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

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 pioneering of 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.

We believe that after the passage of the Personal Data Protection Bill we need to address the issue of Sovereign Rights over residual Non-Personal Data so that big commercial entities donot shut out smaller organizations from using the value of Data as well as enable Government to ensure that national interests are protected. These are addressed by this Non-Personal Data Governance Framework and we hope our thoughts in this regard would be found useful.

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, FDPPI's interest in "Personal Data Protection" is closely related to the "Governance of Non Personal Data .

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 and hence submits its reasoned comments on the report submitted by the Expert Committee headed by Mr Kris Gopalakrishnan.

It is understood that the report of the Committee is the initial recommendation for the Government to formulate further policies and drafting of regulations as it may deem fit. At this stage, the recommendations are considered flexible and amenable for improvement. Hence FDPPI is expressing only "Positive Suggestions".

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 finalized by 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 their study recognized the following requirements

i. Create a modern framework for creation of economic value from use of Data .
ii. Create certainty and incentives for innovation and new products / services creation in India..
iii. Create a data sharing framework such that community data is available for social

/public / economic value creation.

iv. Address privacy concerns, including 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.

Keeping these objectives in mind the following Six recommendations were made.

1. Committee identified 3 kinds of Non Personal Data (NPD), namely Public NPD, Private NPD and Community NPD.
2. Committee identified four different roles in the eco system namely, Data Principal, Data Custodian, Data Trustees and Data Trusts.
3. Committee articulated a legal basis for establishing the rights over the three kinds of NPD
4. Committee defined a new category of business called Data Business as a horizontal classification cutting across different industry sectors.
5. Committee identified three a data sharing purposes namely Sovereign Purpose, Core Public Interest Purpose and Economic Purpose.
6. Committee defined data sharing mechanisms and checks and balances.

Additionally, in order to implement the suggestions, the committee suggested a separate regulatory authority.

After considering the above, we have presented our comments under the following six sub heads.

1. Importance of Data as an Asset and the need to harness its hidden value
2. Definition of Non-Personal Data
3. Stakeholders and Key roles of participants
4. Concept of Data Business
5. Data Sharing mechanism
6. Regulatory Authority.

Importance of Data as an Asset and the need to harness its hidden value

"Data" is a unique commodity. In simple terms, "Data" is an organized collection of information from our observations of the surrounding events.

So far the world has been seeing "Data" in the perspective of how its mis handling could result in Cyber Crimes and Loss of "Privacy". Hence there have been regulations on "Cyber Crimes" and on "Data Protection".

In India Information Technology Act 2000 (ITA 2000) defines "Data". It provided Legal enablement of data use in Commercial and Governance including the authentication systems.

However, the Act was otherwise mainly meant for prescribing the consequence of misuse of data (both personal and non-personal). It was not meant for suggesting how the data can be harnessed for the benefit of the society.

When the Personal Data Protection Act was conceived, it expanded the Section 43A of the ITA 2000 into a comprehensive compliance framework but focussed on extracting "Personal Data" from out of "All Data" which ITA 2000 addressed and prescribed how "Personal Data" has to be secured.

As a result there was no attempt to harness the value out of "Non Personal Data" which was out of contention of the Personal Data Protection as well as the ITA 2000. This was considered a digital waste which today lies in the system as unused but resource guzzling data dump.

Some of the big organizations such as Microsoft, Google, Amazon and some other companies however realised the potential of this "Discarded Non Personal Data" and have made a big business out of it. Additionally they are also resisting the "Personal Data Protection Act" and trying to retain their hold on personal data also.

In this game of harnessing of data, smaller companies donot have any opportunity to lay their hands on the "Non Personal Data Dump" even if they have opportunities to use it innovatively. Even that part of the data which the Government generates goes into the hands of the large private sector and no value is realized by the Government for itself or for public benefit.

The KGC has therefore correctly identified that "Data Interalia contributes to economic wealth… Organizations have been discovering ways to generate value from data.

The premise on which the Committee has submitted its recommendation is that the hidden value of Data must be unlocked and this is a sound principle and needs to be nurtured.

It is to be expected that vested business interests who presently have a dominant use of the Non Personal Data would vehemently oppose the Government taking control of the Non

Personal data being discharged by the users into the open data space since they would like to retain the sole ability exploit this resource.

The Government should ignore such opposition and keep the larger interests of the society in framing regulations to

1. Unlock the benefits of the Non Personal Data that gets generated in the society
2. Enable fair distribution of this Non Personal Data among the different sections of the society

The KGC committee tries to achieve both these objectives by different means such as

1. Defining what is Non-Personal Data which is outside the regulation of Personal Data Protection for the purpose of Privacy Protection.
2. Setting up a "Data Exchange" mechanism for fair value realization by generators of Non-Personal Data in the society which may include individuals, Community, Private sector and the Government

The KGC has provided some of its recommendations on how to go about these objectives and the purpose of this submission is to assist the Government in identifying if there are any better ways of achieving the objectives.

In order to counter the narrative that will surface in the public comments of vested business interests, about what all is wrong with the report, it is considered necessary to also reinforce the suggestions which are in the right direction.

With this view, the following recommendations are submitted.

Definition of Non-Personal Data

The Committee has defined Four categories of Non Personal Data (NPD) namely

1. Public Non-Personal Data
2. Community Non-Personal Data
3. Private Non-Personal Data
4. Sensitive Non personal Data

Out of the above the three categories namely Public NPD, Community NPD and Private NPD are based on who generates the data.

The Fourth category refers to the nature of the data and its likely relation to national security and strategic interests, business sensitivity or confidentiality and risk of de anonymisation. This category can be recognized across all the other three source based categories of Pubic, Community and Private.

While the broad recognition of the different sources from which NPD gets generated and the need to provide rights based on the efforts involved in generating NPD, the definition of Sensitive personal data looks slightly out of place.

We therefore recommend the following:

Recommendation 1: Identifying Sensitive NPD is necessary for excluding it from disclosure requirements.

The objective of the NPD regulation is to unlock the benefits of NPD without adversely affecting the Privacy or Security Rights of the citizens of the country. The definition of "Sensitive NPD" has to therefore continue to serve this objective.

Once "Data" is segregated into "Personally Identifiable" and "Non-Personal Data", the regulation of "Sensitive Personally identifiable information" is covered under the Personal data protection Act. This is not available for harnessing of value under the NPD regulation.

The definition of Sensitive NPD is therefore only concerned with ensuring that NPD which is sensitive does not fall into wrong hands and jeopardise national security or the Intellectual property rights of the private sector, so that it can be kept out of the Data Disclosure mechanisms suggested later in the recommendations.

It is therefore not necessary to define Sensitive NPD as an extension of Sensitive Personal Data. The only criteria to define Sensitivity of NPD should be based on National Security (including Economic Security) and Law Enforcement Considerations, besides the Protection of Intellectual Property.

Recommendation 2: No Need to Discuss consent for Anonymisation

Firstly we consider that "Possible de-anonymisation" means that "Anonymisation" in the first place was not done properly.

Anonymisation refers to "Data which was once a personally identifiable data rendered irreversibly not identifiable through a process of anonymisation".

Un-anonymised personal data is nothing different from "De-identified" or "Pseudonymized personal data" and remains within the jurisdiction of the Personal Data Protection regulation.

The Personal Data Protection Authority (DPA-PD) will take care of defining the "Standard of Irreversibility" which could render a set of data as "Non-Personal" under PDPA.

If this "Irreversible standard" is inadequate or through the passage of time and development, the standard becomes "Breakable", then the standard should evolve to higher levels to keep pace with the developments.

Just as the Controller of Certifying Authorities under ITA 2000, started with hashing standards of MD5 and SHA 1 in 2000 and later degraded MD5 and added SHA 2 , it is the responsibility of the authority to continually evolve the standards to higher levels.

Over and above the reasonable standards fixed by a regulatory authority, if there are technologists who try to break them, it would be like the ethical hackers trying to identify security vulnerabilities. There should be some regulation for controlling the activities of such security professionals so that they remain within the boundaries of legal activities.

PDPA already defines an "Offence" which involves "Re-identification" of "De-Identified Information". This will apply to "De-Anonymisation" as well since the very fact that some data declared as "Anonymized" is "De-anonymisable", renders the first classification as "Anonymised" incorrect and reverts it back to "De-Identified".

Hence "De-Anonymisation Risk" identified by KGC is already covered under the criminal provision under PDPA.

Whether there should be "Consent" for anonymization and further disclosure of "Anonymised Information" is a subject matter of PDPA and can be considered outside the provisions of this Act. If "Unlocking the economic value" of data is the objective, we need to consider "Anonymization of Personal Data" as a "Legitimate Interest" under the Personal Data Protection Act and the Non Personal Data Regulation need not interfere with this by prescribing "Consent for Anonymisation".

The definition of "Anonymised Personal Information" should therefore be adopted as defined in the PDPA just as the definition of data is adopted from ITA 2000. No mention of "Consent" for "Anonymization" need to be included in this Act.

Recommendation 3: Personal NPD

Since data identifiable to an individual remains a "Personal Data", conceptually there is no "Personal Non-Personal Data". The moment we recognize that any data is attributed to an individual, it becomes personal data whether it is sensitive personal data like health or financial data or other non sensitive data.

The personal data becomes Non personal data through a system of Anonymisation which can be done by a person other than the data principal only. PDPA recognizes that the Data Fiduciary may be able to anonymise and as long as it is an irreversible process, it takes the personal information out of the purview of the PDPA and renders it being capable of commercial exploitation or public use through disclosures that donot affect the privacy right of the underlying natural person/s.

Since Personal NPD requires anonymisation by the Data Fiduciary's efforts, it may be considered as "Private NPD" of the Data Fiduciary if the Data Fiduciary is a private body or "Public NPD" if the Data Fiduciary is a public body.

This is not different from either a private body or a public body investing in collection and generation of NPD.

Recommendation 4: Community NPD

While there is no "Personal NPD" in concept and "Anonymized Personal Data" automatically becomes either Private NPD or Public NPD, there is an intermediary category of NPD which is an aggregated personal data of a group of persons rendered unidentifiable by a process of anonymisation of the aggregated data.

KGC has tried to recognize this as the "Community Data" and envisaged that the "Group" having some common interests will appoint a "Data Custodian" to harness the benefits of the Non-Personal data contributed by the underlying identifiable natural persons.

This "Custodian" may collect some group data directly from individuals with a permission to use it in anonymised form for the benefit of the community of which the individual may have a share. This activity will not be different from the role of a "Consent Manager" under PDPA who is a "Data Fiduciary" as well under PDPA.

The custodian may also collect some other community data without the individual passing it on to them. This is similar to the private company putting its efforts to collect data and benefit by unlocking the commercial potential of the data. In this instance, the "Community" is nothing but a "Private Entity" like a "Society or Association of People".

If we define that a "Private" entity under this regulation to include other juridical persons such as the "Association of persons", then the "Community Non Personal Data" will get subsumed by the "Private NPD".

Additionally, "Community Data" which consists of "personally identifiable parameters" which identifies the contributors of the data individually, becomes an aggregation of personal data and should ideally be coming under the PDPA as "Shared Personal Data" or "Joint Personal Data".

It has therefore been recommended by us that the PDPA should incorporate a definition for "Joint Personal Data" and "Joint Data Principal".

In case PDPA incorporates this definition, then there is no need for the NPD regulation considering "Community Non Personal data" as a different category and it gets merged with "Private NPD".

This would mean that there would be only two categories of Non-Personal Data namely the Private and the Public.

To summarize our recommendations on the Classification of NPD we can state as follows:

1. PDPA must include a definition of "Joint Personal data" and "Joint Data Principal" so that PDPA extends its boundaries from "Single Natural Persons" to a "Group of Natural Persons" in terms of "Individually identifiable data".
2. PDPA already includes the definition of "Anonymisation", the standard of anonymization as part of the regulations to be made by DPA (under PDPA). PDPA besides imposing penalties for inefficient anonymisation also provides for criminal punishments for de-anonymisation. The recommendations of KGC regarding the technology of Anonymisation given in the schedules belong to the DPA regulations under PDPA and not under NPD regulations which start after the "Anonymisation" process.
3. In the event PDPA incorporates the definition of "Joint Personal Data" then NPD regulation may include only two categories of stake holders namely the "Private" and "Public". The Private NPD is attributed to NPD generated by any non-Government body including groups of individuals whether organized as a society, association of persons, Proprietary concern, partnership, LLC etc. (Globally there is a difference of opinion on whether Proprietary information is personal information but since proprietary information is considered as arising out of business purpose, it is ideally considered as not belonging to the category of personal information)
4. In case PDPA fails to incorporate the definition of Joint Personal Data, then we may retain the definition of "Community Data" as "NPD whose beneficial rights are recognized to a group of individuals"

Recommendation 5: Key Roles under NPD Regulation

The KGC has defined four key roles in Non Personal Data Eco System namely

1) Data Principal
2) Data Custodian
3) Data Trustees
4) Data Trusts

As has been discussed in the previous paragraphs, Non-Personal Data relates to "Data that cannot be identified to an individual Data Principal as defined under PDPA".

We have recommended that by extending the definition of applicability of PDPA to "Identifiable joint Personal Data", the Non Personal Data is completely insulated from any identity parameters and either deals with non-personal data per-se like the weather data, trade data etc or anonymized personal data both in individualistic form or in the form of aggregated community data form.

We also recommend that the terminology used in NPD regulations should not clash with terminology used in PDPA so that confusions arising out of mixing up of definitions can be avoided.

Hence the term “Data Principal” should be avoided in the NPD regulation and retained only in the context of PDPA where we are dealing with identifiable personal information.

Under NPD regulation we are looking at harnessing the value of NPD and hence it is appropriate to recognize that there are “Beneficial Owners” of the value in the form of “Private Companies” and “Public Authorities”. “Community” is a “Joint owner” of individual rights and is represented by an “Association of Persons or a Society”.

Other than the “Beneficial Owners” there would be “Intermediaries” who are specialized in processing of NPD, creating and managing value for the NPD and managing a platform for exchange of value.

We therefore recommend the following roles to be defined.

Category A: Ownership basis

1. NPD Community Body (NPD-CB)
2. NPD Private Body (NPD-PB)
3. NPD Government Body (NPD-GB)

In each of the categories “Indian” and “Non-Indian” can be created as sub categories

Category B: Intermediaries

1. Data Custodian
2. Data Repository
3. Data Exchange
4. Data Agents

The recommended definitions of these categories are as follows:

NPDCB: (Community Body)

“NPD-CB” is a body that represents owners of anonymized personal data belonging to a group of individuals.

The NPD-CB is created by the individuals and hence it will collect data in identifiable form for a specific purpose of formation of the organization. Once formed, it will handle only anonymized information. Since its role in handling personal information is restricted only to the extent of formation it is constituted either as a society or a company or in any other legally recognized form which can own and deal with any kind of asset including Data as an asset. The personal data of the members or share holders will be handled by the organization as required under the respective law such as the Companies Act or the Societies Act or a Trust Act. The handling of personal data at this stage is governed by PDP regulations read along with other applicable laws to that organization.

Where the community body hands over the output data in anonymized form to another entity, the beneficial ownership passes on. This is the Data Exchange activity.

The entity that receives the identifiable data and converts it into anonymized data is a "Data Fiduciary" under PDPA and will be regulated by the DPA-PD. It may restrict itself to the task of "Anonymization" and may be called "Anonymization Gateway Manager".

If this organization extends its services to representing the rights of the data principals under PDPA, it will become a "Consent Manager" as defined under PDPA.

Both the Anonymization Gateway Manager and the Consent manager are roles which come under the Personal Data Protection regulation and not NPD regulation.

Anonymization facilitates the further disclosure and hence adds some value to the information which otherwise would have gone waste, but considering that the role is limited to being a bridge between PDP Regulation and NPD Regulation, it should be recognized as a separate role not extending to further harnessing of the value which will be the responsibility of the NPD Society or the Private or Government bodies.

Since "Standard of Anonymization" comes within the purview of the PDP regulation, the Anonymization gateway manager would be regulated under the PDP regulations as a "Data Fiduciary".

NPDCB is the recipient of the output of anonymized aggregated data from the "Anonymization Gateway Manager" and should be regulated under NPD Regulations.

The NPDCB will be engaging the services of the Anonymization gateway manager to convert the identifiable personal data to anonymized form and giving it back to the NPCDB for further use such as harnessing its value through a Data Exchange.

It should be clarified that NPCDB shall not handle identifiable personal data and hence is not a Data Fiduciary under the PDP regulation in respect of identifiable personal data collected other than the membership data collection and disclosure of which is regulated under the respective constitution related acts such as the Society act, trust act or companies act.

If all the community members are Indian Citizens or Residents, it may be considered an Indian Community. If all of them are foreign citizens or residents it may be considered as a Foreign Community. If it is a mixed community of Indians and foreign citizens or residents, it may be considered as a "hybrid community". To simplify the sub categorization, the classification may adopt a 50% controlling stake to determine the applicability of the regulation and consider measures to address the interest of minority stake holders separately.

NPD-PB (Private Body)

NPD-PB means an organization that collects NPD either by generating NPD through its own efforts or buying it from others NPD generators through a Data Exchange or a Private purchase.

The essential difference between NPDPB and NPDCB is that NPDCB represents individuals who all have an equal stake in the operations of the NPDCB as members of an association of

persons constituted as Society or Trust owned only by the members who contribute their personal data to the kitty for anonymization and further use as NPD.

NPDPB on the other hand is constituted as a private body which may collect NPD from any Community or on its own and use its capabilities to add and harness value. It could be constituted as a Society or Trust or Proprietary concern, Partnership form or limited company etc.

The organization may be considered Indian, Foreign or Hybrid based on criteria similar to the previous paragraph or otherwise already present in the Companies Act.

NPD-GB (Government Body)

NPD-GB means an organization that belongs to the Government. The Government can be Indian or foreign.

Intermediaries

The data is generated either by individuals, private companies or Government. Accordingly, the community body or the Private Company or the Government will have beneficial interest in the NPD.

The intermediaries provide different services such as “Storage”, “Representation of interest”, “Providing a value Exchange Platform” or “Other services” and accordingly they will assume the roles of a Data Repository, Data Custodian, Data Exchange and Data Agents.

Among the Intermediaries, there could be “Data Repositories” who simply provide data storage facilities to the NPD-CB or NPDPB or NPD-GB. Cloud operators could fall under this category.

Those who act in a representative capacity for individuals such as parents or guardians for minors or contractually appointed agents under Indian Contract Act to represent the interests of the individual or community body or private or government bodies would be the “Data Custodians”. (Similar to Consent Managers envisaged under the Personal Data Protection Bill 2019)

Data Repositories are like “Demat” operation and Data Custodians will be like Portfolio managers or Investment consultants in the investment domain.

Data Exchange may be a term that may be used for bodies which act like stock exchanges providing a platform for sale and purchase of NPD. They enrol NPD owners and allow them to put up the data in different packages and sell on the exchange. The Exchange would help discover the buyers. The Data Repositories/Custodians may come up with different services to help the data owners package and re-package data to create value propositions. Buyers may scout the catalogue, bid for the data and take ownership for further use.

Data Agents may be a term for any other residual category of intermediaries who cannot be classified as Data Custodians or Data Repositories or Data Exchanges. It may include all other consultants who may work in the area.

Appropriate registration criteria and infrastructure need to be created.

In summary we are recommending changing the terms used for defining the key roles and instead of the 4 categories (Data Principal, Data Custodian, Data Trustee, Data Trust), we are recommending the recognition of

1.NPD Community Body

2. NPD Private Body

3. NPD Government Body

4.Data Custodian

5.Data Repository

6.Data Exchange

7.Data Agents

Recommendation 6: Concept of Data Business

KGC has recommended carving out of a "Data Business" as a "Discovery" if an organization is processing a threshold level of processing of NPD.

This discovery will require appropriate technology to identify the level of processing of NPD by an organization and identify the point where it crosses the limit where it may trigger registration formalities.

The monitoring of the Data Business discovery is also required since the KGC recommends recognition of the Government's right on "Sovereign Data" and also need to create "Open Data Access" besides a fair data exchange mechanism to enable smaller entities to have access to data for innovative use.

A lightweight fully digital mechanism is sought to be created for this purpose.

The Concept that any business which generates a particular level of data may be considered as "Data Business" is a concept that has many challenges.

The objective of this requirement being suggested is essentially to identify what is useful data in Non-Personal Data form that can be channelized for being harnessed into a value proposition.

In the case of personal data, there is a core element of "Identity" of a natural person and hence we can define the volume of personal data handled as data of a certain number of individuals and fix threshold levels for either exempting small entities or declaring certain data fiduciaries as Significant Data Fiduciaries or classifying Social media intermediaries.

However, in case of “Non-Personal Data”, it is difficult to have a “Core data element” which is common to all types of non-personal data and decide how much of NPD is being handled by the entity.

One organization may have a weather monitoring system which may record temperature, humidity etc every 15 minutes and collect a certain number such data sets over a period of say 1 month. Another organization may have a CCTV which collects gigabytes of data every day. Yet another organization may be a business entity that collects business trends in the form of surveys, aggregation of statistics from different sources etc.

When can the organization is said to cross the threshold level is therefore a difficult proposition.

Once a criterial is determined, having an API to capture the designated data and identify the reaching of the threshold level etc is a matter of technical enablement that is not difficult.

But measuring the “Raw Data” as it flows into an organization and its conversion into some value added form of NPD before it becomes eligible for being classified as Sovereign data is difficult unless we are able to define the “Raw Data” as it applies in the context of NPD regulation.

Raw NPD need to be defined on inflow basis and outflow basis and if either of the two or together they exceed a threshold then the Data business criteria may be applied.

This measurement can be done on the basis of the byte size “Incoming+outgoing”. This is similar to the banking system where we define the business as Deposits plus loans.

Presuming that incoming and outgoing data includes both personal and non-personal data, while the regulation is limited to NPD, the criteria for defining Data business has to be based at “Raw Level” as including both personal and non-personal data.

However like providing “Input credit” in GST, the organization can be given a “Personal Data Credit” and if it can identify that the total input and output data as measured at the gross level includes a certain data quantity attributable to personal data sets, that can be provided as a “Personal Data Credit” to be deducted to arrive at the threshold level at which the organization becomes a “Data Business” and is subject to the new regulations.

Recommendation 7: Data Sharing mechanism

Having resolved the dilemma of when a business becomes a “Data Business”, the sharing mechanism is dependent on the requirements such as “Data Sovereignty”, “Data as a National resource”, “Need for the Community to benefit” etc. At the same time the need to respect

the “Intellectual Property Rights” and balancing the “Competition Act” requirements also need to be taken into account.

At present KGC recommends that the Regulatory authority will determine what data is to be mandatorily shared, what may be needed to be shared on voluntary basis, whether the sharing will be without any remuneration or with remuneration, and how the remuneration or price would be determined etc.

These are matters of detail may be handled when the Bill is drafted. What is to be discussed now is whether in principle, the suggested scheme is acceptable.

The KGC has defined three purposes for establishing the Data Sharing principle namely

1. Sovereign Interests for national security and legal purposes
2. Community benefits in public interest, research, innovation, efficient delivery of public services etc
3. Economic reasons which includes encouraging competition, providing a level playing field, preventing monopolistic hoarding of data resources etc.

All these purposes are necessary and cannot be disputed. Objections can however arise on how the mechanism would work, whether there would be a fair handling of the data assets for which a private company could have invested money and efforts to develop etc.

These are problems and issues already under management in the IPR laws in the form of compulsory licensing and Competition Act in the form of creating a level playing field.

In principle the objectives given above are considered acceptable and we can move ahead and discuss the actual modalities when an appropriate mechanism is introduced either in the Bill or in the regulations that may follow.

Recommendation 8: Regulatory Authority.

KGC has proposed that a new regulatory authority is to be set up for regulating NPD and it will function independent of DPA (PD) envisaged under PDPA.

This is the correct approach and this should be further developed in the Bill to be drafted to identify the specific responsibilities of the regulatory authority, its constitution etc.

It is clear that this Non-Personal Data Protection Authority will work closely with the DPA (PD) and CCI and several other regulators.

Summary

FDPPI therefore considers that the KGC report on regulation of NPD is in the right direction and it has to be further converted into an actionable regulation.

We have recommend certain changes in the PDPB 2019 which is still to be passed so that a clear distinction is drawn between the jurisdiction of PDP and NPD regulations. These suggestions have already been placed before the JPC for PDPB and hopefully they would be considered favourably.

We recommend that identification of “Sensitive NPD” is necessary but is not to be linked to “Sensitive Personal Data being anonymized”.

We recommend that there is no need to discuss “Consent for Anonymization” as it is in the domain of Personal Data Protection Act. Anonymization should be considered as a legitimate interest of the Personal Data Fiduciary under the Personal Data Protection Act and reason for a Private or Public NPD to be recognized.

With some changes suggested for introduction of Joint personal data under Personal Data Protection Act, only two categories of NPDs, namely Private and Government or Public would be required. Community data will be subsumed by the private NPD ownership with the creation of NPD society.

The key roles will include both ownership and intermediary requirements and will consist of 7 categories such as NPD Community Body, Private Body and Government Body, Data Custodian, Repository, Data Exchange and Data Agents.

Concept of Data Business is sound but a criterion for defining how to measure the threshold has to be defined and we recommend the total data size of incoming and outgoing data could be the criteria, with credits being given for Personal Data inclusion both in the incoming and outgoing data stream.

For the purpose of data sharing the suggested criteria such as sovereign interests, community benefit interests are necessary along with the IPR protection and Competition Act requirements.

The detailed machinery for implementing the suggestions can be undertaken at the next stage when a draft Bill may have to be drafted.

Naavi

11th September 2020