HSA ADVOCATES
HEMANT SAHAI ASSOCIATES

LAW & POLICY UPDATE

TECHNOLOGY, MEDIA & TELECOMMUNICATIONS

Regulatory framework for non-personal data proposed

By: Ashni Gupta, Manager

A draft Personal Data Protection Bill, 2019 (**Draft Privacy Bill**) is presently being considered by the Indian Parliament. In September 2019, the Ministry of Electronics and Information Technology (**MeitY**) constituted a committee of experts (**Committee**) to study and provide it suggestions on regulating non-personal data. The Committee released its report on Non-Personal Data (**NPD**) Governance Framework (**Report**) on July 12, 2020 and made substantive recommendations on the scope, classification, ownership and other issues related to non-personal data. It also made a clarion call for a comprehensive non-personal data regulation in India, to complement the future law dedicated to personal data.

Key recommendations of the Report

- **Definition of NPD:** The report defined NPD as any data that is not personal data and classified into three categories, namely public, community, and private. Public NPD includes data collected or generated by government agencies, community NPD includes anonymized data and private NPD includes data related to privately owned assets of a person or entity or derives as a result of private effort.
- **Sensitive NPD:** The Report defined a new concept of 'sensitivity of Non-Personal Data', as even Non-Personal Data could be sensitive such as data relating to national interest, business interests, or confidential information and anonymized data which bears the risk of re-identification.
- **New regulatory mechanism and authority:** The report suggests the establishment of a separate regulatory authority to enforce underlying rules, undertake risk evaluations and ensure NPD is shared for spurring innovation in the country. The Committee has also recommended the formulation of a new law for the regulation and management of NPD.
- **Regulation of data business:** An organization that collects and provides services using NPD becomes a data business. Such entities have to disclose that they are a data business to the non-personal data regulator. The requirement for registration will be triggered by a threshold decided by regulators.
- **Stakeholders:** Data principal (the person to whom the NPD relates), data custodian (the person who collects/stores, processes, and/or uses the NPD), data trustees (rights based group/community of data principals) and data trusts (institutional structures, comprising specific rules and protocols for maintaining and sharing a given set of data) have been identified as stakeholders that are proposed to be regulated.
- **Consent for anonymized data:** The Report recommends that the data principal should also provide consent for anonymization and usage of the anonymized data while providing consent for collection and usage of his/her personal data. The appropriate standards of anonymization will also be defined to prevent/minimize the risks of re-identification.
- **Ownership of data:** The Report developed certain guiding principles for establishing legal rights over data. These include:
  - **Data sovereignty:** Where data sets are considered a national resource, they will be owned by the State
  - **Beneficial ownership/interest:** In case of community NPD, rights over the NPD would vest in a trustee and the community would be the beneficial owner
  - **Origin:** NPD derived from personal data will be owned by the individual whose personal data is underlying the NPD

- **Data storage:** The principles for storage of personal data stated in the Draft Privacy Bill are suggested for NPD as well. Data storage should be in a distributed format so that there is no single point of leakage and sharing is to be undertaken using APIs only, so that all requests can be tracked and logged. Sensitive NPD may be transferred outside of India but shall continue to be stored locally and critical NPD, which is to be defined and notified by the Government, can only be stored and processed in India. General NPD may be stored and processed anywhere in the world.
- **Data sharing:** Data sharing refers to the provision of controlled access to private sector data, public sector data and community data to individuals and organizations for defined purposes and with appropriate safeguards in place. NPD may be requested by government agencies, citizens, start-ups, companies, NGOs, research institutes and universities for sovereign purposes, core interest public purposes and economic purposes. The report proposes the development of a data sharing mechanism for various purposes and the different categories of NPD.

Data is increasingly taking centre-stage across almost all economic sectors around the world. Data protection and information privacy have been gaining mainstream momentum in India with the forthcoming comprehensive regime for the protection of personal data. The ownership and use of NPD – which refers to data that lacks any personally identifiable information or is data that has been anonymized – is the second prong of the Indian Government's approach to 'data sovereignty.'

While the report is helpful in setting context for the forthcoming regulations for non-personal data and in proposing a data governance regime, the Government is likely to evaluate its content, hold wider consultations and consider other policy aspects prior to formulating a comprehensive data framework governing non-personal data in India.