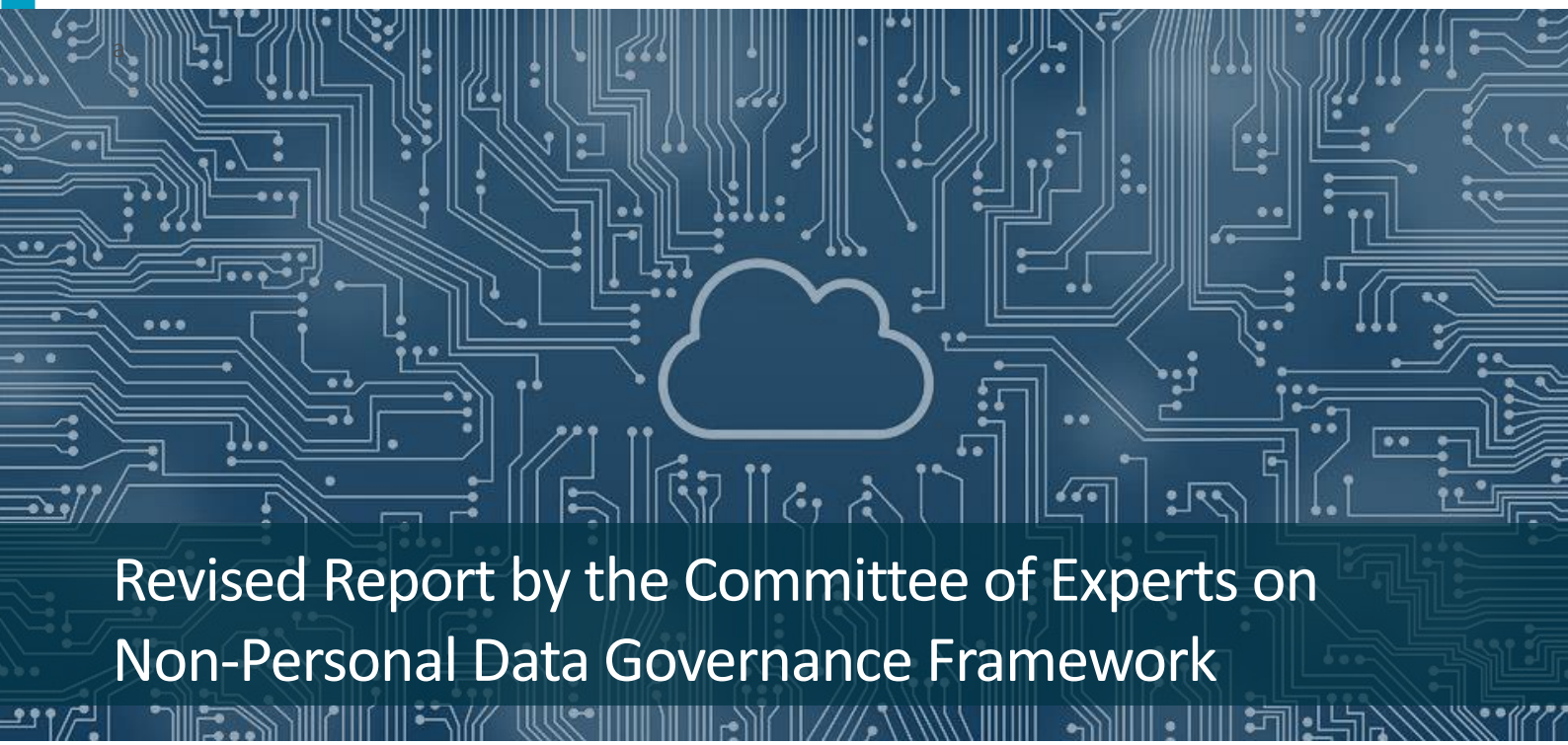
TRILEGAL



Revised Report by the Committee of Experts on Non-Personal Data Governance Framework

08 January 2021

This analysis covers:

The Ministry of Electronics & Information Technology (**MeitY**) constituted a Committee of Experts (**Committee**) in September 2019, to deliberate and devise a framework for governing non-personal data (**NPD**). This Committee released an initial report (**Initial Report**) for public consultation in July 2020, which proposed the introduction of legislation governing NPD (**NPD Legislation**), to be enforced by an NPD authority (**NPDA**) and laid down key principles to be incorporated in the NPD Legislation.

On the basis of over 1500 representations and submissions from industry bodies, companies, civil society and independent experts, the Committee has released a revised report (**Report**) which modifies the previous framework and addresses several issues raised with respect to the Initial Report. Notably, the Revised Report aims to provide more clarity on the definition of NPD and its categorisation, attempts to delineate the difference in the governance of personal data (**PD**) and NPD, streamlines the data sharing purposes that are subject to regulation and modifies the data sharing mechanism. Public submissions on the Revised Report are being accepted till 27 January 2021.

The revised Report introduces key changes to the proposed non-personal data framework including harmonising the legal framework applicable to personal and non-personal data, streamlining data sharing purposes, conceptualising high-value datasets, and modifying the data sharing mechanisms.

We have briefly analysed the key recommendations of the Committee, while also highlighting key changes made from the Initial Report.

1 Objectives

The objectives laid down by the Committee in the Revised Report remain unchanged from those set out in the Initial Report, with the regulation of NPD being considered necessary to (i) generate economic, social and public value from the use of NPD for its citizens and communities; (ii) incentivize innovation and creation of new products/services in India and encourage start-ups; and (iii) address privacy concerns from processing NPD and to examine the concept of collective privacy.

2 Definition of NPD

The Committee has retained the broad definition of NPD in the Initial Report, which defines NPD as data that either (i) never related to an identified or identifiable natural person; or (ii) is sourced from PD, as defined under the Personal Data Protection Bill, 2019 (**PDP Bill**), i.e. data which was initially personal but was later aggregated and made anonymous.

The Initial Report had categorised NPD into three distinct categories i.e. Public, Private and Community NPD, with each category having distinct ownership rights. While the Revised Report has done away with this explicit categorisation, the underlying concepts of Public, Private and Community Data have been retained in the Revised Report.

Notably, the scope of Private NPD, still includes data in a global dataset and which is collected in foreign jurisdictions. Although sharing this data for High Value Datasets (**HVDs**) appears to be exempt, no further clarity is given on how the Revised Report applies to this data. This is likely to have an adverse impact on outsourcing into India.

3 Sensitivity and Localisation of NPD

The Initial Report had created additional categories of NPD classified as 'Sensitive NPD' or 'Critical NPD', which would inherit the sensitivity of the underlying category of PD from which it is derived. The location where NPD was to be stored was required to follow the localisation requirements for the corresponding PD under the PDP Bill, with a copy of all Sensitive NPD being stored in India, while all Critical NPD being stored only in India. The Initial Report had also added certain other grounds on which NPD may be classified as sensitive, such as (i) national security or strategic interests such as vital infrastructure; (ii) business sensitivity or confidentiality; and (iii) risk of collective harm.

The Revised Report does not create such an explicit classification but instead states that NPD that forms a part of an HVD would inherit the sensitivity of the underlying PD for the purposes of complying with the corresponding localisation requirements. It does not base the sensitivity classification on subjective factors such as national security, strategic interest, or risk of collective harm. Unlike the Initial Report, the Revised Report does not discuss the treatment of NPD derived from underlying critical PD (as defined under the PDP Bill), and it is unclear whether such NPD would also be subject to corresponding localisation requirements.

4 Regulation of PD and NPD

The Initial Report had several ambiguities in relation to how NPD and PD were to be separately governed by the proposed legislation on NPD and the PDP Bill respectively. Any PD that has been anonymized becomes NPD that automatically falls outside the purview of the PDP Bill. However, there is a potential for overlap between these two regimes, given that anonymised PD which is classified as NPD has the potential to be re-identified, thereby making it PD. The Initial Report recognised this risk and recommended that appropriate standards of anonymisation be defined to prevent or minimize the risks of re-identification. The custodians are also required to obtain consent for the anonymisation of the PD and the subsequent use of the anonymised data.

The Revised Report introduces several clarifications to the Initial Report that seek to harmonise the PD and NPD regimes, with respect to regulation of data, prescribed operational standards and thresholds, as well as specific amendments to avoid overlaps. Firstly, it clarifies that any NPD that may be re-identified in any manner would once again be governed by the PDP Bill. On this basis, the Revised Report also goes on to recommend specific amendments to be made to the PDP Bill to ensure that there is no overlap in regulation. The Revised Report also clarifies that where a dataset contains inextricably linked PD and NPD, it would be governed under the PDP Bill. The Revised Report goes on to recommend that the standards of anonymisation under the NPD framework be harmonised with those prescribed under the PDP Bill to ensure standard practices can be followed by all data collection entities.

With respect to consent for anonymisation of data, the Revised Report has diluted the explicit consent requirement under the Initial Report. The Committee has now suggested that Data Principles be notified of anonymisation, and that they would be able to exercise control in the form of an opt-out to anonymisation. Such an opt-out would function prospectively, and would not impact any past anonymisation carried out before the exercise of the opt-out. However, where such data has not already been anonymised, they can withdraw their consent for any future anonymisation.

5 Data Businesses

The Revised Report retains the concept of Data Businesses, which are public and private sector entities who collect, process, store or otherwise manage NPD. The Revised Report clarifies that a Data Processor could also be a Data Business. Similar to the Initial Report, only those entities who meet specific thresholds are required to register as Data Businesses, and the Revised Report provides greater clarity with respect to what these criteria would be, such as gross revenue, number of consumers/households/devices handled, percentage of revenues earned from consumer information etc. In an attempt to further harmonise the NPD framework with the PDP Bill, the Revised Report also recommends that the criteria suggested in the PDP Bill in relation to registration of Significant Data Fiduciaries be linked to those for Data Businesses.

6 Establishing rights over NPD

The Revised Report states that NPD is not associated with a specific Data Principal and therefore any group of people bound by common interests and purposes (Community) can exercise the right to derive value and eliminate harms from the NPD through Data Trustees (explained below), and raise complaints in relation to the harms arising from the sharing of NPD relating to their Community. The Revised Report emphasizes that the benefits arising from the NPD should not be limited to the entities collecting and processing such NPD (Data Custodians). Therefore, Data Custodians have a duty of care towards a Community with respect to handling NPD associated with such a Community and an obligation to share NPD when requests are made for the specified purposes (discussed in Section 7 below).

The Revised Report has identified other legislations that adopt a similar construct to throw some light on the contours of a Community. While this offers some explanation, given the inherently distinct nature of NPD it might be difficult to directly translate those principles within the NPD framework. Therefore, a certain level of ambiguity remains. However, the extent of the impact of this broad definition is more limited than under the Initial Report, given that the only effective right that is directly exercisable by the Community is the right to complain. Although Data Custodians may also face some uncertainty in determining the Community(ies) towards which they should extend a duty of care.

7 Data sharing

The Revised Report refers to data sharing as the 'provision of controlled access to NPD for specified purposes and with appropriate safeguards'. Although this definition does not depart from the Initial Report, the Committee has taken a different approach in relation to the circumstances under which NPD must be shared by refraining from offering recommendations on data sharing for sovereign purposes with the government and business purposes *inter se* private companies.

Data Businesses are required to make all meta-data with respect to the NPD they collect available for open access through a directory managed by the NPDA. Organizations registered in India will have open access to this directory, and Data Trustees may refer to the meta-data to make requests for relevant sub-sets of data to create certain data sets for public good called High Value Datasets (HVDs).

7.1 High Value Datasets

HVDs are understood to be datasets that are beneficial to the community at large and useful for various purposes such as policy making, job creation, financial inclusion and innovation. Data Trustees are responsible

for the creation, maintenance and sharing of HVDs. However, the Revised Report states that any group of individuals can constitute a Data Trustee, which leaves room for uncertainty. It permits the creation of several bodies that can demand valuable data from Data Custodians. Various HVDs are to be identified and created by Data Trustees on an ongoing basis. Each HVD will have one Data Trustee, which could request NPD from every significant Data Custodian relevant to the identified HVD. The Revised Report recommends that there should be non-discriminatory access to data from the ecosystem. If a Data Custodian refuses to share NPD with the Data Trustee, a request may be raised with the NPDA. The Data Trustees are required to share HVDs with private and public entities in India for public good. The Revised Report permits Data Trustees to charge a nominal fee for this.

The Revised Report classifies NPD into three categories of granularity, namely: (i) raw data, (ii) aggregate data, and (iii) inferred data. Raw data refers to the basic factual/transactional data such as anonymised records of an individual's consumption pattern. Complete raw datasets may not be collected for the creation of HVDs, but specific subsets may be collected. Aggregate data is an aggregation of various data points but does not expose the underlying raw data. This may be collected for the creation of HVDs. Inferred data is derived insights developed through a combination of several data points. While this data may not be collected from private entities for the creation of HVDs, it may be collected from public organisations unless such dataset has an impact on national security. While the nature of NPD that needs to be provided for the creation of HVDs has been specified in this Revised Report, it adopts a somewhat similar stance to the Initial Report to the extent of mandating private entities to share certain data for public good purposes. This mandatory policy would constrain domestic players and disincentivize overseas players.

This construct of data sharing retains some of the issues identified in the Initial Report. The data sharing obligation has been applied uniformly to all Data Custodians, irrespective of their size, market share and other economic factors, which may disadvantage new entrants and small players, and stifle competition. The prejudicial impact of this measure is lesser as compared to the Initial Report given that the sharing is for HVDs. Further, Data Businesses typically collect a wide range of data in the course of their business and decisions made using this data, including what data is collected, are an important source of revenue. Requiring them to provide open access to this information is likely to defeat their competitive advantages.

The Revised Report identifies that data sharing, even when it is for public benefit, may give rise to certain issues such as infringing the trade secrets or proprietary information of companies, or violating the privacy of individuals or groups. However, it does not provide a concrete framework on how to overcome these other than to mention that some of these data sets would be outside the sharing obligations.

7.2 Sharing by Data Processors

Unlike the Initial Report, Data Processors are exempt from the data sharing obligations with respect to NPD processed by them for Data Custodians. This amendment provides much needed clarity.

7.3 Specificity of Data Requests

The Revised Report recommends that data requests should be specific and directed towards the defined purpose. This is a helpful clarification and would provide some relief to Data Custodians, but the NPD Legislation must issue detailed guidelines in this regard.

8 NPD Authority

The Committee recommends the creation of a specialised regulatory authority, the NPDA, to govern the NPD ecosystem. The NPDA's functions include the creation of a data sharing framework, maintenance of meta-data directory of Data Businesses, addressing issues in relation to privacy and misuse of data, and adjudication of disputes in relation to the creation of HVDs.

The Revised Report clarifies that the NPDA will be independent of other sectoral regulators such as the Data Protection Authority (DPA) and the Competition Commission of India (CCI) given the specialized area of its operation. While the Revised Report draws a distinction between the roles of these regulators, there is likely to be significant overlap in their functions.

9 Legal and Economic Analysis of the NPD Framework

The Revised Report analyzes the NPD governance framework from a legal perspective and concludes that there are no statutory protections for data under property law or competition law that may interfere with the sharing contemplated under the Revised Report (with limited exceptions). Further, the Revised Report identifies Articles 39(b) and (c) of the Constitution of India as the basis of enacting a law that mandates data sharing. Therefore, the Committee suggests that the mandatory data sharing provisions recommended in the Revised Report may be validly incorporated into the NPD Legislation.

The Committee also analyzes the NPD governance framework from an economic perspective and states that the Revised Report reduces the transaction costs for stakeholders by recommending sharing only in relation to HVDs. The Revised Report further suggests that the NPDA must take actions on an ongoing basis to ensure that domestic organizations with foreign control are not the only entities benefitting from the creation of NPD datasets, and to distinguish between active and accidental misuse of NPD although these two terms have not been explained. It appears that the NPDA will play a pro-active role to monitor the activities of all entities within the ecosystem.

10 Technology Architecture

The Revised Report retains the suggestions for technology architecture from the Initial Report and recommends that these may be used to ensure effective creation and sharing of HVDs. The guiding principles recommended by the Committee include (i) enabling access through APIs and sandboxes so that stakeholders can request and obtain data digitally and maintain a log, (ii) storing NPD in a distributed manner to avoid single point leakage, data corruption and data loss, (iii) making NPD available in a standardised and usable manner, and (iv) preventing deanonymization or reidentification of NPD. As discussed in our analysis of the Initial Report, stakeholders may need to restructure their existing data architecture to comply with the proposed guidelines.