Indian Personal Data Protection Act (IN-PDPA) 2018 – Distillation paper

Developed and Written by: *Arijit Sengupta, August 1, 2018*

Understanding of critical areas

The recently released draft of the IN-PDPA aims to protect personal data from the lens of informational privacy as it deems the right to privacy as a fundamental act enshrined in the constitution. The draft covers several aspects – both from a legal standpoint as well as operational framework that will provide oversight during and after implementation.

Initial impressions relating to this law are that significant challenges are bound to occur as the draft is more from a legal point of view without taking into account the technological issues and processes that need to be mandated down to acceptable limits. This would have removed opacity and presented a clear and focussed lens on what is desirable, actionable and acceptable under the lens of the law.

Another point that we would like to highlight is that this Legal draft is placing far too much emphasis on the creation of a Data Protection Authority of India and expecting them to design processes, timelines and technological competence so as to tackle quite a few issues that have not been addressed adequately or been referred to under general terms of reference.

As a report – while we agree to a greater degree on the need for a Privacy law cumulatively, we tend to disagree with an initial assessment(s) (as in points) of the underlying need to have such a law. Namely:

"WHEREAS the growth of the digital economy has meant the use of data as a critical means of communication between persons"

- Our understanding is that while communication is one aspect of the Digital economy – it is not the only / and or key aspect of the same.
- Data is the culmination/fruit of the process that drive the digital world/economy and can be either farmed in isolation for furthering business prospects
- or taken cumulatively as a process of communication between people and societies leading to ever increasing connectivity

"WHEREAS it is necessary to create a collective culture that fosters a free and fair digital economy, respecting the informational privacy of individuals, and ensuring empowerment, progress and innovation"

- Use of the word collective is misleading – our contention is that it should be shared responsibility and objective in nature without bias
- Privacy is not just a matter of informational privacy but rather a lot larger than what forms the basis of this report

"AND WHEREAS it is expedient to make provision: to protect the autonomy of individuals in relation with their personal data, to specify where the flow and usage of personal data is appropriate, to create a relationship of trust between persons and entities processing their personal data…"

- Usage of the word appropriate needs clarity and definition

The Point 2 of the act specifies applicability areas:

(a) processing of personal data where such data has been collected, disclosed, shared or otherwise processed within the territory of India; and

(b) processing of personal data by the State, any Indian company, any Indian citizen or any person or body of persons incorporated or created under Indian law.

- What it does not specify in particular is whether it supersedes the Aadhaar act under the applicability areas.

(2) Notwithstanding anything contained in sub-section (1), the Act shall apply to the processing of personal data by data fiduciaries or data processors not present within the territory of India, only if such processing is —

(a) in connection with any business carried on in India, or any systematic activity of offering goods or services to data principals within the territory of India; or

(b) in connection with any activity which involves profiling of data principals within the territory of India.

Notwithstanding anything contained in sub-sections (1) and (2), the Act shall not apply to processing of anonymised data.

While point 2 under this section is particularly applicable to International companies, data mining firms or tech firms – there is a significant leeway being provided with the provision for not applying the law "under anonymised data".

- This means that cluster data has been left out of the purview of this act.
- The problem is not in as far as the cluster data itself, but rather the process applied to convert personal data sets into a homogenised cluster – this means that some point in it's journey from individual to cluster – this data will be vulnerable to manipulation

Under Point 3 of the Definitions:

Sub section 7

- Clarity is required whether the word "Equipment" encompasses BOTS/AI/ML

Sub section 20, 22 & 41

- "Genetic" and "Health" and "Transgender" data – Clarity is required whether this encompasses Bio-metrics

<u>Chapter II – Data Protection Obligations</u>

Point 4, 10 (Sec. 1)

- "Reasonable" – There is additional clarity required as this can be challenged/misconstrued and will differ basis point of view

Point 10 (Sec. 3)

- Clarity on time frame for assessment needs to be incorporated as this is open to interpretation

Chapter III – Grounds for processing of Personal Data

Point 12 (Sec. 4 & 5)

- This is important for Data fiduciaries – the burden of proof of consent lies with them – however it also does not specify a demarcated method of taking consent. This essentially means that the act of taking consent is largely left to the fiduciaries as well as the methodology. However in the event that the data principals pull out/ invalidate the consent then the legal consequences fall on the principals. What is not clear whether there is scope for any financial consequences which can fall on the Principal.

Point 13 & 14 - Processing of personal data for functions of the State

This is an important point that allows the State/Functionaries of the State/Departments and Parastatal's to process personal data for functions that involve service or benefit – What needs clarity is whether the consent of the Data Principal is required for these activities

***Point 16 - Processing of personal data* necessary for purposes related to employment**

Sub section 2

- This point needs clarity – is this related to conflict of interest clause? If so – then it should have merited a separate section under Definitions

Point 17 - Processing of Data for reasonable purposes

Sub Section 1 – Clause (a)

- Needs clarity as well as framework explaining "reasonable"

Sub Section 1 – Clause (d)

- Conflict of interest needs clarity especially if this runs counter to clause (c)

Sub Section 2

This section is essentially absolving the state and watering down the Privacy aspect for data principals in general. This is open to interpretation and open to data being accessed by multiple official departments without the rightful consent of the data principals. Further clarity is required.

Chapter IV – Grounds for processing of Personal Data

While the "Explicit consent" clause has been inserted under Point 12 and further bolstered by Point 18 (subsection 2a and 2b) – Points 19 and 20 allow the state/official bodies to bypass the same if required by Parliament and/or State legislature as well as by Law and/or a court of law. Clarity is

sought whether consent sought can be specific to these points or whether there is no need for consent during conditions explained under Point 19 and 20.

Point 22

Sub – section 2 Clauses (a), (c) and (d)

These causes require further definitions and implications

Chapter V – Personal and Sensitive personal data of children

Point 23 – Sub section 5

While Guardian data fiduciaries are covered under this point – what is unclear are the following:

- Implication for schools and universities/colleges
- Whether this allows parental data to be mapped and if there are any implications

Chapter VI – Data Principal Rights[1]

The right to be forgotten falls under this segment Point 27 (Subsections 1 – 5). The first 3 points and related clauses explain the environment under which a data principal can contest (for lack of a better word) by way of ensuring that his/her data disclosure in specific instances. This is significantly different from the EU GDPR clause of Right to be Forgotten and corresponding clause of Right of Erasure (Article 17, Paragraph 2). Therefore this Right to be Forgotten is significantly different from what has been enshrined under the EU GDPR

Chapter VII – Transparency and Accountability Measures

Point 29 Clause (a)

- Business Practices – This needs clarity and who will provide "Oversight" – Any checks and balances are being suggested?

Point 29 Clause (c)

- There should be well defined technology practices and models otherwise in conjunction with Clause (a) – this will be almost impossible to track and correct/control

Point 30 Transparency

This is an important segment for Foreign companies operating in India (especially Tech companies like Google, Amazon etc). Typically the law does not define "Reasonable" and what can be the likely processes that are mandatory. Clarity is also sought in terms of categories of data under clause (c)

Point 31 Security Safeguards

Quis custodiet Ipsos custodes! – Who guards the guards? While the Data fiduciary and processor are urged to take "adequate" safeguards – the manner, technology and processes have not been defined by law. This leaves it open to interpretation and challenge and something that cannot be argued since the law does not state the exact steps and methods/framework that need to be followed.

Point 32 Personal Data Breech

[1] https://gdpr-info.eu/issues/right-to-be-forgotten/

Point 1 refers to fiduciary notifying the "Authority" by which we presume the official body created to provide oversight for the Privacy laws if any data breech has occurred. It is interesting to note that the data principal will not be notified concurrently by the fiduciary thereby lowering his/her stature as the owner/creator of the said data.

Point 3 and 4 is even more ambiguous when it calls for "Time period" within which the breech needs be revealed by the fiduciary. The present act leaves a lot of definitions to be developed by the said Authority and we are not sure that as an act this is good form.

Point 5 goes on to state that the Authority[2] will decide on whether the matter of the breech needs to be released to the data Principal by the fiduciary. This is very different in the case of the EU GDPR wherein the controller will within a period of 72 hours notify the principal under normal circumstances. The difference is that unlike the Indian authority who will get to decide on whether to report the matter to the principal in the first place, unless otherwise stated the authority in the EU will report the breech to the principal as a matter of normal operations.

Point 33 Data Protection Impact Assessment

Point 1 – While there is scope for an Impact assessment before commencement of profiling using new technologies – guidelines are absent, presumably to be set by the relevant authority in question.

Record keeping/Legal/Audit Compliance Sections (Points 34 till 39)

These are important segments for foreign owned fiduciaries, especially those involved in digital transactions. Under Point 36, subsection 4 – While the law calls for the appointment of a Data Protection Officer to be based in India even for activities/processing not physically taking place in India – there is no clarity as to how compliance will be ensured with this appointment.

Chapter VIII – Transfer of Personal Data outside of India

This is a significant segment as it deals in the modalities for controlling or providing oversight in cross border data for trade, mining etc. The law clearly states the following:

- Point 40 - Sub section 1 – One functional set/copy of the personal data has to be kept within the physical confines of India
- The Central government will notify which personal data is critical in nature and this data cannot be ever processed of sent outside of the physical boundaries of India – Point to note is that the Data Authority will not be the one to decide but rather the Government in power will notify the same. This will be subject to possible political whimsy.
- The technical ramifications of having core data stored within India and operating data for developing profiles and services using the same core data (especially for Financial services) has not been fully explored. It is generally understood that the lesser the number of P2P gateway connections there are – the better the chances of preventing hacks.
- Point 41 further explains the conditions for cross border transfer of personal data and sub section 2 is essentially similar to the EU GDPR Recital No. 116
- **Counter to earlier point** – While Point 40 – Sub section 2 and 4 are categorical in defining the non transference of personal data deemed critical outside of India: Point 41, sub section 3 states that sensitive data deemed safe by the Central government can actually be stored outside of India – Operative words "Critical" and "Sensitive" need defining. This point also

[2] https://gdpr-info.eu/art-33-gdpr/

negates (if critical and sensitive are used to convey the one and the same thing) the earlier point and keeps the issue a bit nebulous and open to socio-political interference. We certainly need additional clarity on the usage of critical/sensitive and what it implies for the law. Though allowance of data (critical and or sensitive) outside of the physical limits of India can work for international tech fiduciaries

Chapter IX – Exemptions

A continuing theme through the draft is who can control data fiduciaries who are not physically present in India. What is the mechanism that needs to be elaborated for such an eventuality to be dealt with? Civil or Criminal jurisdiction outside of India will be dependent on other laws and treaties that are in existence and pursuant to oversight mandated by the country of existence or registry.

While Point 42, sub section 1 makes it clear that data processing will not be allowed in the interests of state security unless mandated by parliament or under and existent legal precedent, it also makes it clear (subsection 2) that if such an eventuality was to present itself then the provisions of this law will not be applicable under various points and subsections.

Under Point 43, subsection 3 provides immunity for data principals who are victims, witness etc with a rider that their data processing will not take place only if it victimises or compromises them. However, there are no clear guidelines on what the steps will be to prevent such a thing occurring in the first place.

Under Point 45 – there is guidance for Research, Archival and Statistical mapping of data, however there is no clarity on what steps need to be taken in the event data is compromised during the process.

Chapter XI – Penalties and Remedies

While there are defined parameters for levying penalties by way of calculating a percentage on worldwide turnover – we need clarity on implementation and final recovery process. The pertinent sections are:

Explanation I. For the purposes of this section, "total worldwide turnover" means the gross amount of revenue recognised in the profit and loss account or any other equivalent statement, as applicable, from the sale, supply or distribution of goods or services or on account of services rendered, or both, and where such revenue is generated within India and outside India.

Explanation II. For the purposes of this section, it is hereby clarified that total worldwide turnover in relation to a data fiduciary is the total worldwide turnover of the data fiduciary and the total worldwide turnover of any group entity of the data fiduciary where such turnover of a group entity arises as a result of the processing activities of the data fiduciary, having regard to factors, including

Chapter XII – Appellate Tribunal

A significant draft ruling under this section is that of (Point 89) no civil court having any jurisdiction on any decision arrived at or delivered by the Appellate Tribunal under this act.

These are the majority of the points that we felt, one should highlight. The larger report (which have been marked by us earlier) covers all the points that have been missed in this distillation note. For a greater understanding, it would be beneficial to read this in conjunction with the full draft law.