Inputs by The CyberPeace Foundation on the
**Revised Non Personal Data Governance Framework 2020**
by Committee of Experts, Ministry of Electronics and Information Technology
About CyberPeace Foundation

CPF is an award-winning nonpartisan civil society organization, think tank of cybersecurity and policy experts. At CPF, we work with netizens and institutions to facilitate inclusivity, security, stability and trust in cyberspace and our vision is to build a peaceful, responsible and inclusive cyberspace. To achieve our mission, we are involved in Inclusion & Outreach, Collaboration & Connect, Policy & Advocacy and Innovation & Outreach related to all aspects of Cyber Peace and Cyber Security. Our focus areas are research on technology governance, citizens awareness - women & children, capacity and capability creation of law enforcement agencies (LEAs) through partnerships with various citizens, cyber security experts, government organizations, private enterprises, academic institutions and civil society entities working in cyber-crime and cyber security. This submission presents CPF’s feedback along with policy recommendations that we feel would expedite the implementation process of NPDGF.
The CyberPeace Foundation (CPF) is grateful to the Committee of Experts formed by the Ministry of Electronics and Information Technology, Government of India for providing the opportunity to all stakeholders to contribute to the discussion on the Revised Non-Personal Data Governance Framework (NPDGF). CPF applauds the efforts made by the experts to incorporate the suggestions, feedback and the inputs provided by the stakeholders on the previous draft. We are especially pleased to see that the revised framework provides a more focused approach towards using data for the public good.
CPF had conducted a stakeholder consultation on 23rd January 2021 with seven experts to discuss the gaps in Revised NPDGF and suggest policy recommendations that are holistic and actionable:

**Mr. Satish Babu**  
Co-Founder and President of InApp

**Mr. Shilohu Rao**  
General Manager, Capacity Building, National e-Governance Division (NeGD)

**Ms. N S Nappinai**  
Supreme Court Advocate and Founder of Cyber Saathi

**Ms. Aprajita Bharti**  
Co-founder, The Quantum Hub

**Dr. Irfan A Siddavatam**  
Associate Professor, K J Somaiya College of Engineering

**Ms. Bhavna Sharma**  
Assistant Professor, GIBS, GGSIPU

**Mr. Rahul Sharma**  
Founder, The Perspective
1. The revised framework has suggested removing provisions Section 91(2) and Section 93(x) within the Personal Data Protection Bill (PDP) 2019 which suggested a framework to regulate NPD under the PDP Bill. There are apprehensions for achieving the harmonisation between the two frameworks, especially since the life cycle of data is dynamic, in most cases, there would be overlaps. This would create problems for young start-ups as they will have to constantly juggle between the two regulatory authorities especially since the standards for data anonymization have not been established. We run the risk of losing out on investment opportunities by taking away incentives from current and future investors by complicating mechanisms for data governance especially for start-ups that are completely dependent on foreign investors. Harmonisation between the two also remains a concern as the intentions for developing both the frameworks are conflicting, while one provides complete protection of data of individuals, the other talks about utilising that data to balance the goals of fair competition and public good by facilitating data sharing. The government should start by utilising the vast datasets that are available in the public domain such as government data for facilitating principles of fair competition for public good and to minimize the damage of overregulated regimes to Indian startups.

2. The revised report suggests that this framework will be used as a basis for the new NPD legislation and lists the guiding principles on which the regulation will be based. But the framework has not demarcated the responsibilities and powers of NPDA. A clear demarcation will assist in determining the review mechanisms that will be adopted and the extent of authority exercised by the regulatory body. There are also no changes in the way NPD has been defined. A legal definition of NPD needs to be precise, comprehensive, practicable and permanent to not be over or under-inclusive. This would be necessary to ensure transparency and to evaluate the implications of the legislation. We understand that suggesting a definition that checks all the aforementioned points would be a difficult task especially since technologies like Internet of Things, Quantum Computing, Machine Learning, and Artificial Intelligence are constantly evolving and the nature of data is constantly changing. The scope of understanding NPD has to be dynamic. There are two dimensions to NPD - one type of dataset which cannot be attributed to a person such as weather updates or traffic lights and on the other hand is personal data that has been anonymised and has become NPD. We need separate labelling for the same and develop a risk management framework accordingly. Our recommendation would be to stick with the suggested definition and work on defining the responsibilities of all the stakeholders involved in the data sharing process in a precise manner.
3. NPDA is assigned with the gargantuan task of regulating NPD. Our recommendation is to not create a separate regulator for NPD. The Data Protection Authority can have two divisions to manage personal and non-personal data. This will ensure synergy between the two frameworks and will reduce the complex interface that people have to deal with. The report suggests that the NPDA will not adjudicate the validity of data requests under sovereign purposes such as national security, law enforcement and so on. While this helps in providing a narrow focus to the NPDA, there are concerns as to which datasets would be omitted in the process.

4. Many stakeholders had raised concerns over the mandatory data sharing requirements in the previous report. The revised draft proposes to limit the scope of mandatory sharing by private businesses subject to the scope and purpose of data collected. Only High ValueDatasets fall under the ambit of mandatory sharing requests. This will assist in breaking down data silos and enable the use of this data for societal development and facilitating innovation. There are apprehensions regarding public good as the focus of the framework is to ensure maximum benefit is generated from data rather than protecting it. The definition of the public good would also help businesses understand the type of datasets they would have to share. Data licenses can be issued to the organisations and startups to limit the scope of use, re-use and data downstream to reinstate the balance of public good while ensuring privacy.

5. The revised report has proposed the creation of High Value Datasets (HVDs). HVDs will be utilised in evidence-based policymaking, better delivery of public services, and supporting societal objectives such as science, healthcare, urban planning. They would be subject to mandatory data sharing requirements and will be maintained by Data Trustees. This proposal has raised numerous concerns such as determination of HVDs, the responsibilities of data trustees and so on as there are no guidelines in place to check the granularity of the requests made. While the framework has explained which datasets would not fall under HVDs, it has not explained the scope of datasets that would fall under it. Moreover, it is important to mention the delimitations of end-users of HVDs and build accountability mechanisms to ensure that misuse of data does not happen.
6. The present framework understands that communities should be provided rights over their data but a dynamic understanding of a community seems to be missing. The idea of a community depends on belongingness and all of us have different and intersecting layers of identity. The expert committee needs to build a framework based on an intersectional understanding of the community. There remain apprehensions for representation of interests and determination of public good. The framework must ensure that the duties and responsibilities of data trustees are clearly defined, as that will avoid jurisdictional overlaps between different stakeholders involved in the data sharing process. The framework must define public good and make sure that the boundaries of a data trustee do not overlap with data fiduciary.

7. The revised report attempts to distinguish between ‘Active misuse of NPD’ and ‘Accidental misuse of NPD’ but does not define how the two will be identified. It suggests that the data custodian must have mechanisms in place to swiftly remedy the situation in both cases. We recommend a system for constant engagement to be put in place between the data trustee and the data consumers. Data trustees would have to constantly monitor how data is used and processed based on set standards so that data trustees do not overstep its boundaries under ‘duty of care’. To balance the degree of intervention and discretion to be followed by a data trustee, these standards should be backed by legislation.

8. A Data Business would be required to share the meta-data collected by them i.e. the name of the data fields, with the Non-Personal Data Authority. Mechanisms need to be developed to address competition, financial and technical risks that arise due to the formation of a meta-data directory. The traditional understanding of Intellectual Property Rights has also changed over the years. There is no doubt that this will inform citizens about the data fields collected by the industries and also help the government to identify the use cases for collected data to make public service delivery better but for companies, this would mean sharing their business models on which their products work. It would be a major concern for businesses as algorithms are proprietary and protected under IPR as they are trade secrets. The government can instead collect metadata under primary, secondary and derived categories to further divide the datasets and the risks associated with them.

9. The framework suggests that the data principals have the choice of opting out of data anonymization. This will be an added burden for young organisations and will complicate the compliance mechanism within the two frameworks. This will further increase the compliance cost. This will create friction in the data sharing process. Alternatively, we propose that the organisations should be incentivised monetarily to ensure privacy and data protection under the PDP framework.