Report Summary

Non-Personal Data Governance Framework

- The Expert Committee constituted by the Ministry of Electronics and Information Technology (Chair: Mr. Kris Gopalakrishnan) to study various issues relating to non-personal data submitted its report in July, 2020. The Committee observed that non-personal data should be regulated to: (i) enable a data sharing framework to tap the economic, social, and public value of such data, and (ii) address concerns of harm arising from the use of such data.
- **Non-personal data:** Any data which is not personal data (data pertaining to characteristics, traits or attributes of identity, which can be used to identify an individual) is categorised as non-personal data. In terms of origin, non-personal data can be data which never related to natural persons (such as data on weather or supply chains), or data which was initially personal data, but has been anonymised (through use of certain techniques to ensure that individuals to whom the data relates to cannot be identified).
- Non-personal data can further be classified as: (i) Public non-personal data: data collected or generated by the government in course of publicly funded works. For example, anonymised data of land records or vehicle registration can be considered as public non-personal data. (ii) Community non-personal data: raw or factual data (without any processing) which is sourced from a community of natural persons. For example, datasets collected by municipal corporations or public electric utilities. (iii) Private non-personal data: data which is collected or generated by private entities through privately owned processes (derived insights, algorithms or proprietary knowledge).
- **Risks associated with non-personal data:** The Committee observed that even when personal data has been anonymised, the possibility of harm to the original data principal exists as no anonymisation technique is perfect. Therefore, it is necessary to address privacy concerns arising from possible re-identification of anonymised personal data, to ensure no harm is caused due to such processing. The Committee recommended certain categories of data to be considered as sensitive based on the risks: (i) non-personal data which is derived from sensitive personal data (such as health, caste or tribe) which bears a risk of re-identification, (ii) data which bears risk of collective harm to a group, and (iii) data related to national security or strategic interests.
- **Key roles in non-personal data governance framework:** The data principal is the entity to whom the non-personal data relates to. This entity can be an individual, a community, or a company. A data custodian collects, stores and processes data in a manner that is in the best interest of data principal. Data principals may exercise rights over their data through a representative entity, called data trustee. For example, Ministry of Health would be the trustee for health data of the citizens. Trustees can recommend transparency and reporting obligations to the regulator for data custodians to follow. The Committee recommended establishing 'data business' as a new category of business in the country. Entities (including government agencies) which collect, process or store data beyond a threshold (as specified by the regulator) will be classified as data businesses.
- **Non-Personal Data Authority:** This regulatory authority will be established for putting in place the framework for governance of non-personal data. It will consist of experts in fields such as data governance and technology. The Authority will be responsible for framing guidelines with respect to data sharing and risks associated with non-personal data.
- **Sharing of non-personal data:** Any entity may raise a data-sharing request for a: (i) sovereign purpose (such as national security or legal requirements), (ii) public interest purpose (policy making or better delivery of services), or (iii) economic purpose (to provide for a level playing field or for a monetary consideration). The Committee recommended that public data, community data or private data (limited to raw/factual data collected by a private entity) can be requested at no remuneration. Private data where the processing value add is significant may be shared based on remuneration which is fair, reasonable and non-discriminatory. Algorithms or proprietary knowledge may not be considered for data sharing. Data sharing request can be made to a data custodian. If the custodian refuses the request, the request will go to the Authority which will evaluate it based on social, public or economic benefits of such data sharing.
- Further, all entities will have open access to meta-data of data collected by data businesses (including government). Meta-data provides information about other data. The Committee observed that this will encourage innovation in the country. For example, automobile companies may collect data about roads through censors. The meta-data provided by such companies can be used by a startup to combine it with traffic data to identify safest routes for citizens.

Anurag Vaishnav
anurag@prsindia.org

July 28, 2020