

## Member Consultation | Report of the committee of experts on Non-Personal Data

The Ministry of Electronics & Information Technology (MeitY) constituted a Committee of Experts to deliberate on a Data Governance Framework (committee). Office Memorandum No. 24(4)/2019-CLES dated 13.09.2019 was issued to create the 8-member committee. Stated goals for the committee were:

- a. To study various issues relating to Non-Personal Data.
- b. Provide specific suggestions for consideration of the Central Government on regulation of Non-Personal Data (NPD).

The committee under the chairmanship of Mr. Kris Gopalakrishnan (Co-Founder, Infosys) and comprising of Ms Debjani Ghosh (President, NASSCOM), Mr. Parminder Jeet Singh (Executive Director, IT For Change), Mr. Lalitesh Katragadda, (CTO, Avanti Finance), Dr Ponnurangam Kumaraguru, (IIIT Hyderabad), Shri Gopalakrishnan S., (former Additional Secretary, MeitY), Dr Neeta Varma (Director General, National Informatics Centre, Government of India), Additional Secretary/Joint Secretary, Department for Promotion of Industry and Internal Trade ("DPIIT"), Ministry of Commerce and Industry, released its report on July 12, 2020.<sup>i</sup>

The recommendations of the report are summarised below:

1. **Objectives for regulating NPD:** **a)** To generate economic benefits for citizens and communities in India and unlock the immense potential for social / public / economic value data. **b)** To create certainty and incentives for innovation and new products / services creation in India (encourage start-ups in India). **c)** To create a data sharing framework such that community data is available for social /public / economic value creation and **d)** To address privacy concerns, from re-identification of anonymised personal data, preventing collective harms arising from processing of Non-Personal Data, and to examine the concept of collective privacy. (Para 3.8, Page 11)
2. **Definition of NPD (Scope):** The committee has defined three categories of NPD-
  - a. **Public NPD** – NPD collected or generated by the Government, or by any agency of the Government, and includes data collected or generated in the course of execution of all publicly funded works. Provided that all non-personal data collected or generated by the Government where such data is explicitly afforded confidential treatment under a law, it shall not constitute public non-personal data.<sup>1</sup> (Para 4.2, Page 14)
  - b. **Community NPD** – NPD, including anonymized personal data, and NPD about inanimate and animate things or phenomena – whether natural, social or artefactual, whose source or subject pertains to a community of natural persons. Provided that such data shall not include Private NPD. (Para 4.3, Page 14-15)
  - c. **Private NPD** – NPD collected by persons or entities other than the Government, the source or subject of which relates to assets and processes that are privately-owned by such person or entity and includes those aspects of derived and observed data that result from private effort. (Para 4.4, Page 15)
3. **Sensitive NPD:** The Committee has also defined a new concept of 'sensitivity of Non-Personal Data', recommending that NPD could be sensitive from the following perspectives – **a)** It relates to national security or strategic interests; **b)** It is business sensitive or confidential information; **c)** It is anonymised data, that bears a risk of re-identification. The sensitivity taxonomy seen in the Personal Data Protection Bill, 2019 has been adopted by the committee, to classify NPD as General NPD, Sensitive NPD and Critical NPD. The report states that Non-Personal Data inherits the sensitivity characteristic of the underlying Personal Data from which the Non-Personal Data is

---

<sup>1</sup> **Examples of Public Non-Personal Data:** a) Anonymised data of land records, public health information, vehicle registration data etc. b) A university collects pollution levels in the city based on a publicly funded project.

derived. Therefore, the Non-Personal Data arising from Sensitive Personal Data may be considered as sensitive Non-Personal Data.<sup>2</sup> (Para 4.5, Page 15-16) Hence, the conditions of transfer and storage restrictions applicable to the underlining personal data would also apply to NPD based on sensitivity.<sup>3</sup>

- (a) General NPD can be transferred outside India and stored anywhere in the world;
- (b) Sensitive NPD can be transferred outside India based on the conditions transfers laid down in the Personal Data Protection Bill, 2019, and it must continue to be stored in India.
- (c) Critical NPD to be stored only in India.

4. **Consent for anonymisation:** The Committee recommends that the data principal should also provide consent for anonymisation and usage of this anonymized data while providing consent for collection and usage of his/her personal data. (Para 4.6, Page 17)
5. **Roles and Stakeholders in the NPD Ecosystem:** The following are the roles and stakeholders have been envisaged in the report-
  - a. **Data Principal** - The Data Principal, in case of NPD that is anonymized personal data will be the Data Principal of the personal data so anonymized. In case of Community NPD, the relevant community. (Para 4.7, Page 19)
  - b. **Data Custodians** – The Data Custodian undertakes collection, use, processing, storage, etc. of data in a manner that is in the best interest of the Data Principal, with “best interests” being defined under relevant legislative instruments, and closely aligned with the well-defined grounds of “public purpose”. (Para 4.8, Page 19)
  - c. **Data Trustees** – Are trustees of the Data Principal’s beneficial interests in NPD. The primary role of the Data Trustees should be of safeguarding the interests of the Data Principal, and advising the NPD Authority on whether the sharing and processing of NPD is in the interest of the Data Principal; and informing the NPD Authority of instances where Community NPD is processed in a manner detrimental to the Community and leading to consequent harms. The legitimate trustee for any set of community data will be the closest and most appropriate representative body for that Community, which would be an appropriate Central/ State/ Local Government agency. (Para 4.9, Page 20)
  - d. **Data Trusts** – Are institutional mechanisms constituted of specific rules and protocols for containing and sharing a given set of NPD. These will be the interfaces between Data Custodians, Data Businesses, Data Trustees and the NPD Authority. (Para 4.10, Page 21)
  - e. **Data Business** – Are Data Custodians who, by reason of their usage of NPD beyond certain thresholds, are registered as a Data Business. Data business is not an independent industry sector. It is a horizontal classification cutting across different industry sectors. This will be applicable to not only commercial organizations, but also Governments and other non-government organizations that collect, process or otherwise manage data. (Para 6.1,6.2, Page 27-28)
  - f. **NPD Authority** – The regulator in charge of enabling the sharing of data, enforcing rules on data sharing and harm prevention, and mitigating the risks of NPD sharing. Given overlapping issues of jurisdiction, the NPD Authority will have consultative obligations with the Data Protection Authority (DPA) and the Competition Commission of India (CCI) (Para 8.2, Page 40,41)
6. **Ownership of data:** The committee recommends that a) where Non-Personal Data is derived from personal data of an individual, the data principal for personal data will continue to be the data principal for the Non-Personal Data, which should be utilized in the best interest of that individual and b) that the rights over community Non-Personal Data collected in India should vest with the trustee of that community, with the community being the beneficial owner, and such data should be utilized in the best interest of that community. (Para 5.1, Page 23)

---

<sup>2</sup> For example: If the Non-Personal Data is about health of people (even though it may be anonymised and aggregated), on the sensitivity spectrum it will be classified as Sensitive Non-Personal Data since the underlying data (on health) is classified as Sensitive Personal Data as per Clause 3 (36) of the PDP Bill.

<sup>3</sup> Clause 33, 34, Personal Data Protection Bill, 2019.

7. **Non-Personal Data Sharing:** Data sharing is the core objective for the regulation. The report recommends sharing of NPD through voluntary as well as mandatory mechanisms.
  - a. **Voluntary Mechanisms:** Voluntary mechanisms will include voluntary sharing of NPD on an NPD Exchange. This will function as an NPD marketplace and enable access to NPD that is not covered within the scope of mandatory mechanisms.
  - b. **Mandatory Mechanisms:** Given the recognition of the economic, social and public value of NPD, mandatory sharing of NPD may take place on either of the following grounds:
    - I. **Sovereign Purpose:** Mandating the sharing of NPD required for discharging Sovereign Functions of the State. (Para 7.1, Page 32)
    - II. **Core Public Purpose:** Mandating the sharing of NPD on well-defined grounds of public interest, especially when NPD has high social and public value associated with it (for example, traffic data sets, weather and climate data sets, etc.) This should be subject to compensation. Absent such compensation private investment in NPD Datasets having high social and public value will reduce. (Para 7.2, Page 33)
    - III. **Economic and Regulatory Purpose:** Mandating the sharing of NPD, for ensuring a level playing field, or other regulatory purpose. Equally, mandating the sharing of NPD for unlocking its economic potential. This should be subject to licensing and compensation on a fair, reasonable and non-discriminatory (FRAND) basis. (Para 7.4, Page 34)
8. **Technology Architecture:** The report lays down the guiding principles for the proposed architecture- a) API mechanisms for accessing data, b) Data security – storage in distributed format, c) Creating a standardized data exchange approach (regardless of data type, exchange method or platform) and d) Preventing de-anonymisation through usage of different techniques to prevent re-identification. (Para 9.1, Page 44)

Member inputs (if any) are sought on the aforementioned recommendations of the committee, and any other recommendation laid down in the report, which the member organisation wishes to comment on. Please send your feedback by **3<sup>rd</sup> August (Monday), 2020** to [membership@dsci.in](mailto:membership@dsci.in) or [anand.krishnan@dsci.in](mailto:anand.krishnan@dsci.in)

---

<sup>i</sup> Report of the Committee of Experts on Non-Personal Data Governance Framework, available at [https://static.mygov.in/rest/s3fs-public/mygov\\_159453381955063671.pdf](https://static.mygov.in/rest/s3fs-public/mygov_159453381955063671.pdf)