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: 12th February 2020

To

The Director
Loksabha Secretariat,
Room No 152, Parliament House Annexe
New Delhi 110001
Via E Mail: jpc-datalaw@sansad.nic.in and mrs.mlekhi@sansad.nic.in

Sub: Joint Committee on the Personal Data Protection Bill 2019

With reference to the press release of 27th January 2020, we are submitting comments from our organization on the Personal Data Protection Bill 2019 (PDPB2019) for the kind consideration of the members.

Foundation of Data Protection Professionals in India (FDPPI) is a Section 8 Company established in 2018 dedicated to the development of the data protection eco system in India. Sri Vijayashankar (Popularly known as Naavi, who is the founder of www.naavi.org) is the Chairperson of FDPPI and the members consist of professionals from the industry engaged in the activities surrounding Data Protection.

We would be happy to provide any clarifications on the points raised in the enclosed note.

Thanking you

Yours faithfully

Na.Vijayashankar

(Chairman)

Comments on PDPB 2019

Introduction

It is noted that the subject of Privacy is of interest to the legal community and dear to the hearts of those who swear by the Indian Constitution and the fundamental right of Privacy enshrined there in. At the same time, the PDPB 2019 which is a legislation to provide the Right to Privacy through a Data Protection regime is of interest to the IT community involved in the Data Processing related activities. At the same time "Data" is a valuable raw material that a business would like to harness and is often referred to potentially a "New Oil" which on processing could yield many valuable by-products. Business managers therefore have their own perspective of "Data Protection Regulation" and how it impacts business.

In view of the differing perspectives of these three types of observers, the PDPB 2019 would invoke different view points which needs to be balanced in the final Act to the extent possible.

It is noted that the Bill does recognize these multiple stake holders and has tried to balance their interests. However it is recognized that in the current phase of receiving of public comments, there is a renewed assault of vested interests to get the draft changed to suit the vested interests of different stake holder segments.

FDPPI is aware of the prevalence of different perspectives and has tried to moderate its comments taking note of the compulsions under which the final Act has to be passed by the legislators.

We believe that many of the comments that are raised in the media donot take into account that currently we are discussing the Bill to be passed into an Act and several of the concerns that are being expressed can be addressed in the regulations following the constitution of the Data Protection Authority. We are also aware that there is a lack of common understanding on different aspects of Information Privacy Protection through Data Protection laws and it is a complex legislation to formulate. Often experts respond from their interpretation of GDPR without recognizing that India can have a law which is different from GDPR and perhaps better than GDPR.

Our comments take this view the above and focus more on what is required to be addressed in the Bill/Act without depending on GDPR related interpretations.

Recommendation 1: Correcting a typo error

Section 67(2) reads :

> *"The Appellate Tribunal shall consist of a Chairperson and not more than members to be appointed"*

The number of members in the Tribunal has been omitted. We recommend that the words "Two" can be added between the words "than" and "Members" so that the amended section would read as under;

> *"The Appellate Tribunal shall consist of a Chairperson and not more than* ***two*** *members to be appointed"*

Recommendation 2: Definition of Personal Data

Section 2(28) now reads as under:

> *(28) "personal data" means 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, whether online or offline, or any combination of such features with any other information, and shall include any inference drawn from such data for the purpose of profiling;*

The definition is silent on whether any protection of Privacy Right is limited to a "living natural person".

A Clarification on the treatment of personal information upon the reported death of the data principal needs to be included in the regulations.

Recommendation 3: Re-identification

Section 82(1)(a) presently reads as under:

> *(1) Any person who, knowingly or intentionally— (a) re-identifies personal data which has been de-identified by a data fiduciary or a data processor, as the case may be; or*

It is necessary to recognize that de-identification or pseudonymization and subsequent re-identification is also a process of sanitization of personal information undertaken during a processing activity within a Data Fiduciary or Data Processor. Such internal de-identification/pseudonymization and subsequent re-identification is not to be confused with the criminal activity of re-identification of a de-identified personal data set undertaken with a fraudulent or malicious intention.

We therefore recommend that Section 82(1)(a) be modified to read as under:

(1) Any person who, knowingly or intentionally ***and with dishonest or fraudulent or otherwise malicious intention****— (a) re-identifies personal data which has been de-identified by* ***another*** *data fiduciary or a data processor, as the case may be; or…*

This may require a consequential addition of an explanation under section 82 (1) stating

Explanation: The word "dishonest" or "fraudulent" or "malicious" shall have the respective meaning assigned to them under Indian Penal Code.

Recommendation 4: Gender as Sensitive Information

Under Section 2(36) the definition of "Sensitive Information" includes

Sexual orientation, transgender status, intersex status which are often treated as a third gender beyond "Male" and "Female".

To simplify the definition of sensitive information, the above three aspects can be deleted and replaced with the following:

"Gender" other than "Male" or "Female".

This will facilitate service providers collecting personal information as "Male" or "Female" or "Other" and the choice "Other" can be treated as sensitive.

Recommendation 5: Sunrise period

Though section 1(2) provides that the act may come into force on different dates for different provisions, the industry is concerned that compliance without pain would be facilitated if the Act is implemented with a clear time line.

Currently there is a time line of 3 months for the constitution of the DPA and there is no indication of the further time line.

It can be recommended that a proviso may be added to Section 2 to accommodate a time line as was present in the 2018 version of the Bill.

The modified Section 1(2) may therefore read as under:

(2) It shall come into force on such date as the Central Government may, by notification in the Official Gazette, appoint; and different dates may be appointed for different provisions of this Act and any reference in any such provision to the commencement of this Act shall be construed as a reference to the coming into force of that provision.

Provided further that

a) the Chairperson and the Members of the Data Protection Authority shall be appointed within 3 months from the date of notification of this Act

b) *the DPA shall commence its activities not later than 6 months from the notification of the Act*
c) *the Registration of Data Fiduciaries as envisaged under the different provisions of the Act shall commence not later than 9 months from the date of notification of this Act*
d) *Adjudicators and the Appellate tribunal as envisaged under the Act shall commence not later than 12 months from the notification of this Act*
e) *All other provisions of the Act unless otherwise specified by the DPA shall be deemed to be effective not later than 18 months from the notification of this Act.*

Recommendation 6: Publication of Privacy by Design Policy

According to Section 22(4), it is provided that

> *(4) The privacy by design policy certified under sub-section (3) shall be published on the website of the data fiduciary and the Authority.*

Considering that the "Privacy By Design Policy" as envisaged would contain many confidential and proprietary information of the Data Fiduciary, the industry would be reluctant to let the policy be published either on the DPA website or on its own website. While the DPA has the right to get the detailed information of how the data protection is handled by a data fiduciary which will be part of the DPIA (Data Protection Impact Assessment) also, the publication of the same on the website is avoidable.

It is therefore recommended that Section 22(4) be modified as under:

> *(4) Subject to the regulations made by the Authority, the Certificate issued by the Authority in respect of the privacy by design policy or an abridged representation of the Policy there of be published on the website of the data fiduciary and the Authority.*

Recommendation 7: Adjudicator

Under Section 62 of PDPB 2019 the Adjudicating officer would be appointed by the DPA and also prescribes certain credentials for appointment which includes an experience of 7 years in a relevant field.

The Government has retained the option of indicating the terms of appointment.

As the section indicates now, an Adjudicator could be a permanent employee of the DPA.

It would be advisable that Adjudicator be appointed on a contract of around 5 years so that experienced legal professionals presently working in the industry and practicing advocates can take up the position as a short/medium term quasi judicial posting and later revert back to practice.

Accordingly, Section 62(1) may be modified as under:

(1) For the purpose of adjudging the penalties under sections 57 to 61or awarding compensation under section 64, the Authority shall appoint such Adjudicating Officer as may be prescribed under a contract for a period not exceeding 5 years.

Recommendation 8: Right to erasure and Right to deletion

Currently the Bill refers to the "Right to Erasure" under Section 18 and "Right to be forgotten" under Section 20. There is an overlapping of the two provisions and further with the obligations of the data fiduciary not to retain the personal data after the purpose for which it was collected is no longer relevant.

One way this can be corrected is to remove the "Erasure" reference from Section 18 and retain only the correction.

Alternatively an explanatory statement can be added as under after Section 18 and 20

Section 18: Explanation: "Right to erasure" under this section is a right to stop further use of the personal data in the processing activity. It does not extend to retention of the personal data in an archive as part of the legitimate interest of the data fiduciary or data processor.

Section 20: Explanation: "Right to be forgotten" under this section is a right to get all identifiable personal information about the data principal irreversibly removed from the custody of the data fiduciary as distinct from the right of erasure under Section 18.

Recommendation no 9: Conflict of Interest of Data Protection Officer (DPO)

As per the current version of the Act, appointment of a DPO is mandatory for every significant data fiduciary and such DPO and such DPOs can be assigned with other duties.

Considering the need to maintain the independence of the DPO, it would be necessary for the Authority to ensure that the DPO does not come under undue internal pressures to dilute his duties to the Data Principals.

It is expected that the regulations can ensure that the DPO reports to the highest authority in the organization and is provided with the freedom to exercise his duties.

Since all Significant Data Fiduciaries need to register themselves with the DPA, DPA can exercise its control on the status of the DPO as a part of the registration process.

It is however necessary to ensure that the information on appointment and removal of DPOs to be made available to the DPA. DPA can also consider that DPOs be registered similar to the Data Auditors.

The rules may also ensure that the organization indemnifies the DPO against personal liabilities that may arise on account of his discharging the duties as envisaged under the Act.

Since this provision can be addressed in the regulations, no specific recommendation is made for amendment of the Act on this ground.

Recommendation no 10: Restrictions on transfer of personal data

The Government has yielded to the pressure of the industry in dropping the restrictions for transfer of personal data outside India and retained the provisions of data localization only for sensitive and critical data.

In order to ensure that the Government retains supervision of data fiduciaries who transfer personal data out of India, a provision can be added under Section 26 to declare all data fiduciaries who transfer personal data outside India without maintaining a serving copy in India as "Significant Data Fiduciaries".

Accordingly, Section 26 (1) may be modified as under:

> *(1) The Authority shall, having regard to the following factors, notify any data fiduciary or class of data fiduciary as significant data fiduciary, namely:—*
>
> *(a) volume of personal data processed;*
> *(b) sensitivity of personal data processed;*
> *(c) turnover of the data fiduciary;*
> *(d) risk of harm by processing by the data fiduciary;*
> *(e) use of new technologies for processing;*
> *(f) Transfer of personal data outside India without keeping a serving copy in India, and*
> *(g) any other factor causing harm from such processing.*

Recommendation 11: Constitution of DPA

A concern has been expressed that since as per section 42, the Chair person and the members of the DPA are appointed by a selection committee consisting of the Cabinet Secretary and Secretaries of the Ministry of law and the MeitY, without the Chief Justice being part of the selection panel, there is a possibility of dilution of the independence of the DPA.

It is recommended that the Government should not yield to this objection since any appointment is amenable for judicial scrutiny and if the appointment is flawed, the Courts can intervene.

Otherwise, involvement of CJI for an administrative appointment would introduce an element of delay in the selection process.

Recommendation 12: Powers of the Government

A Concern has been expressed that as per Section 35, the Government may abuse the powers by exempting itself from the provisions of the Act.

However it is to be pointed out that the exemption is only within the limitations of the reasonable exemptions to a fundamental right as provided under Article 19(2) of the Constitution and hence does not violate the powers conferred on the Government.

It is necessary for the Government to re-iterate that there is a duty cast on the Government to provide security to honest citizens and excessive protection of the “Right to Privacy” cannot dilute the “Right to Security” of other individuals. Failure to do so would be a dereliction of the constitutional duty of the Government.

Government may however ensure that appropriate checks and balances are introduced through regulations so that a different Government department which may be provided with some exempted powers does not abuse the powers.

For Foundation of Data Protection Professionals in India

Chairman
(Na.Vijayashankar)