



## ERGO

*Analysing developments impacting business*

### NEW NON-PERSONAL DATA FRAMEWORK IN THE WORKS - KEY CONSIDERATIONS

13 August 2020

The Ministry of Electronics & Information Technology (MeitY) have constituted a committee of experts to deliberate a data governance framework alongwith issuing an Office Memorandum No. 24(4)/2019-CLES dated 13 September 2019 to create an 8 member committee (NPD Committee) to study issues and make suggestions pertaining to the regulation of non-personal data (NPD). The NPD Committee has published a report titled 'Report by the Committee of Experts on Non-Personal Data Governance Framework' on 12 July 2020 (NPD Report).

The stated objectives for creating a new framework under the NPD Report were:

- Increased transparency through sharing NPD collected by government and private entities;
- Assisting businesses in creating new services and products;
- Helping researchers, academia and governments for creating public goods and services; and
- To create a level playing field for all Indian players to maximise Indian data's value and to ensure fair and effective competition in digital and data markets and industry.

#### Definition of NPD

A general definition of NPD has been provided as:

- Data that was never related to identified or identifiable natural persons;
- Data which may have been personal data, but was later anonymised; and
- Data that is aggregated and transformed to an extent that individual-specific events are not identifiable.

#### Categorisation of NPD

Three categories of NPD have been proposed by the NPD Committee:

- **Public NPD:** Data obtained by governmental entities including data obtained in the course of execution of all publicly funded works. Data that is explicitly

afforded confidentiality under law is excluded. Examples include land records, public health information, publicly funded research, etc.

- **Community NPD:** Anonymised personal data and NPD pertaining to phenomena whose source or subject pertains to a community of natural persons. Private NPD has been excluded. Examples include public utility data, telecom data, etc.
- **Private NPD:** Data collected or produced by entities other than governments, the source or subject of which relates to (or derived from) privately owned assets or processes. This includes generative adversarial networks, or data derived through proprietary processes.

## Categorisation of Sensitivity

The NPD Committee has proposed that the NPD be further categorised on the basis of the underlying personal data into (i) general; (ii) sensitive; and (iii) critical NPD. Some perspectives which have been considered for categorising sensitive data, include:

- National security and strategic interests;
- Risk of collective harm to groups;
- Business sensitivity and confidential information; and
- Risk of de-anonymising data.

## Stakeholders in the NPD Ecosystem

The NPD Committee has identified four classes of stakeholders:

- **Data Principal:** The data principal will be defined on the basis of the type of NPD collected (ie public, community, and private data). The principal would be the natural person to whom the collected data relates.
- **Data Custodian:** This is the entity undertaking collection, storage, use, etc of the data collected. Custodians may be considered to be data fiduciaries and be required to act in the 'best interest' of data principals. Further, a duty of care would arise to community from which the data is derived. Compliances such as recommended data practices, anonymisation standards, and data sharing standards and practices have been proposed.
- **Data Trustee:** The data principal group / community will exercise its data rights through an appropriate community data trustee, which would exercise such rights on behalf of the group / community. The report is silent on whether private entities can be data trustees.
- **Data Trusts:** These are institutional structures that will create specific rules and protocols for containing and sharing data. Governmental and some non-profit non-governmental entities are envisaged as data trusts.

## Ownership of data

The NPD Committee has adopted the notion of 'beneficial ownership / interest' of data due to the potentially overlapping ownership rights and privileges due to the nature of NPD.

- Individuals would be data principals in case of NPD derived from individuals;

- A data trustee, who is the closest and most appropriate representative of a community, shall have the rights and privileges over Community NPD; and
- The NPD Committee has also proposed that Public NPD be treated as a national resource.

In addition to the above, all data generated / collected in India or about Indian subjects or by Indian entities shall be subject to the Indian regulatory framework.

## Data Businesses

Any business deriving economic value through data, above a prescribed threshold, shall be required to mandatorily register as a data business. Any businesses below the prescribed threshold also have the option to voluntarily register as a data business. The NPD Committee has stated that the registration process would be light touch through prescribed means, with certain specified disclosures and submissions, and not a license requirement.

## Sharing of NPD

The NPD Committee has envisaged a framework for sharing of NPD. Appeals to the Non-Personal Data Authority (NPDA) has also been envisaged for data sharing requests that are rejected. The NPD Committee also had some key considerations:

- Data may be shared for sovereign purposes, core public interest, or economic purposes;
- Checks and balances to be created to ensure compliance with data sharing requirements;
- Only raw / factual data to be shared by private entities; and
- Valuation of remuneration to be determined on the basis of 'value-add'.

Cross-border restrictions discussed include: (i) General NPD can be stored and processed anywhere in the world; (ii) Sensitive NPD may be transferred outside India, but would continue to be stored within India as well; and (iii) Critical NPD may only be stored and processed in India.

## Non-Personal Data Regulatory Authority

The NPDA will be created under the proposed framework. Unlike the Data Protection Authority (under the Personal Data Protection Bill, 2019), the NPDA will be focused on unlocking value in NPD instead of prevention of personal harm. It would be a proactive support for the industry, instead of being empowered like a traditional regulator. The NPDA will combat lack of information pertaining to NPD usage, addressing negative externalities caused by NPD collection, and ensuring sufficient levels of competition and access to NPD.

The mandate of the NPDA will include:

- Power to regulate data businesses;
- Imposing mandatory sharing requirement; and
- Certifying rules and technology frameworks for data sharing, security, anonymisation, etc.

### Comment

*Considering the immense economic value and wealth that data can generate and contribute to a nation and to avoid the emergence of a few dominant players in the data industry creating an imbalance in the data market, India has sought to regulate the creation and use of non-personal data. While the aim and object of creating the NPDA is valid and necessary, the MeitY will need to address concerns and obtain the support of private players for the new framework to become a success, especially considering the voluntary nature of a majority of compliances. Further, the government's role in sharing public NPD with Indian entities and other private players including foreign multinationals and companies registered in India (but with foreign shareholding) for the common economic good of Indian citizens is still unclear and unaddressed in the report.*

*It is necessary to emphasise that Government will need maintain a clear-cut segregation between the nature of data to be regulated under upcoming personal data protection legislation and framework finalised for regulating NPD. The key concepts under parallel framework will need to steer clear of any overlaps so that reasonable efforts made towards protecting data do not get stifled. The final law governing the NPD should take into account the broad level suggestions of the industry members and frame simplistic law with underlying objective that data would be used for innovations, creation of new products/services as well as for public good.*

- Harsh Walia (Partner), K A Alakiri (Principal Associate) and Rohit Beerapalli (Associate)

For any queries please contact: [editors@khaitanco.com](mailto:editors@khaitanco.com)

*We have updated our [Privacy Policy](#), which provides details of how we process your personal data and apply security measures. We will continue to communicate with you based on the information available with us. You may choose to unsubscribe from our communications at any time by clicking [here](#).*

#### **For private circulation only**

The contents of this email are for informational purposes only and for the reader's personal non-commercial use. The views expressed are not the professional views of Khaitan & Co and do not constitute legal advice. The contents are intended, but not guaranteed, to be correct, complete, or up to date. Khaitan & Co disclaims all liability to any person for any loss or damage caused by errors or omissions, whether arising from negligence, accident or any other cause.

© 2020 Khaitan & Co. All rights reserved.

#### **Mumbai**

One Indiabulls Centre, 13<sup>th</sup> Floor  
Tower 1 841, Senapati Bapat Marg  
Mumbai 400 013, India

T: +91 22 6636 5000  
E: [mumbai@khaitanco.com](mailto:mumbai@khaitanco.com)

#### **New Delhi**

Ashoka Estate, 12th Floor  
24 Barakhamba Road  
New Delhi 110 001, India

T: +91 11 4151 5454  
E: [delhi@khaitanco.com](mailto:delhi@khaitanco.com)

#### **Bengaluru**

Simal, 2nd Floor  
7/1, Ulsoor Road  
Bengaluru 560 042, India

T: +91 80 4339 7000  
E: [bengaluru@khaitanco.com](mailto:bengaluru@khaitanco.com)

#### **Kolkata**

Emerald House  
1 B Old Post Office Street  
Kolkata 700 001, India

T: +91 33 2248 7000  
E: [kolkata@khaitanco.com](mailto:kolkata@khaitanco.com)