POLICY MONKS

POLICY BRIEF

Examining the Draft Regulatory Framework for Non-Personal Data in India

By Sudhanshu Sarangi, Jemini Sara Nainan and Ritwik Mehta, August 2020
Edited by Bhaskar Pant

This Policy Brief has been prepared as a response to the Draft Non-Personal Data Governance Framework. The link to the Report by the Committee of Experts on Non-Personal Data Governance Framework is available at: https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf

Executive Summary

India is one of the only, if not the sole nation to come out with a regulatory framework for non-personal data, which is the data unrelated to individuals. The government released the draft last month and is presently seeking suggestions on it. Though the regulatory framework put forward by the government for using non-personal data for public welfare and establishing a market is quite innovative, the draft lacks clarity when it comes to implementation. It does not put forward any concrete rules and procedures for compensation to companies for buying data.

This policy brief examines the Draft Non-Personal Data Governance Framework to propose concrete policy recommendations for developing an effective legislation to govern and protect non-personal data in India. The policy brief recommends easing up on the localisation of data, providing data processors with reasonable power, getting rid of significant data fiduciaries and for the regulator to remain independent and not over-regulate.

Problem Statement

The Non-Personal Data Protection (NDP) report, which was formulated by a committee of experts on Non-Personal Data Governance Framework recommends regulating the non-personal data to access the social, economic and community benefits of data. The report addresses some crucial subjects such as ownership of data, data business and also proposes to set up a new regulator- Non-Personal Data Authority (NPDA). However, the report suffers from fundamental shortcomings.

- The report contradicts the competition laws. According to the competition law, the data should not be shared with the competitors; as a result, it protects the consumers, not the competitors. Mandating the businesses to share resources with the companies could restrict incentives to invest, innovate and compete, thereby reducing the quality of the products and services available for the consumers. Additionally, the report violates the principles of fair competition by favouring Indian businesses over foreign businesses, which could deepen the existing trade relations with other countries.

- In order to prevent the potential danger caused by the de-anonymisation of the data, the report suggests the use of anonymisation techniques and that the data principal's consent is considered before collecting or using the data. But as per the report, it is not clear whether the principal could be informed of all the uses of the data, considering the anonymised data. The report fails to address the interests of data principal thus making it vulnerable. The vulnerability can hurt individuals, businesses and also by discouraging the consumers from sharing the data with companies.

- The collection of the non-personal data is mainly for national security, legal purposes, etc., as mentioned in the report. This broad purpose raises concerns regarding state surveillance and discourages the public from sharing data with the government or businesses.

- The non-personal data report is a pioneer in identifying the power, role and usage of anonymised data, with little clarity in defining the different types of non-personal data, especially community data.

- Additionally, it establishes non-personal data as not personal data or data that is without any physically identifiable information like weather conditions, data from sensors installed on industrial machines and so on, thus creating ambiguity in clearly defining the non-personal data. It also gives the government immense powers to define and identify non-personal data, thus potentially increasing the possibility of misuse of data.

- The report does not clearly demarcate the roles and interaction of the players it envisions like data principal, data custodian and data trustee

- The ambiguity on cross-border data flow raises questions on data security. Also, the transmission guidelines mentioned in the report lacks clarity, i.e. 'NPD may be transferred outside India, but shall continue to be stored in India', it is unclear if it means that data could be moved abroad while a copy remains in India or it can be processed elsewhere but must be returned to India.

These ambiguous statements and other factors undermine the noble vision of this report resulting in a not-so-progressive regulatory regime.

Features of the Policy

The European Union brought in a regulatory framework to enable the free flow of non-personal data among the member countries. This framework suggested the member states cooperate on matters related to data sharing with any hindrance. In case any member state introduces a draft act on data localisation they must inform the commission, and in case of any existing data localisation act then necessary changes needed to be made. The regulation put forth by the EU

defines non-personal data as any data which does not come under the personal data is non-personal data.

The recommended non-personal data defines it as any data which is not personally under the PDP Bill, or without identifying any individual's identity. The non-personal data is translated into three categories:

Public Non-Personal Data: It is the data generated or collected by any agency of the government or by the government itself. This amalgamation of data could include the data collected or generated by the government while performing tasks that are publicly funded. The data generated or managed by the government is strictly confidential under the law and does not come under the purview of Public Non-Personal Data. For instance, anonymised data on land records, vehicle registration, public health information can be regarded as Public Non-Personal Data.

Community Non-Personal Data: The definition of community prescribed by the committee is 'any group of people that are bound by common interests and purposes, and involved in social and/or economic interactions. It could be a geographic community, a community by life, livelihood, economic interactions or other social interests and objectives, and/or an entire virtual community' (Ministry of Electronics and Information Technology, Government of India, 2020). Community Non-Personal Data includes anonymised personal data and non-personal data of a community of natural individuals, and it should not contain any Private Non-Personal Data. For instance, it might consist of data collected from various municipalities, public electricity, and also use information gathered by private players like telecom, e-commerce, and other such public service entities.

Private Non-Personal Data: Any Non-Personal Data collected or produced by agencies not acquainted with the government is considered as Private Non-Personal Data. The source or

subject related to the assets and processes is privately owned by such person or entity. This also includes the derived and observed data that result from the private effort.

Under section 11 of PDP, the requirement of consent does not apply to non-personal data; in such cases, the committee recommends that the data principle gives permission for anonymisation and usage of anonymised data. The data principle could also provide the necessary consent for the usage of individual personal data.

The recommendation recognised the non-personal data might have sensitive data. The possibility of anonymised and aggregated data produced from sensitive personal data could have delicate data. The anonymity of personal data does not necessarily remove the possibility of risk to the data principle, and non-anonymisation technique provides perfect irreversibility. The non-personal data could be sensitive in cases such as:

Areas of national security and strategic interests

Collective harm to any faction

Confidential or business-sensitive information

Anonymised data which could help in re-identification

Definition of Non-Personal Data and key Non-Personal Data roles

Data Principal

The report defines roles and stakeholders in the non-personal ecosystem. In Non-personal data principal is determined by the category of non-personal data:

Public non-personal data: The government's collection of the data of citizens, companies, and communities. The data principal is the corresponding body, such as organisations, communities, and individuals from whom the data is extracted.

Private non-personal data: The non-personal data collection by the private sector related to companies, communities, and citizens. The data principal is the corresponding body, such as organisations, communities, and individuals from whom the data is extracted.

Community non-personal data: The community is the data principal as the data is collected or generated out of the community. This also provides the community with fundamental rights over the data collected, which could include economic rights.

Data Custodians

The non-personal data also appoint a data custodian. The work assigned to the data custodian includes storage, collection, processing, etc. of data that could be useful to the data principal. The data custodian is subjected to specific directions and control to serve the interest of data principal/group/ communities. The data custodians have the responsibility of handling Non-Personal Data. The duties assigned to data custodians include maintaining anonymisation standards and requirements, protocols, and safe data sharing. The NPD, along with providing community data rights, also enforce principles and guidelines for incentives for data custodians, respective data privileges, compensations, and other such necessities.

Data Trustees

The data rights could be exercised by the data principal/community through an appropriate community data trustee. The trustee would exercise control over the data on behalf of the community. The legislation on non-personal data lays down principles and guidelines for who is an appropriate trustee for the community/group data.

Data Trusts

This is the institutional structure consisting of specific rules and protocols for sharing and containing any set of data. Data trusts can have multiple sources, custodians, etc. which are

relevant to any particular sector and are essential for providing any digital or data services. Data custodians can voluntarily share data with the data trusts, and private organisations could also share data held by them. The public organisations could also come forward to share the data held by them.

Ownership of different types of Non-Personal Data

Public Non-Personal Data: As the data is derived from public efforts, so it is considered a natural resource.

Private Non-Personal Data: The raw/factual data of the community might be share but at strict grounds of no remuneration but if the data processing adds some value to the raw data then compensation may take place.

Community Non-Personal Data: The data is related to the community but rights over the data vests on the data trustee of the community. Community Non-Personal Data have overlapping contributions and interests, making it a shared asset by multiple parties. The community would enjoy the maximum benefit for itself and minimising harms.

Data Sharing

Data sharing provision provides controlled access to the public sector, private sector, and community data to individuals and organisations for specific purposes and with appropriate safeguards. The argument presented in the draft states that it might "open-access to metadata and regulated access to the underlying data of Data Businesses will spur innovation and digital economy growth at an unprecedented scale in the country". The sharing of data according to the committee might help in, (i) Data Sharing for Sovereign Purposes, (ii) Data Sharing for Core Public Interest Purposes such as policymaking, and improving public service, (iii) Data Sharing for Economic Purposes. The committee also recommended a few checks and balances to ensure appropriate implementation of rules and regulation regarding data sharing.

Non-Personal Data Regulatory Authority

The committee recognised the need for a separate Non- Personal Data Authority (NPDA). The authority will consist of experts with specialised knowledge so to keep pace with the rapidly evolving technology space. This agency will work towards the prevention of personal harm. It will also support the digital industry of India, including start-ups and make sure appropriate data is available to social, public, and economic purposes. The sectoral regulators will enjoy the power to build additional data regulators. The authority will work in consultation with Data Protection Authority (DPA), Competition Commission of India (CCI), and other sectoral regulators to solve issues related to data sharing. The authority has two parts to play:

Enablers: To ensure that data is shared for a sovereign, social welfare, economic welfare, regulatory and competition purposes to spur innovation in the country.

Enforcing: To enforce rules and regulations on stakeholders, undertaking extensive evaluations of the risk of re-identification of anonymised personal data among various other roles.

Technology Architecture

Application Programming Interface (APIs): Representative State Transfers (REST) API enable the sharing of all Non- Personal data and datasets created by companies, government, university, research institutes, and NGOs.

Standardised Data Exchanges: Regardless of the type of data, exchange method, and platform, all the data exchanges are to be standardised. Data exchange for stakeholders of the collated data should be available so that entities could make the required inferences. The output and data during the transfer should be in such form that it could be useful to all the stakeholders.

Distributed/Federated Storage for Data Security: All the data sharing is done through APIs so that all the exchanges of data could be tracked and logged avoiding any leakages. Coordination

of data trusts and data infrastructures are required for critical non-personal data in different sectors.

Anonymisation of data: To prevent de- anonymisation, different mechanisms are employed, such as differential privacy, homomorphic encryptions, and blockchains.

Policy Recommendations

1. Data sharing should not be made compulsory for the companies but should be on a voluntary basis—a proper sharing mechanism for sharing public, community, and individual needs to be established. Since companies are not getting anything for sharing the raw community, therefore, the companies must have the option of not sharing knowledge data and algorithms at all.
2. If the raw data is typically processed, then companies will get very less remuneration, but if advanced processing is involved, then might attract a lot of profit and market for the companies.
3. Inclusion of a new category of businesses called "Data Business" should be formed which will collect, process, store, and manage data.
4. The data can be requested from businesses and government by various stakeholders -- the government, citizens, start-ups, private organisations, and non-profit organisations --- for "social welfare, regulatory, sovereign, and economic purposes. Data for sovereign purposes may be requested for national security, legal purpose, or meeting a sectoral regulation requirement".

5. Public interest should be the basis of sharing data and must be adjudged on a case-by-case basis. If the government asks for data for public policy, then public interest will

be the test, but in the case of competitors, the government should not decide it rather public interest should be taken into consideration.

6. In order to encourage innovation and allow the secure sharing of data between the competitors, economic cost should be considered.
7. The completely anonymised data, in addition to data voluntarily being shared by a private company, should be put on the MeitY's Open Government Data Platform.
8. There should be clear rules about the misuse of data and liability. The targeted requests for data sharing must be handled by a third-party.
9. Data should be a part of a regulator for each and every industry as the "standard of data sharing is very domain-specific". Thus, an insurance regulator should have a department which specialises in data affairs, including its sharing, exchange, publicly available data sets, etc. With more than 625 million internet connections and around 500 million internet users, we will need a set of DPAs to deal with issues surrounding privacy itself. Therefore, there must be an industry-specific data regulator.
10. The data steward is placed between the users and entities as well as people who are acquiring the data. A data steward/trust:

- Has the responsibility or duty of care towards the users whose data it is
- Potentially look at data as labour.
- Helps you negotiate better with technology companies
- Examine what the data is being used for.
- Data trusts could be used to help share data between users and entities. They could also answer queries related to technology standards, quality of data, etc.

Easing up on the localisation of data

It is essential to get rid of Clause 33 that mandates data mirroring for the cross-border flow of sensitive personal data as it won't help with data protection. Instead, it can accelerate service costs and disrupt companies operating in India. The right approach would be to recognise the role of private contractual arrangements, internationally recognised certification mechanisms, and other transfer mechanisms to increase accountability and cross-border data flow.

Define "sensitive personal data" narrowly to mitigate the impact on digital payments and healthcare industry. This categorisation needs to be reserved for "categories of data that carry special risks in relation to discrimination and abuse of fundamental rights".

Define "critical personal data" keeping national security considerations in mind in order to foster predictability for companies that process such data or simply exclude it entirely from the Bill.

There needs to be a focus on accountability for cross-border data flows instead of adequacy and/or consent. This will enable, entities that process personal data to remain responsible for its protection, irrespective of the geography where it is processed. If adequacy is used as a parameter, it should be made compatible with existing data protection frameworks, including APEC's Cross-Border Privacy Rules and standard contractual clauses of the European Union.

Furthermore, explicit consent should be one basis for cross-border data flows instead of being an obligatory requirement. Cybersecurity and fraud prevention can also be included as "reasonable purposes" exemptions.

Provide data processors with reasonable power

It is vital that fiduciaries engage with data processors with only a "general written authorisation" instead of a contract like in the case of GDPR where the processor informs the data controller of intended changes and replacements thus enabling the controller to object. This approach is pliable to governing data processors while letting the guardians of data exercise reasonable opportunity to differ.

Get rid of criminal liability

Scrap criminal liability as it can "chill beneficial and harmless data practices" and is not a proportionate response to violations with regard to data protection.

The degree of cooperation with the regulator should be used to reduce financial penalties. This may well act as a motivation for business to cooperate with the NPDA.

Get rid of significant data fiduciaries

Remove significant data fiduciaries. Instead, impose stricter obligations on data fiduciaries "undertaking activities that carry greater risk" to users.

Provide data protection impact assessments to the NPDA only on request but keep them on record as they could otherwise overwhelm the NPDA with paperwork.

NPDA should remain independent and not over-regulate

The NPDA should function as an independent sectoral regulator free of any government oversight. However, there is much room for regulatory confusion as at least four regulators are set to be incubated for the digital ecosystem including – the proposed NPDA, DPA, an E-Commerce Regulator and the Central Consumer Protection Authority.

Works Consulted

1. Author, G., 2020. *Five Key Concerns With India'S Non-Personal Data Report*. [online] MediaNama. Available at: <https://www.medianama.com/2020/07/223-five-key-concerns-with-indias-non-personal-data-report/>
2. Editorial. *The Draft Report On Regulating Non-Personal Data Does Not Allay Misgivings Over Data Use*. [online] @businessline. Available at: <https://www.thehindubusinessline.com/opinion/editorial/the-draft-report-on-regulating-non-personal-data-does-not-allay-misgivings-over-data-use/article32104610.ece>
3. Agrawal, A., 2020. *Summary Of Non Personal Data Report By MEITY Committee*. [online] MediaNama. Available at: <https://www.medianama.com/2020/07/223-summary-non-personal-data-report-meity/>
4. Agrawal, A., 2020. *Don'T Deal With Non-Personal Data, Ease Up On Data Localisation: BSA On Data Protection Bill | Medianama*. [online] MediaNama. Available at: <https://www.medianama.com/2020/03/223-bsa-submission-data-protection-bill-2019/>
5. Report by the Committee of Experts on Non-Personal Data Governance Framework. 2020. [online] Available at: <https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf
6. Burman, A., 2020. *Will India'S Proposed Data Protection Law Protect Privacy And Promote Growth?*. [online] Carnegie India. Available at: <https://carnegieindia.org/2020/03/09/will-india-s-proposed-data-protection-law-protect-privacy-and-promote-growth-pub-81217>

Policy Monks Consulting Services Private Limited
https://www.policymonks.com/

 /policymonks/  @policymonks/

 contact@policymonks.com