition to this, it should be clarified if the personal and non-personal data are intertwined, which authority will be responsible for grievance redressal in such cases and will have the jurisdiction to adjudicate upon it. Example, in the European Union, when personal and non-personal data is inextricably linked, it is treated as the personal data and therefore, the relevant Data Protection Authority can take action.

The Report also provides that the Authority will be addressing harms including the exploitative or exclusionary harms such as market entry barriers, restriction competition, discriminatory harms to

the businesses or customers. Therefore, it will be prudent to distinguish the functions of the Authority from the functions and jurisdiction of Competition Commission of India, in order to avoid overlaps and multiplicity of cases.

The function of the Authority should not be limited to ensuring a level playing field for all Indian actors. There are two-fold problems with this, firstly, how shall one ascertain Indian-ness of a company? Example: Facebook has acquired a 9.9% stake in Reliance Jio. Will Reliance Jio be considered as a wholly Indian Company ? There should be some clarity on this. The Report states that Non-Personal Data Authority will have some members with relevant industry experience. However, it does not clearly specify the constitution of the Authority. Considering the complexity of issues involved,, the Authority should be comprised of judicial members, members with relevant industry experience and at least one member from the civil society. The diversity of the Authority should be kept in mind and there should at least be one woman, and a representative from marginalized communities in the Authority.

The character of the Authority is not clear i.e. if it will be a judicial authority or a regulator with powers of a civil court vested upon it and acting in quasi-judicial capacity. These should be clarified. The functions of the Authority should be clearly spelled out as well e.g. SEBI, IRDAI are sectoral regulators with clearly spelled out functions in their respective legislations.

Lastly, instead of having two separate data regulators for the Non-Personal Data and Personal Data, one data protection regulator should be vested with the function to address grievances and regulate both personal and non-personal data. For instance, in case there is a data set on direct taxes paid by users, it will have both personal and non-personal data in it. In case there is a dispute around such mixed data not inextricably linked, a common regulator should be able to address concerns arising from the Personal and Non-Personal Data Legislation.

- **Key Recommendations**

1. The Authority must be vested with powers of grievance redressal.
2. Terms like "sovereign", "social welfare" and "competition purposes" should be more precisely defined.
3. It should be specifically mentioned that if personal and non personal data are inextricably linked, which Authority (Non Personal Data Authority or Data Protection Authority) will adjudicate on such cases.
4. Since there is an overlap of the Authority's functions and the functions of Competition Commission of India (CCI), the functions and scope of the Authority should be demarcated in clear terms to avoid multiplicity of cases.
5. The restrictions on ensuring a level playing field for Indian companies should be avoided as this has the potential to stifle innovation and "Indian-ness" may not be defined in strict terms.
6. The Non Personal Data Authority's constitution should be clear and diverse. There should be one or two judicial members and a member from civil society. There should at least be one woman member and a member from marginalized communities.
7. The role of the Authority should be made clearer i.e. if it will be a regulator or a regulator and a quasi-judicial body.
8. Only one data regulator should be vested with powers to adjudicate and issue regulations on both personal and non-personal data.

8. Transparency, Citizen Engagement and Ethics

The Report does not provide for robustness in order to maintain the trust and confidence of individuals in the rules designed to protect their data.

Clause 3.9(i) of the Report states that :

"In the context of this Committee, the case for regulating data is made in such a manner that the benefits accrue to India and its communities and businesses. For instance:

(i) Sharing non-personal data collected by both government and private organsiations with citizens is likely to lead to increased transparency, better quality services, improved efficiencies, and more innovation".

However, the Report has not specified how this interacts with the Right to Information framework in India.

9. Reconciling the Non-Personal Data Governance Framework with various government agencies

The Report has made references to various policy documents by various government agencies like the Telecom Regulatory Authority of India in its consultation paper on privacy, security and ownership, e-commerce policy etc.. However, it does not reconcile what regulators like TRAI, Competition Commission are doing with the Non-Personal Data Governance Framework.

i Soumyarendra Barik, *Anja Kovacs on the problems with India's report on non-personal data governance framework*, August 13, 2020. Medianama. <https://www.medianama.com/2020/08/223-non-personal-data-report-problems-anja-kovacs/?utm_source=feedburner&utm_medium=feed&utm_campaign=Feed%3A+medianama+%28Medianama%3A+Digital+Media+In+India%29>

ii Non Personal Data Governance Framework Report, Page 14.

iii *Kartar Singh v. State of Punjab*, (1994) 3 SCC 569. ¶ 130

iv *Guidance on the Regulation on a Framework for the free flow of non-personal data in the European Union*, Communication From The Commission To The European Parliament And The Council, COM (2019) 250 Final, <https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52019DC0250&from=EN>

v Clause 4.9 (ii), *Non Personal Data Governance Framework Report,Page 20.*

vi Clause 4.9 (ii), *Non Personal Data Governance Framework Report,Page 21.*

vii Clause 4.10 (iii), *Non Personal Data Governance Framework Report*, Page 21.

viii Clause 5.1(iv), *Non Personal Data Governance Framework Report*, Page 21.

ix Clause 6, *The Non Personal Data Governance Framework Report*, Page 27.

x Clause 7.3,*The Non Personal Data Governance Framework Report*, Page 34.

xi Clause 7.3(i),*The Non Personal Data Governance Framework Report, Page 35.*

xii Clause 7.3(ii),*The Non Personal Data Governance Framework Report, Page 35.*

xiii Clause 7.3(ii),*The Non Personal Data Governance Framework Report, Page 38.*