Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees: CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.in: E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

14th January 2021

To

MyGov

New Delhi

Inputs on Draft Non Personal Data Governance Framework

Dear Sir

Foundation of Data Protection Professionals in India (FDPPI) is a Not for Profit company of the Data Protection Professionals in India, dedicated to the empowerment of the Data Protection community with Knowledge, Skill and the Right attitude.

Operating since 2018, FDPPI is credited with the India's Self Reliant Projects in Data Protection such as Certification programs for Data Protection professionals on par with or better than the global certification programs and Data Protection Management system named Personal Data Protection Standard of India, uniquely constructed for a Unified Compliance environment for multiple data protection regulations.

We are pleased to provide our inputs to the furtherance of the Non Personal Data Governance Framework as suggested by the expert Committee headed by Sri K Gopalakrishnan. This is the response to the revised Kris Gopalakrishna Committee report submitted on 16th December 2020.

We shall be happy to provide any further clarifications as and when necessary.

Thanking you

Yours Sincerely

Na. Vijayashankar (Naavi)
Chairman

Foundation of Data Protection Professionals in India
[Not for Profit, Section 8 Company limited by guarantees: CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK first Stage, Second Block, Bangalore 560050
Web: www.fdppi.in: E Mail fdppi@fdppi.in: Ph: 08026603490: Mob: +91 8310314516

Inputs on Non-Personal Data Governance Framework suggested by Sri K Gopalakrishnan Committee

Introduction

As "Personal Data" and "Non Personal Data" are the two faces of the same Coin, regulation of one will automatically reflect on the other. FDPPI believes that regulation of Personal Data from the point of view of protecting the Privacy of individuals is integrated with the unlocking the potential of the residual data for commercial purposes and national interests.

It may be noted that this expert committee was an outcome of the closing comments made by the Justice SriKrishna Committee when it finalized it's report on Personal data protection, when it raised the issue of "Community Data" outside the ambit of PDPB to be addressed separately.

Some of the suggestions made here may have immediate relevance since the Personal Data Protection Bill 2019 (PDPB 2019) is in the final stages of being presented to the Parliament and some of the discussions presented here could be relevant to providing clarity on some of the provisions of the PDPB 2019.

We hope the suggestions would be useful to the Government to frame necessary detailed regulations in multiple iterations.

Background Recommendations

The Kris Gopalakrishnan Committee (KGC) after the release of its draft report and studying the comments received has now come up with the revised report in which the committee has

a) Clarified the definition of personal data
b) Examined the legal basis for asserting the rights of India and its communities over Non Personal Data
c) Expanded the idea of High Value assets and the roles of data custodian, data trustee etc.
d) Consent for anonymization of personal data
e) Clarified data sharing recommendations for public good.

We would like to place our recommendations on each of these points.

Definition of Non Personal Data (NPD)

The definition of non personal data was clear even in the earlier version and would continue to be of two types namely,

a) Data which was never personal. This includes data which is outside the definition of "personal Data" as per the definition in Personal Data protection Bill 2019 (PDPB 2019).
b) Data which was once a "Personal Data" and has been subsequently "Anonymized" by removing of the personally identifiable elements.

The distinction between Personal and Non personal data and the jurisdiction of PDPB 2019 and NPD regulation would depend on whether the subject data is "Personal" or not.

To the extent "Personal Data" relates to data identifiable to a natural person, the corporate data falls within the definition of NPD. There are certain issues regarding personal information of deceased persons and business related data where the name of an individual or a proprietor is integral to the name of a company or an internet domain or an e-mail entity.

These are issues that fall within the jurisdiction of PDPB 2019. The NPD regulation should avoid the temptation of poking its nose in the Personal Data regulation and has to accept the "Residual Definition" of what constitutes Non Personal data emanating from the PDPB 2019 and any interpretations coming from the Personal Data Protection Authority whenever a reference is made to them.

The recommendation under Para 5.3 suggesting the deletion of Section 2(B) of PDPB 2019 as infructuous is not fully correct. While there will be no need for Section 91 after the Non personal data regulation Act may come into being, in the interim period until such a regulation becomes operative, the current provisions in Section 91 and Section 2(B) of PDPB 2019 may be retained.

Consent for Anonymization

If it is accepted that the distinction between "Personal data" and "Anonymized erstwhile personal data" is determined on the basis of the system of "Anonymization" which is as per the standard of irreversibility recommended by the Personal Data Protection Authority of India, then there is no legal uncertainty between what data comes under PDPB 2019 and what comes under NPD regulations.

The discussion on whether the "Erstwhile personal data now anonymized" can be "Re-identified" depends on how strong or weak is the "Irreversibility" standard defined by the personal data regulations. The re-identification may be accidental or deliberate. If it is accidental, then the irreversibility standard could be considered weak or that the anonymizer who is a data fiduciary under the PDPB 2019 has not carried out the anonymization as required under the standard and it remains in a "De-identified" status.

De-Identification or Pseudonymization is an intermediary status between "Identifiable personal data" and "Erstwhile personal data now anonymized" and belongs to the Personal data regulatory regime.

Technically it is possible to consider "De-identification" as well as "Anonymization" as "Processing" of personal data and "Consent" can be required for the Data Fiduciary to anonymize the personal data.

However, the moment personal data is anonymized, it goes out of the jurisdiction of Personal Data Regulation and hence any disclosure or use of Anonymized data becomes feasible under the NPD Governance.

The Non Personal Data Governance law has no jurisdiction on the processing of personal data and hence it would be the prerogative of the PDPB 2019 to include "Anonymization" as part of the definition of processing.

In the event Anonymized data being re-identified, then it should be possible only by way of application of an "Intention to re-identify" which is a fraudulent intention, and it would be covered as an "offence" under PDPB 2019. Even and "Unsuccessful Attempt" can be made punishable on the basis of the "Malicious intention".

The Non personal data regulation may therefore leave it as a suggestion for the PDPB 2019 to include the "Consent for Anonymization". The committee goes onto recommend that an "Opt out" mechanism should also be provided by the PDPB 2019 for anonymization.

This suggestion must be considered as ultra-vires the Kris Gopalakrishna Committee to have added this recommendation.

It is our considered opinion that "Anonymization as per the standard set by the personal Data Protection should be considered as "Legitimate Interest" of the Data Fiduciary representing the "Right to carry on business of choice" which is also a fundamental right guaranteed by the constitution.

Hence if PDPB 2019 recognizes "Anonymisation" as part of "Processing" and "Anonymization as per standard set by the regulator" as "Legitimate Interest" of the data fiduciary, then the concern expressed by the Kris Gopalkrishna committee would have been more than addressed.

The Non Personal Data regulation should therefore keep itself clear from either defining the term "Anonymization" or prescribing "Opt-out" for anonymization.

Definition of Data Business

Data Business is sought to be defined as any organization that collects and **manages both personal and non-personal data.**

Since managers of Personal data are already classified as Data Fiduciaries, Data Processors, Consent Managers and Social Media Intermediaries, as per the Personal Data Protection regulation, there is no need to interfere with the managers of Personal data. "Personal Data Business" is therefore in the realm of PDPB 2019.

NPD regulation can restrict itself to defining "Data Business" as a business that manages "Non Personal Data" or simply "Non Personal Data Business".

Just as the Committee suggests that PDPB 2019 need not speak about Non Personal Data under Section 91,

Non Personal Data regulation need not make reference to Data Business related to Data Fiduciaries covered under the PDPB 2019.

Definition of Roles

The Committee suggests that Rights over Non Personal Data may be recognized to a "Community". This is however is a challenge since a "Community is an aggregation of individuals" and the "Community Data" when profiled may involve harm to individuals.

Hence Community data also has to be anonymized before it is treated as "Non personal data". In other words the identity of the community. Alternatively the standard of "Anonymization" to be published by the Personal Data Protection Authority of India, may include Anonymization standard of Personal data and Anonymization standard for Community data separately.

The committee has defined three roles namely the Data Custodian, Data Processor and the Data Trustee.

The person who collects Non personal data will be the Data Custodian. The person who processes the NPD will be the Data Processor.

The Committee has also identified another entity called "Data Trustee" as an organization that is responsible for the creation, maintenance, data sharing of High Value data (HVD) sets in India. The HVD itself is defined as a category of NPD as an aggregated data set which is beneficial to the community at large and shared as a public good.

Instead of discussing HVD under the roles, it should be discussed under the definition of NPD and classified as a special category of NPD. This is more like defining the "Sensitive personal information".

The concept of Data Trustee can be also considered as a "Specialized Data Processor" more like the "Significant Data Fiduciary" in the Personal Data Protection regulation.

It is preferable to reduce the clutter and merge the Data Trustee role to a Specialized Non Personal Data Processor role. Also, to avoid confusion with the Data Processor role in the Personal Data Protection regime, the Data Processor may be called by a different name such as "Non personal data Value aggregator".

The Grey Area

The main objective of the law is to enable unlocking of the value of Non Personal Data. This requires a mechanism for discovering a value system for data and getting visibility for the data vale held by an organization. While the market may discover value after trading, in the production stage itself there is a need for the organization to recognize a value for the NPD asset.

Currently the Committee has not addressed this requirement. In the Personal Data scenario, FDPPI has been suggesting accountants to evolve a method of bringing the value of personal Data Assets and Non Personal Data Assets into the Books of account by

developing an appropriate method of valuation which could be a combination of replacement cost, market value, acquisition cost etc. In the interim period before the Accounting standards are developed, it has been suggested that organizations need to bring the data assets into the balance sheet at a notional value as a "Contra Entry" without bloating the real distributable value of Assets.

Summary

The recommendations of the committee are to be considered as the preliminary framework for development of the law. The report appears to have combined certain aspects which have to go into the law and certain aspects that have to go into the regulations to be framed under the law. If these are separated, the law will look simpler and the regulatory framework will have the flexibility that is essential for creating a formal framework for NPD Governance.

If all aspects are hard coded into the law which will be the first such law in the world, it is likely to create problems when changes may be required.

It is therefore suggested that a simple framework of law is adopted first and after the regulations are implemented, based on the experience over a period of at least one or two years, the law can be expanded.

The simple law needs to define the NPD and HVD, Define the roles of the Custodian and Data Processor as well as the HVD Data Processor, create the mechanism for valuation of the NPD, Create the concept of data exchanges as another category of a data processor and let the market discover the value of non personal data.

The law has to set up the regulatory authority which should frame the rules and regulations that should be tested in the market place.

The regulatory authority may work with organizations like ICAI and FDPPI in developing a system of valuation of personal and non personal data and bringing it to the books of account.

Once the law and the regulations mature with the experience in the market for about 2 years, it may be reviewed.

Naavi

14th January 2021