Foundation of Data Protection Professionals in India

[Section 8 Company limited by Guarantees]
[CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK First Stage, Second Block, Bangalore 560050
E mail: fdppi@fdppi.in: Ph: 08026603490: Mob:+91 8310314516

Date: 10th October 2018

To

The Joint Secretary
Ministry of Electronics and Information Technology
Room No 4016, Electronics Niketan
6 CGO Complex, CGO Complex
Lodhi Road
New Delhi 110003

Sub: Comments on the Draft Personal Data Protection Bill

This has reference to the feedback sought from the General Public in respect of the Draft Data Protection Bill.

We are pleased to provide our considered feedback in this respect.

In putting together this feedback, we have taken into account the recent Judgement of the Supreme Court on the constitutionality of Aadhaar in which several opinions on the concept of "Privacy" were expressed and several recommendations for legal provisions were made by the Court.

We have also taken into consideration the recommendations specifically made on the Aadhaar Act by the Justice Srikrishna Committee which was not included in the draft PDPA 2018 bill because at that time the Supreme Court judgement was not available.

We have also taken into considerations the effect of Information Technology Act on the suggestions made by the Aadhaar Judgement which need to be implemented in PDA 2018.

We hope these suggestions would be useful. We will be happy to provide any further claritications on the thoughts expressed here.

Thanking You

For Foundation of Data Protection Professionals in India

(Sd)

Chairman
(Na.Vijayashankar)

Foundation of Data Protection Professionals in India
[Section 8 Company limited by Guarantees]
[CIN No: U72501KA2018NPL116325]
Registered Office: No 37, "Ujvala", 20th Main, BSK First Stage, Second Block, Bangalore 560050
E mail: fdppi@fdppi.in: Ph: 08026603490: Mob:+91 8310314516

Date: 10th October 2018

Comments on the Draft PDPA 2018

1. Definition of Informational Privacy

The Preamble to the draft of PDPA 2018 records the objective of the legislation as **"Protection of personal data as an essential facet of informational privacy"**.

The term "Informational Privacy" was also referred to in the Puttaswamy Judgement of the Supreme Court, declaring "Privacy is a Fundamental Right". In this judgement, it was acknowledged that "Privacy is a State of Mind" and it is difficult to define the contours. Hence protection of Privacy Right was limited to protection of "Informational Privacy".

The draft PDPA2018 under section 48 refers to "Processing of Information Manually" and exempts "Small Entities" from the major part of the provisions of this Act. (This reference is to "Information which is in paper form"). This implies that manual processing per-se is within the provisions of this Act.

Hence this Act may be deemed to the Privacy Protection Act in information in paper form also. However Privacy infringement in "Oral Form" may still be outside the provisions of this law if the "Oral" information is not in the form of an electronic document.

Whether PDPA 2018 be considered as a comprehensive Privacy Protection law for India or it will be a Data Protection Law. limited to protecting data related to protection of Privacy is to be determined by the detailed provisions.

There is no doubt that the focus of the law is on "Information in Electronic Form" and hence it is called "Personal Data Protection Act" and not "Personal Privacy Protection Act".

The legislative intent of the Act can be squarely identified as protection of Privacy through information in electronic form which the data principal can manage at his own discretion.

Keeping this perspective in mind, we need to add a definition of the term "Informational Privacy" within the Act so that the scope and limitations of the Act is properly defined.

We suggest that the following definition of "Informational Privacy" be added to the draft along with a modification of Section 1 as follows.

Section 1(3): The Act applies to "Informational Privacy" as defined under Section 3(43)

Consequently, Present Section 1(3) will become 1(4).

Section 3(43): Informational Privacy means,

-the ability of a natural person to independently determine and exercise his or her choice
-to experience a mental state of freedom without an intrusion by others
-by exercising control on how personal data is collected, shared, processed.

2. **The definition of "Personal Data"**

The definition of "Data" includes information processed by human beings which means it includes "Non Electronic form".

"Personal data" is defined as data about or relating to a natural person who is directly or indirectly identifiable, having regard to any characteristic, trait, attribute or any other feature of the identity of such natural person, or any combination of such features, or any combination of such features with any other information.

In the recent Aadhaar judgement, the majority opinion expressed an opinion that

" All matters pertaining to an individual do not qualify as being an inherent part of the right to privacy. Only those matters over which there would be a <u>reasonable expectation of privacy</u> is protected under Article 21" (page 546).

The current definition of "Personal data" which talks of "Indirectly identifiable" information as part of the Personal data is impractical since in the current generation of Artificial Intelligence, even very small in-consequential information can be used to arrive at some "Derived Information about the identity of the person".

A Very large part of information floating around is therefore "Identifiable to a natural person" and there is no information that maybe considered as "Not identifiable to a natural person". Even a "Corporate Information" that say Company's invoice of sale of a TV includes the personal information of the buyer. A mere name without any associated data can be used to easily extract additional information which are deeply personal. Even the name of the Company can lead to the names of the directors and their personal information. Hence we need to recognize and accept that the clause "Indirectly able to identify" makes every information "Personal Information".

It is therefore necessary that in PDPA 2018 a proper clarification on the scope of the definition should be provided.

E.g.: The definition of Personal data can be simplified by stating

3(29) Personal Data means, such data about a natural person which the person would reasonably expect to be held confidential.

This meets the Supreme Court Judgement on Aadhaar. The definition of **"Profiling"** given in the Act takes into account the rest of the present definition.

3. The terms "Anonymization" and "De-identification"

The terms Anonymization and De-identification require being suitably distinguished to avoid confusion between the two terms.

Currently in the Act, it appears that De-identification refers to the measures voluntarily taken by the data fiduciary to mask the identifiable aspects of personal data and "Anonymization" refers to the standards that the DPA (Data Protection Authority) may provide and make a data impossible to be re-identified.

Again, given the development of AI, it is impossible for the DPA to provide a standard for "Anonymization" that cannot be bypassed. The standards in Cyber Forensics indicate that even over writing of the data is a reversible process and hence there is no perfect standard of "Anonymization".

DPA would therefore not be able to find such a standard and even if it tries to arrive at a standard it would be only a compromise. It is therefore prudent not to make the definition of Anonymization it dependent on a DPA's notification in future.

Instead the current definition itself can be modified like

"Anonymization" in relation to personal data, means a process of transforming or converting personal data to a form which is reasonably considered irreversible in identifying the data principal subsequent to such a process.

It should be the responsibility of every Data Fiduciary to define a process of de-identification and Anonymization as he determines is suitable to his activity and register this process as a "Code of Practice" with the DPA when a registration is required.

The Data Fiduciaries there by commit themselves to the adequacy of the process in terms of this definition. DPA need to only monitor the adequacy as expressed as a "Uberrimae Fidei obligation" and strict adherence to the stated obligation.

This will be part of the self-regulating "Code" which data fiduciaries and data processors may develop and register with DPA.

If the implementation is at variance to the agreed registered self regulation, necessary penal action can be initiated by the DPA.

4. The definition of "Sensitive personal information"

Currently, the definition of Sensitive personal Information

a. Includes "sex life", "Sexual orientation". "transgender status", and "intersex status" which are all related to "Sexual status and preferences" of the data principal.

   It would be preferable to combine these four categories in to one single category of "Sexual Status and Preferences" and leave out the individual definitions to reduce complexities.

b. The inclusion of "Caste" and "Tribe" in the definition of Sensitive personal information when read with the current definition of "Personal Data" that includes "Any information which indirectly can identify the data principal" will render most of the Indian names as "Sensitive Personal Information" since the names of persons often includes a caste identifier. Eg: Rame Gowda, Ramesh Iyer etc.

   Hence all data fiduciaries collecting names will automatically become Data Fiduciaries processing sensitive personal information.

   Hence "Caste" and "Tribe" should be deleted from the list of sensitive personal information.

c. The word **passwords** in the list of sensitive personal information should be extended as "Password or any identifier used in lieu thereof" for identifying the credentials of a person to access data

5. The Applicability

Under Section 2 (1) (b), the Act is applicable to Indian Companies or other bodies registered under Indian law. In its current form, if an Indian Company is processing the personal data of a foreign citizen in respect of an activity outside India and operating abroad, it will still come under the provision of this Act including the Data Transfer restrictions.

But in such data, there may be no interest of an Indian Citizen for data breach and the processors will be working on the confidence of the data controllers under a contract.

It may not therefore be necessary for the Indian Privacy law to protect this data which is not of an Indian Citizen and has no relation to the activity of the natural person in India. On the other hand it creates a ground for opposing other provisions such as prevention of data transfer across the borders. (Data Localization)

The only reason that it comes into the domain of Indian law is because it is processed by an Indian Company.

Section 104 of the Act enables the Government by a notification to exclude processing of personal data by Indian Data Processors pursuant to any contract with any person outside India.

It is suggested that this provision should be part of the “Applicability” under Section 2 instead of being an optional enablement by notification.

Hence a suitable re-wording of section (2) may be considered.

One possibility is to re-define the section as follows:

The Act Applies to the following….

2(1)(b): processing,
-by the State, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law,
-of personal data collected, disclosed, shared within the territory of India and
- any other personal data not covered under a contractual agreement with another entity established outside India and is subject to the data protection law of another country but processed within the territory of India

6. Conflict with Foreign Laws

Data Protection Laws are today present in different Countries. Each such law tries to impose the views derived from the culture of that country and the security requirements of that country and also imposes extra-territorial jurisdiction.

Such laws create an overlapping of regulations and expose business entities to liabilities under multiple laws.

Section 2(1) (b) of draft PDPA 2018 recognizes the applicability of Indian law when a company incorporated under Indian law processes personal data even outside India. (If suggestions made here are not implemented)

It is possible that the intention was to include processing of the personal data of Indian Citizens in a foreign location as part of this regulation. But the current draft can be interpreted as applicable to any personal data processing whether it is of an Indian Citizen or not as long as the processor is an Indian Company.

In the earlier paragraph, we have suggested removal of this extra responsibility to protect the interests of foreign citizens for data processing that happens in their territory.

At the same time, it is necessary that the sovereignty of Indian law and the Indian Data Protection Authority needs to be preserved by establishing that Indian Companies are subject to the Indian Privacy Laws primarily and not to the foreign laws.

There cannot be a “Double Jeopardy” when a data breach occurs with two regulators going after the same company.

Further there are differences in Data Erasure provisions with other laws and there could be conflicts between Indian law and the International law imposed through a Contractual obligation to which Indian Companies are exposed to.

As per the Supreme Court judgement on Aadhaar, it can be implied that a "Fundamental Right cannot be abdicated by a person through a contractual obligation imposed on him". In most cases such contracts would be dotted line contracts as well and can be held unconscionable.

Hence an Indian Company when exposed to liabilities under a foreign data protection law through contracts they may sign, must be subjected to the limitations otherwise applicable under Indian law for Indian Citizens or Companies.

While there is no issue in an Indian Company adopting higher data protection standards if available in an International law or standard, when it comes to facing "Liabilities" and erosion of national wealth, Indian law cannot be superseded by a foreign law imposed through an indemnity clause or penalty clause in a contract.

In order to ensure that Indian Companies are not subjected to unfair harassment under international laws, it is necessary to assert in the applicability clause the supremacy of Indian law when there is a conflict.

We therefore suggest introduction of Section 2(4) as follows.

2(4) Not withstanding any contractual obligations entered into by any Indian Citizen or State, company, or body of persons incorporated or created under Indian law, no penalties shall be imposed on such entities, for reasons originating from data protection regulations/laws of other countries except

a) through a grievance process under this Act including Adjudication and consequential Appeals or

b) Mutual Agreements of Assistance between Indian Data Protection Authority with the Data Protection Authority of the foreign country, approved through a Parliament approved Gazette notification or

c) International treaties binding on the nation

7. Consent Based Processing:

In all data protection laws in the world, informed consent is the main criteria under which a private sector can process personal data. It is not possible to eliminate this requirement. As regards the "Sensitive" personal information, the basis for consent now is moving towards "Express Consent" which means that there has to be an "Online Authentication" to confirm consent if services are provided online.

The Aadhaar judgement has lent a body blow to the "Consent based processing of data" as a concept since in respect of "Aadhaar", Supreme Court does not favour a "Consent Contract" for enabling Aadhaar to be used for authentication.

However Supreme Court is agreeable if such authentication could happen with a proper legal process.

The Supreme Court judgement adds two problems to the use of Consent for personal data processing which needs to be addressed in the PDPA 2018.

The first Problem is that what holds good for the processing of Aadhaar information which is a “Sensitive Personal Data, may in principle be applied to any other Sensitive personal data by extension.

can therefore conclude that the Supreme Court is not in favour of a contract based consent for processing of Sensitive personal data since such a contract bypasses the fundamental right of a person.

If this view is accepted, then it is also possible to extend this undesirability of the use of Consent Contracts further to the Personal data.

If such a view is to be given effect to, then every use of personal data should be part of a law such as the PDPA 2018.

It is therefore necessary to ensure that the law itself define a method by which an integrated definition of different types of processing to which personal data may be subjected to by a data processor.

Given the multitude of ways that personal data may be used in data processing, it is not feasible to specify different types of permitted processing in law except in some generic terms.

The use of data is specific to the processing situation and hence if there is any law, it should incorporate flexibility to accommodate different types of processing in different situations.

Such law should also provide for new uses of data to be discovered by a data processor during the processing routine and not known to the data principal himself, where the Intellectual property Right of the Processor may be involved.

To accommodate this, the existing laws are inadequate and we need to define a “New Legal Instrument”.

This legal instrument has to facilitate that every data processing situation be accommodated in the “Consent”. This instrument cannot be a formal contract as it would violate the Aadhaar judgement.

The Second Problem introduced by the Aadhaar judgement is by dismantling a system of real-time authentication which was unique to the use of Aadhaar e-KYC.

Hence Aadhaar itself was a means of obtaining explicit consent through e-kyc and e-Sign (Electronic Signature recognized under Section 3A of ITA 2000) and the Supreme Court has now raised objection to the use of Aadhaar based consent for data processing which could extend to its use for e-Sign.

This means that the one form of authenticated explicit consent which was possible in India to be obtained on real time basis has now vanished because of the Aadhaar judgement. PDPA 2018 has to therefore overcome the hurdles created by the Aadhaar judgement. It has to also save the e-Sign system which has a large role to play in the digital economy. There will be utter chaos in the economy if e-Sign is not protected as a system even if “Biometric Authentication” of Aadhaar is disabled and we have to replace it with OTP (or other alternatives to OTP) based authentication of another identification instrument such as Virtual ID or PAN.

The opportunity to set things right exists in PDPA 2018 by the creation of a new legal instrument that meets the Supreme Court judgement on Aadhaar and also meet the accepted Privacy requirements is available because of the ingenuity of the Srikrishna Committee in using the concept of “Data Fiduciary” instead of the more popular “Data Controller” or “Data Ownership” Concepts in defining the relationship of a Data Subject and a Data Processor.

Under PDPA 2018, the data principal will entrust his personal data to a Data Fiduciary with certain permissions which we loosely call as the “Consent”.

At first glance, the consent looks like a “Contract” but under the concept of “Data Fiduciary”, the Consent is more like a “Trust Deed” and the Data Fiduciary is like a trustee of the personal data.

Now “Contract” is objected to by the Supreme Court and under Indian laws the “Trust” also has an issue.

For example Trust deeds need to be stamped and perhaps registered in certain cases. Further, under Section 1(4) of Information Technology Act 2000, (ITA 2000) Trust deeds in electronic documents are out of the provisions of ITA 2000 including recognition under Section 4 and authentication under Section 5.

If therefore a “Data Fiduciary” is to be appointed by a Data Principal and the instrument should be recognized as a Trust Deed, amendments are required to the Stamp Act, Registration Act and Information Technology Act.

Further, “Data” or “Personal Data” has not been defined as “Property” in the PDPA 2018 though DISHA 2018 may define so. We know that Data cannot be a movable or immovable tangible property. It cannot also fit into known forms of intangible properties also though it is nearest to the “Intellectual Property of a Virtual Nature”. Hence law of transfer of rights on “Data” cannot fall into law of transfer of property as we know now.

Data is essentially a sequence of “States” of an object which can take the values zero or one. The sequences of the states are interpreted under a given protocol as either a letter or a number or a sound or a video etc. based on the configuration of the reading devices. Hence Data does not have independent existence and only have a dependent existence.

Such a property therefore cannot be brought under any of the existing laws of the physical society except with inconsistencies and compromises.

Hence there is a need to define the nature of property of “Personal Data” along with defining a new type of instrument that can create a “Data Fiduciary” with legally enforceable obligations”.

The “Consent” under PDPA 2018 will therefore be such a type of new instrument.

We therefore need to add in the definition part of the draft PDPA 2018 a new sub section… say 3(42) as follows.

> **3(42) "Data Fiduciary Creation Instrument"** means, an instrument
>
> -executed by a natural person as a Data Principal for the purpose of designating a Data Fiduciary,
>
> - containing the terms under which the personal data of the data principal may be processed by the Data Fiduciary or his authorized agent and
>
> -which may be authenticated in electronic form as provided under law.
>
> Explanation:
>
> a) The Data Fiduciary Creation Instrument is not a "Contract" under the Indian Contract Act 1872 or a Trust Deed under Indian Trust Act 1882.
>
> b) The Data Fiduciary Creation Instrument in electronic form may be authenticated
>
> -by electronic signature approved under law and with the use of non biometric authentication of an appropriate identity such as a Virtual ID created by any process, whether derived from other existing IDs including Aadhaar, PAN or any other identities or a combination thereof.

8. Data Protection Officer

According to the current proposition, designation of a Data Protection Officer is mandatory for all data fiduciaries and preferably by the Data Processors.

According to Section 36 (2), the designated data protection officer (DPO) may be assigned functions other than what is designated as responsibilities of a Data Protection Officer under Section 36(1).

Hence in most of the cases one of the existing persons in an organization would be designated as a Data Protection Officer just like designation of a Compliance Officer.

The PDPA 2018 differs from GDPR in this respect since GDPR provides that a Data Protection Officer where required could be an external consultant and also that a group of companies can use the services of a single Data Protection officer.

The GDPR provision recognizes that there is a possible conflict of interest in the functioning of the DPO if he is an internal employee with additional duties assigned to him.

While GDPR does not prohibit an internal employee being designated as DPO, he has to be at a sufficiently senior level as to be able to advise the Company at the level of CEO or even the Board. GDPR therefore recognizes that in certain circumstances, it is better if an external consultant is appointed as a DPO.

PDPA 2018 by allowing an employee to be designated as a DPO is more convenient to the Data Fiduciary. However it does not recognize the conflicts of interest for a

DPO who is answerable to the Data Principal on the one hand, the Data Protection Authority (DPA) on the other hand besides the Company management.

Management of this three way loyalty is likely to be difficult in the situations where security is compromised for business reasons and data breaches are tried to be buried under the carpet for business reasons.

PDPA 2018 recognizes the need for annual external data audits but it is considered better if an enabling provision is made for the DPO to be appointed as an external consultant besides the option of using an internal professional.

For this purpose it is suggested that a new sub section be added to Section 36(5) on the lines of Article 37 of GDPR, as follows.

36 (5) : Nothing in this section will prevent a Data Protection officer **not being** an employee and fulfilling the tasks on the basis of a service contract and discharging such responsibilities for a group of undertakings.

This will enable development of a cadre of professional Data Protection officers like the Company Secretaries and Chartered Accountants in India and ensure that adequate number of trained professionals would be available to provide the necessary services.

9. Offences

As per Section 93, it is proposed that offences under the Act shall be “Cognizable” and “Non-Bailable”.

This could turn out to be a draconian provision and amenable to misuse.

Considering the complexities involved in adjudging Data breach incidents and fixing responsibilities, the possibility of harassment of the industry professionals by the Police using the “Non Bailable Provision” is very high.

There is also a possibility of unscrupulous management misusing the Police to take revenge on disgruntled employees. Even DPOs who are more loyal to their duties than the orders of the management may come under fire because of this “Non Bailable” provision.

In order to avoid PDPA 2018 becoming another Section 498A (IPC) kind of law, it is absolutely essential to make the offences “Bailable”.

Additionally, while the investigations of offences under PDPA 2018 may be undertaken by a police officer of the rank of an Inspector as proposed, No arrests should be allowed except with the written permission of a “Data Protection Prosecution Committee” that should be created on the lines suggested by the T.K.Vishwanathan Committee on amendments to Information Technology Act (which suggested amendment to CrPC but is yet to be formally adopted). A similar approach was suggested by one bench of Supreme Court in respect of Section 498A though it was later over turned by another bench with instructions to the Government to make suitable laws for the purpose.

Now in respect of offences under PDPA 2018, such a law can be incorporated in this PDPA 2018.

This may require addition of a new section in Chapter XIII to the following effect.

Section 93 should therefore be amended to say

Sec 93: (1) Notwithstanding anything contained in the Code of Criminal Procedure, 1973 (2 of 1974), an offence punishable under this Act shall be cognizable and Bailable

A subsection to be added to Section 93 as follows

93(2): No arrests or seizure of assets shall be permitted under the PDPA except by a written order of a PDPA Offences Regulation Committee constituted as a State level committee with the following composition.

1. The DIG in charge of Cyber Crimes in the State, who will be the Chairman of the committee
2. The IO involved in the investigation
3. One expert from public with necessary qualifications and experience in data protection
4. One designated Data Protection Officer from the industry to be co-opted by the other members
5. One Public Prosecutor designated by the Chairman
6. One representative designated by the DPA

The Gazette notification of the constitution of the committee shall be placed before the State legislature and passed.

10. Data Localization

As regards the Data localization requirements, the main proposition as indicated in the draft may be retained.

But as discussed under “Applicability”, an exemption needs to be provided for Personal Data of foreigners and activities not related to India which come under this regulation because the data is processed by Indian Companies from the requirements of Section 41.

A subsection 41(7) may be added for this purpose stating as follows:

41(7) Nothing in this section shall apply to a Data Fiduciary when the personal data does is not related to an Indian Citizens or representing any activity within the territory of India and the personal data is collected and processed outside India.

10: Various Recommendations on Aadhaar Act in the Report

Justice Srikrishna Committee had included a list of amendments proposed to Aaadaar Act from its perspective of Privacy protection. Some of these recommendations may have to be seen now in the context of the Supreme Court judgement. These are amendments that may happen in the Aadhaar Act but are relevant to be mentioned here so that there are no conflicting inclusions in the PDPA 2018.

i) Amendment to Section 2: It was proposed that the definition of Aadhaar number may be modified to include the words "and any alias thereof generated in a manner specified by regulations". **We suggest dropping of these words.**

   It is necessary that services created by UIDAI such as Virtual ID should not come under the definition of Aadhaar and restrict their use.

ii) Keeping the recommendations of the Supreme Court in its judgement, any person aggrieved by the action of any other person using Aadhaar data and causing a wrongful harm, should be eligible to approach the Adjudicator for claiming compensation if any or the relevant law enforcement authorities for prosecution.

iii) The PDPA 2018 contains the DPA and a system of Adjudication and Appellate Tribunal. Most of the issues that may arise in Aadhaar may relate to Privacy infringement and hence will be the subject matter of PDPA 2018 as well. Hence there may be a need to make the Adjudication and Appellate Tribunal formed under PDPA 2018 to also take up the Adjudication and Appeals that may come up under the Aadhaat Act without the need for a separate set up.

iv) The Section 57 may be amended as suggested by the Supreme Court to delete the contractual use of consent to process Aadhaar information as there is no alternative.

v) We have no comment on the other recommendations made by the Committee on the Aadhaar Act.

11. Other Miscellaneous Observations

We do not see any need to make changes to

a) Right to erasure being subjected to Adjudication
b) Amendment proposed to the Right to Information Act

which have come for discussion in the professional circles.

For Foundation of Data Protection Professionals in India

(Sd)

Chairman
(Na.Vijayashankar)