Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees: CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.in: E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

Dated 16th March 2022

To

Ms Kavita Bhatia
Scientist
Ministry of Information Technology and Telecommunications
New Delhi
(E Mail: kbhatia@gov.in , pmu.tech@meity.gov.in)

Sub: Draft India Data Accessibility & Use Policy 2022: Feedback and Comments

This has reference to the draft India Data Accessibility & Use Policy 2022 released for public comments.

We, Foundation of Data Protection Professionals in India (FDPPI) are a Not for profit company registered under Section 8 of the Companies Act, limited by guarantee, established in 2018 by data protection professionals in India. We are dedicated to the development of developing skilled manpower in the field of Data Security and otherwise empowering the Data Protection eco system in India.

We submit herewith some of our observations on the India Data Accessibility and use policy 2022 and hope it would be of assistance to the Government.

The background paper has captured several challenges and the way forward and has indicated the following 4 objectives for the way forward.

1. Unlocking high value data across the economy
2. Facilitating a congruent and robust governance strategy
3. Realization of an interoperable digital infrastructure
4. Development of Data Skills and data driven culture

The reference to "Unlocking high value data across the economy" indicates that the primary objective of this policy is different from the objective of the DPA 2021(Erstwhile Personal Data Protection Bill 2019 or PDPB 2019) which is "Preserving the Right to Privacy of natural person through regulation of the collection and use of personal data".

Hence this policy is in close alignment with the Kris Gopalakrishnan Committee report on Non personal Data Governance and the information security principles emanating from Information Technology Act 2000 (ITA 2000).

At some part of the policy reference is made to "Privacy and Security" but this is considered as related to the "Privacy or Security of Data the inanimate object" and not the "Privacy Protection of a natural person as a fundamental right under the constitution".

This policy will have to co-exist with a "Privacy and Personal Data Protection Policy compliant with the DPA 2021" with a rider that some aspects of Non Personal Data Governance such as reporting of data breach also become part of the compliance of DPA 2021.

FDPPI recommends that the framework Data Protection Compliance Standard of India (DPCSI) has the potential to be developed into a framework for compliance of both this policy and the policy for protection of Personal Data though a description of this framework (Earlier this framework was referred to as PDPSI or Personal Data Protection Standard of India and has now been modified as Data Protection Compliance Standard of India, details of which will be available with FDPPI and/or at the website www.naavi.org.

Our detailed comments on each of the elements of the policy are as follows.

Applicability	
Policy	**Comments**
This policy will be applicable to all non personal data and information created/generated/collected/archived by the Government of India directly or through authorised agencies by various Ministries/Departments/Organizations/Agencies and Autonomous bodies.	The applicability does not include "Personal Data" and is restricted to non personal data only. However, reference under para 5.7 to "Privacy & Security by design" and the references to "Anonymisation" create a confusion whether this policy also addresses protection of "Privacy" of data principals. The concept of "Anonymisation" is more relevant for processing of "Personal Data". It is the means of converting Personal data into Non personal data. Personal Data when anonymised becomes non personal data. In the case of Non Personal Data, "Anonymisation" has no relevance. The stock of "Non Personal Data" includes a) Anonymised Personal data b) Data related to an entity other than a living natural person c) Data related to environment and other events not associated with a living natural person or a corporate or juridical entity d) "Transaction Data" coming out of E Governance and "Community Data"

	In the absence of a separate law related to "Non Personal Data Governance" which was envisioned under Kris Gopalakrishnan committee report, "Community Data" may consist of "Identifiable individual data" which is "personal" and "Anonymised community data" which is non-personal. These have to be clarified under definitions. The Kris Gopalakrishnan committee had envisaged the recognition of data ownership by Public bodies, private companies and communities and envisaged a framework for value discovery and exchange. These terms also need to be clarified in the definitions. However, it is preferable for this policy to use the term "Information Security by design" instead of the word "Privacy & Security by design" if the intention of the policy is only to regulate the non personal data. This will be consistent with the background paper which mentions "Unlocking high value data across the economy" as one of the policy outcomes. The CDO envisaged under this program can be the executive to design and implement the policies for monetization of non personal data which is presently not addressed in the PDPB 2019/DPA 2021, within the limits defined by the Data Protection Authority. Hence this policy would fill a void created by the push back on the Kris Gopalakrishna Committee report after JPC on PDPB 2019 expanded the scope of the Bill.
State Governments will also be free to adopt the provisions of this policy and the protocols as applicable	It is presumed that the Central Government would like to develop a template of Data Governance which can be later used by the different State Governments. If the State Governments are included at this stage, the project could get delayed for lack of cooperation from the State. However, some select State Government representatives may be included in a consultative committee to ensure that the specific problems encountered at the State level are taken cognizance of.

	Otherwise keeping this policy at the Central Government level for the time being is considered as the correct approach.
Principles	
Following 12 principles have been recognized under this India Data Accessibility and use policy 1. Identification of datasets for sharing 2 Transparency in operations 3. Interoperable, integrated and technology agnostic. 4 User-centred practices & systems 5 Risk managememt over risk avoidance 6 Trust among stakeholders. Systems and transactions 7 Privacy & Security by Design 8 Well-defined accountability for all stakeholders 9 Equal and non-discriminatory access **10** Regulatory clarity & structured enforcement **11** Proactive data sharing for innovation & research **12** Protection of Intellectual Property	As the name of the policy indicates, the focus of the policy is "Accessibility" and "Use". However, 12 principles have been identified for the policy. All the principles are consistent with "information security" on the basis of identified "Risk" and "Mitigation of Risk". The system requires appropriate data/data set classification and tagging before the security principles are applied. Since the data security needs to be compatible with Information Technology Act, 2000, the framework developed should be ITA 2000 compliant. Need for ITA 2000 Compliance needs to be clarified in the "Principles" . At present, it is only ITA 2000 which is the legal regulatory requirement since no personal data is involved in the implementation of this policy and hence DPA 2021 compliance may not be relevant except to the extent of Section 25 (Notification of non personal data breach notification). Since any of the existing frameworks such as ISO 27001 would not be best suited, indigenous frameworks (eg: Data Protection Compliance DPCSI) need to be adopted for this purpose which would achieve satisfactory ITA 2000 compliance.
Institutional Framework	
India Data Office, India Data Council and Chief Data officers if different departments envisaged.	The framework appears to meet the requirements.
Identification of Data Sets	
Every Government Ministry/Department/ Organisation shall identify the non-personal datasets available with it and classify them as open, restricted or non-shareable.	This is the basic classification only from the security/access perspective. The "Restricted" category may have to be separately defined to include "Critical" data which should be subject higher level of security. For the purpose of monetization it may be necessary to adopt a more detailed category related

	classifications. (Eg: National data, Regional Data, Past Data, Projected Data, etc)
Government-to-Government Data Sharing	
All government ministries/departments shall identify all existing data assets and create detailed searchable data inventories with clear metadata and data dictionaries.	Defining a data asset, it's breadth and depth should be standardised. A Data Asset may be a single element of data or a combination of data elements. Defining the boundary of a data set is complicated. A data asset may consist of a document of 1000 pages or a video of 1 hour or a data base of multiple rows and columns. A data asset element can be a single unit of a name or a number. In the context of personal information, a data asset can be any "Identifier" which along with other elements represent "Data about a person". The core of personal data is an identifiable natural person. All data attributable to the core person is one data asset. In the context of non personal information, a data asset needs to be identified to a core element which could be an "Object" or "Event". All data about the core object or event would be a data asset. It could be a document in PDF or word or a video or a data base or an entire website. A Data asset may be a combination of data elements. This is similar to the structure of matter which consists of the nucleus consisting of Protons, Neutrons, an Element comprising of a stable combination of the nucleus and associated electrons, a molecule consisting of a stable combination of multiple elements to an organic compound of a complex structure of bonded molecules. The definition and examples of how a data asset should be defined need to be part of this document. Appropriate identity parameters for data sets need to be defined.
Approved inventories will be federated into a government-wide searchable database for government-to-government data sharing. This will minimize duplication of data processing efforts and enable better delivery of citizen centric services.	Creating a search base is dependent on the definition of a data asset since the key terms need to include both identity of data elements and the identity of the larger data atom and data molecule.
Integrated Data Portals	
All data portals/dashboards maintained by line ministries/departments should be integrated through APIs or other	No comments

appropriate integration mechanisms with the open government data portal	
Technical & implementation support required by line ministries/ departments to integrate their dashboards/ data portals shall be provided by lndia Data Office.	No Comments
Protocols for sharing of non-personal datasets	
India Data Office will notify protocols for sharing of non-personal datasets. Most datasets shall be made available at no cost to promote innovation and research & development	No Comments
Departments/Ministries of Central & State Government organisations and institutions may notify certain datasets for restricted access and define the protocols and processes for access and sharing of such datasets.	No Comments
To incentivise and promote such data sharing, innovative and just licensing frameworks that enable fair access and use will be made available by India Data Office which can be used by concerned ministries/departments.	No Comments
For restricted access data sharing as per the licensing model adopted, the processes and protocols will be decided by the concerned government department or agency and must be notified in a transparent manner	No Comments
Data Quality & Meta-Data Standards	
Each Central Ministry/Department shall adopt and publish its domain-specific metadata and data standards. These standards should be compliant with the interoperability framework, Policy on open standards, Institutional Mechanism for Formulation of Domain-specific Metadata and	No Comments

Data Standards and other relevant guidelines published on the e-gov standards portal.	
Data standards that cut across domains shall be finalised by India Data Council and once finalised adopted by all concerned government ministries/departments.	No Comments
Data Anonymization and Privacy Preservation	
Reference anonymisation tools and decision-making frameworks will be provided to all ministries/departments to assist data officers in managing data sharing requests.	The term "Anonymisation" is normally used in the context of Personal data and not in the context of non personal data. In the context of personal data, "Anonymisation" refers to an irreversible removal of personal identity parameters associated with a data set which results in conversion of personal data set to a non personal data set. Policy should clarify that "Anonymisation" refers to the "Governance of Personal Data" and should be used by the "Personal Data Protection Officer" as defined under the DPA 2021. Once the personal data becomes "Anonymised personal data", it is one category of Non Personal Data. "Anonymisation" defines the boundary between personal and non personal data. Once a personal data is anonymised, it should not be technically feasible for re-identification and any attempt made thereof maybe an offence under DPA 2021. The question of de-anonymisation as a theoretical possibility is like saying that any encryption can ultimately be broken with a deployment of adequate resource for discovering the decryption key. It may be theoretically possible but the anonymisation standard has to be defined to set the boundaries of what is a reasonable security for anonymisation. Just as in encryption we may say 1024 key encryption is considered a sufficient level of encryption for one type of data while a 2048 key encryption may be the sufficient level for another set of data, the anonymisation levels need to be defined for "Non Sensitive personal data", "Sensitive Personal Data" and "Critical Personal Data" separately. Defining the "Anonymisation Standard" has to be the responsibility of the Data Protection Authority under DPA 2021 and the role of the IDO should be only to implement the standard set by the DPA with due diligence.

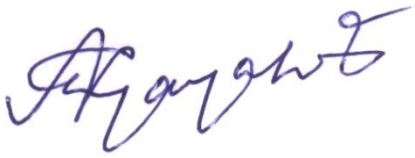
All ministries/departments must comply with the anonymisation standards defined by IDO/MeitY or by any statute/act/policy issued by the government of India.	Refer above
Any data sharing shall happen within the legal framework of India, its national policies and legislation as well as the recognized international guidelines.This will prevent misuse of data and assure security,integrity and confidentiality of data.	No Comments
Data Retention	
Each Central Ministry/ Department shall define its data retention period for specific datasets and ensure compliance with the same while managing storage and sharing of datasets.	No Comments
A broad set of guidelines would be standardized and provided to help ministries/departments define their data retention policy. These can be based on the DQGI framework notified by NITI Aayog.	No Comments
Capacity & Skill Building Measures	
Competitive capacity building and training initiatives for government officials is imperative to build capacity in all government agencies to manage, publish and make use of data.	No Comments
India Data Office will assist in setting up of Data Management Units in Ministries and Departments to create dedicated capacity for data management.	No Comments
Data Sharing Toolkit	
A data-sharing toolkit will be provided to all ministries/departments to help	No Comments

assess and optimally manage risk associated with data sharing and release. The framework will help data officers to identify whether the data set qualifies for release, restricted sharing or needs to be on the negative list, identify the appropriate release mechanism and the required degree of anonymisation.	
Data shall remain the property of the agency/department/ ministry/ entity which generated/collected it. Access to data under this policy shall be strictly in accordance with any act and rules of the government of India in force. Legal framework of this policy shall be aligned with various acts and rules covering the data.	Ownership tag has to be assigned in the classification of data into data sets and the disclosure permissions.
The acquiring organization/ individual shall always cite the original data source and assume all responsibilities as to the use, analysis and interpretation of the data being provided.	No Comments
All data being shared must ensure compliance to guidelines for legal, security, IPR, copyrights and privacy requirements.	It is necessary to have a close coordination with the relevant DPO of the Ministry or the Department who has to be responsible for compliance to DPA 2021
Policy Monitoring & Enforcement	
India Data Office. constituted by MeitY shall be entrusted with the responsibility of monitoring the implementation and enforcement of this policy.	No Comments
India Data Council shall be the entity responsible for finalizing Data standards and Metadata standards. The department which is the primary owner of a particular dataset shall also be an associate member of India Data Council for the concerned dataset.	No Comments
The India Data Council will be supported by a dedicated support	No Comments

unit to coordinate data sharing across Ministries. provide technical support and periodically evaluate their performance.	
Implementation Manual	
Detailed implementation guidelines including the data sharing toolkit, criteria and mechanism for restricted access data sharing, licensing frameworks and sharing models would be brought out by the Ministry of Electronics & Information Technology.	No Comments

Thanking you

Yours faithfully



Na.Vijayashankar
Chairman