STAKEHOLDER CONSULTATION ON THE PERSONAL DATA PROTECTION BILL, 2019

Organized by:

The Dialogue and Priti Suri Associates (PSA)

Chennai, 7th March 2020

Overview

The Dialogue organized a stakeholder consultation on ***The Personal Data Protection Bill 2019*** in partnership with **Priti Suri Associates** on **March 7th, 2020**. The event was held at The Raintree Hotel, St. Mary's Road Chennai.

The discussion at the event was aimed at analysing the Personal Data Protection Bill 2019 and voicing the various implementational or fundamental concerns that various stakeholders believe exist within the new framework. The aim of the event was to find ways for the Government and stakeholders to understand each other's concerns and find a balance between economic growth, individual's privacy and national security while drafting this new law.

The discussion was moderated by Mr. Kazim Rizvi, founder of the Delhi tech-policy focused think-tank, The Dialogue and Ms. Priti Suri, Managing Partner at Delhi based law firm, PSA Legal.

Amongst the people who attended, there were members of the tech policy space from different organizations such as PayPal, Renault Nissan Automotive India Pvt. Ltd, Zoho Corp, SIAM computing, Virtusa Software Services Pvt. Ltd, Sify Technologies, Isuzu, Ashok Leyland, Cognizant Technologies, The Hindu, Deloitte, IAPP, Grant Thorton, Intellect Design Arena Ltd, SIAM computing, Detect Technologies, W Square Incubation Centre and Carnegie India. The event had an attendance of 26 individuals.

Recommendations

Transition period

1. It was recommended that, there should be a minimum time of 24 months for entities to prepare and comply from the date of notification of a particular standard/code of practice or rule.
2. It was also recommended that phased implementation of the legislation takes places in a manner similar to the following:

    a) By providing for timelines for formation of the Data Protection Authority

    b) By stating minimum lay off periods of 24 months for applicability of any particular rule / standards / code of practice from the date of its notification. (This period will exclude the stakeholder consultation period that the Authority needs to undertake before notification of such standard/code of practice or Rule.)

Consent

1. It was recommended that Government revaluate it's consent requirements to better understand business models and to ensure that the consent collected is truly 'informed'. The aim should be to have requirements that uphold the basics of informed and specific consent, rather than onerous requirements that would not be feasible to a variety of business models.
2. It was also recommended that the Government develop models for non-consensual processing in certain situations such as public health emergencies,

grave issues of national security. However, it is recommended that such models are intricate and an individual's privacy is at the heart of any such model.

Cross Border Data Flows

1. It was recommended that the Government reconsider the data localization requirement and instead aim to develop a multilateral or bilateral framework that governs the cross-border flow of data. As the Government of India is mainly looking to localise and limit cross-border data flows, primarily owing to security concerns. We believe that bilateral and multilateral agreements on data sharing and data access can be the way forward. Either bilateral or multilateral avenues along the lines of EU-US Privacy Shield, Convention 108 or the APEC-CBPR privacy model would help the Government to achieve its objectives while being at par with other jurisdictions globally. In addition to this, the government must also consider a bilateral arrangement with the US Government through the CLOUD Act to seek access to data for law enforcement.
2. It was recommended that if a localization mandate is to exist, it ought to be sector based. Such requirements will be decided based on consultation between the sectoral regulator and the DPA. The said consultation should involve active participation of the all affected players in the sectoral ecosystem.

Data Protection Authority

1. It was recommended that there is inclusion of a judicial member and a member of the opposition in the Select Committee to ensure that there is judicial oversight and impartiality in the selection process.
2. It was further recommended that there is an inclusion of non-executive members the structure of the Data Protection Authority (DPA). They serve as independent observers in the functioning of the Data Protection Authority (DPA) and alert the Government of any non- compliance of law by it.
3. It was recommended that there is a need to enhance the technical and judicial expertise of the members of the Committee. This is a move imperative to ensure that Data Protection Authority (DPA) has the requisite technical and judicial expertise to carry out the variety functions entrusted to it.
4. It was recommended that in order to avoid overburdening of the Data Protection Authority (DPA), it is suggested that a tiered structure of the Data Protection Authority (DPA) is envisioned, with a Central body and State authorities existing simultaneously. It was suggested that a model where separation into ombudsman for complaints and then rule making process with a regulatory body can exist, thereby dividing the powers.
5. It was recommended that the platform for interacting with the DPA be made multi-lingual, more graphic and less text-based and overall less dependent on literacy (and digital literacy) so that a broader section of the population can raise their concerns with the Authority.

Regulation of Non Personal Data

1. It was recommended that since the draft bill does not cover non personal data under its ambit, the Government avoid the hasty inclusion of a clause dealing with non-personal data in a bill that seeks to protect personal data. Secondly, in light of the ongoing process of consultation being undertaken by the

Committee of Experts on Non Personal Data, chaired by Shri Kris Gopalakrishnan, we recommend that no regulation of non-personal data take place until the committee has put forth its recommendations.

Penalties

1. It was recommended that the Government re-assess the requirement of calculating penalties as percentage of the annual worldwide turnover of companies, keeping in mind that such provisions could be detrimental to small players and also prove to be an unfair method of calculation as the volume of business for companies varies in each jurisdiction.
2. It was recommended that the Government remove the provision that provides a jail term as a penalty for violation of certain provisions of the Act, in order to prevent having an environment that would precipitate fears of entrepreneurs to operate and innovate, and remain an unconducive environment for growth.

The Dialogue
Inform Engage Ideate

PSA
LEGAL COUNSELLORS

Summary of discussions

Kazim Rizvi and Priti Suri began the discussion by sharing a brief background of the Personal Data Protection Bill and discussing the severity of its impact on a variety of sectors ranging from healthcare to data processing. They stressed on the need for engaging with stakeholders at this stage of the legislative process and ensured that the recommendations and insights brought up at this consultation would be presented to committee members.

To begin the discussion, participants shared their views on the comparisons between the 2018 draft of the bill and the bill that was tabled in Parliament this December. There was consensus among members that a host of recommendations with respect to certain aspects were taken into consideration by the Government. However, it was felt that some broad concepts have been left unaddressed. Many stakeholders felt that since a law governing data is an evolving law, there must be mechanism for collaboration between stakeholders, the regulatory authority and the Government. The importance of public and stakeholder consultations was discussed.

Transition

As the discussion progressed, the first key concern shared by all stakeholders was the lack of clarity regarding the transition phase of this legislation. The lack of an implementation timeline or strategy being laid out in the main text of the bill, as compared to the older drafts was a cause of surprise to many. The earlier draft of the bill had a transition provision, where in a period of 18 months was provided for phased implementation of the law. With respect to the Data Protection Authority (DPA), to be established by the law, a period of 3 months was provided for it be operationalized.

Such a provision entailed a process where there would be a tiered notification of different provisions and subjects would also be provided with ample time to become compliant. It was highlighted that technological and business models that rely or use data are pre-existing and well established, thus it is imperative to take an approach which would make it easier for models to adapt to without undertaking unnecessary structural changes. In the situation that the entire legislation will come into force at the get-go, the need for air-tight law was stressed upon. A parity with the competition law framework was drawn to bring emphasis to the time required for the system to function smoothly.

Stakeholders agreed that at present the law is rather incomplete, which further highlights the need to have a more strategic and well-planned implementation timeline. Certain important provisions such as the definitions of Sensitive Personal Data and Critical Sensitive Personal Data and a host of rules and processes have been left to be notified later. In such a situation if an attempt is made to

Consent

One of the concerns that resonated across the room was the issue of consent-based processing. Stakeholders believed that it would be a dangerous proposition to make consent a sole basis for processing. Other requirements such as legal contractual obligations, must also be taken into consideration. Consent is a dynamic concept and the bill must take this into consideration. Processing solely on the basis on consent would not serve the best interests of data subjects. Complications such as consent fatigue and uninformed consent are already widely discussed side effects of a consent-heavy regime. There is a need to ensure that the consent requirements are not heavy-handed and serve their true purpose of receiving a data subjects 'informed and free'

consent rather than work to their detriment. At present, individuals are often giving up their legal rights as a consequence of consent fatigue.

The need to bypass consent-based processing in a variety of situations was also discussed. For example, it was noted that the 2018 draft of the bill allowed employers to process sensitive personal data and critical personal data without the consent of employees for employment purposes. However, with the changes in this draft this would be limited to personal data, with the narrow scope of personal data, many businesses are likely to face hardships while undertaking simple processes.

It was noted that other nations have managed to address the situation of ensuring a mechanism to securely process data taken without consent. Especially in situations of emergency, it is imperative that there are provisions that allow for the processing of data without consent. The recent response of the Government of Singapore (Health Ministry) to the COVID-19 outbreak by allowing certain exemptions with respect to processing for companies to facilitate better containment and treatment measures for the Government was stated as an example. A collaborative approach, with the executive having enhanced flexibility in certain situations was viewed as an ideal solution. However, it was noted that the executive must not be given too much power and any such orders must have proper jurisprudential backing.

A point regarding the importance of the consent model, was of how consent plays and important role in women protecting their data was also raised. A lot of sensitive data regarding women's health, finances, etc is shared with a variety of apps and services. In such situations it is imperative that any processing is done with the complete consent of the individual. This aspect helped highlight how that we must create a non-

consent-based model for certain situations but the even within those models it is the individual's privacy that must be given paramount consideration.

Cross border data flows

On the topic of data localization, the stakeholders first addressed the issues of safety of data. They largely believed that the narrative for localization has survived due to the notion that data is secure if it is within their own territory. However, a key point was made that ensure high level security of data, it is imperative that there is a strong infrastructure in place, both in terms of cyber security models and regulation. India at present unfortunately does not possess that level of infrastructure to serve such a purpose of ensuring safety and security of data. Stakeholders also warned that cyber security and personal data protection are separate issues and must not be confused to be one same issue.

The second issue addressed was that of access to data for law enforcement agencies for the purposes of maintaining law and order and national security. However, data access is largely dependent on legislative and policy measures. The physical location of data does not influence access to data to a large extent. Stakeholders recommended that strengthening of existing measures by reducing procedures and timelines would serve the purpose better than mere localization of data. Stakeholders suggested the inclusion of data sharing provisions as a part of bilateral agreements or following a cross-border privacy agreement model to enhance access to data for law enforcement. It was pointed that globally, models along the lines of Mutual Legal Assistance Treaties (MLATS) and other Government-to-Government discussions are the preferred mode followed by countries to ensure access to data for their law enforcement agencies. They

provided an example of the current system followed with foreign companies, where legislative and policy measures to get access to data.

Aside from these concerns, it was pointed out that restrictions on the cross-border flow of data will impact the Indian industry in a variety of ways. Stakeholders pointed out that mandatory localization of data will lead to huge compliance requirements for businesses across sectors to develop or acquire the adequate safety standards. These compliance issues could force a large number of SMEs out of the business owing to the inability to sustain costs. Localization requirements for the data of foreign nationals will be detrimental to the domestic data processing industries at large.

A large volume of IT services and BPOs operate out of India, these provisions would prove to be a setback to their business models, thereby affecting our economy. Stakeholders pointed out the difficulty faced across the board owing to the RBI's requirement to localize all financial data, largely owing to the lack of sufficient infrastructure. Stakeholders believed that as India's digital economy and technology infrastructure continues to grow, localisation of data will occur as a business consequence and it would be advised to not force such a requirement at this juncture.

The concerns of increasing India's carbon footprint as a result of large-scale establishment of data centres was also raised. Considering the focus on climate change mitigation efforts worldwide, India should be mindful of increasing its carbon footprint as we are already a largely industrial nation.

Data Protection Authority (DPA)

With regard to the proposed Data Protection Authority (hereinafter referred to as "DPA") as established by the law, stakeholders pointed out that the draft largely deals with the creation of the authority and does not deal with the functionality of the authority in detail. Major concerns regarding the authority include the selection process and criteria, independence of the authority, concerns regarding lack of qualified members and overburdening. Stakeholders also questioned the creation of new appellate authorities and adjudicating officers for this purpose and discussed if existing authorities (regulators) could be empowered to handle such functions instead.

The Selection Committee of the DPA as per the 2019 Bill, consists of a Cabinet Secretary (as a chairperson, a secretary from the Department of Legal Affairs and a secretary from the Ministry of Electronics and Information Technology. Earlier drafts, included a judicial member (either the Chief Justice of India or another Supreme Court judge), however the present change in the composition of the selection committee has raised concerns regarding the independence of the body. Stakeholders believe that the suggested procedure undermines the independence of the authority and creates an impression that the regulator is completely dependent on the Central Government for its creation and composition. They were of the opinion that due to the presence of only members of the executive in the committee, it would be hard to pacify individuals regarding the absence of a central government influence in the selection and thereby the functioning of the authority. Further, to enhance the independence of the authority it was suggested that the authority be financed through the consolidated fund of India as opposed to the executive. Stakeholders stressed the importance of independence owing to the fact that the Government is the largest data fiduciary.

Another major concern that plagues the authority is regarding possessing adequate technical and legal expertise. As the authority is to deal with complex issues relating

to data governance and technology, stakeholders were of the opinion that it is imperative that members possess adequate technical capacity to deal with such issues. They suggested adopting a model along the lines of the Telecom Regulatory Authority of India (TRAI) and Securities Exchange Board of India (SEBI), where a distinction is made between whole time and part-time members, wherein technical experts could also be brought into the fold. As the body is required to perform an array of judicial functions, stakeholders stressed on the need for having a judicial member in order to ensure that there is better understanding of the legal aspects involved. Alternatively, mandatory training in these areas for members was also suggested.

Aside from these concerns, stakeholders were sceptical about employing the use of the Code of Civil Procedure to undertake proceedings (disputes and enquires). They believed that this may bring on the same delays that exist in conventional courts and lead to stagnation of the process. It was pointed out that a fast-track administrative process is important as technology moves fast and the regulators must be able to keep up with it. For the same, it was suggested that the model of the information commission be followed. The removal of a requirement to publicise annual reports of the DPA at regular intervals was flagged as a concern by many as well.

Stakeholders also believe that there is a need for authority to be accessible in all forms. As India has a very diverse demographic profile, it is imperative that every section of society has access to such an authority. The challenge of addressing the many languages of India must also be tackled. Stakeholders suggested that the authority be made multi-lingual, more graphic and less text-based. The need to not depend on literacy and digital literacy was also mentioned.

Issues regarding the vast burden of responsibilities placed on the DPa with respect to further legislation on the topic in the form of policies, rules and regulations yet to be notified formed a large part of the discussion. Stakeholders believed that the variety of functions that the DPA sets out to perform are enormous and range from monitoring to adjudication and will contribute to reducing its efficiency as a regulator.

Aside from concerns regarding capacity of the members and the regulator itself as raised earlier, stakeholders pointed out that the sheer volume of complaints that will be received by the DPA would be difficult to process in a timely manner. As time is key in matters relating to data and its protection, this may prove to undermine the purpose of the authority. In addition to handling such complaints, the authority will also be required to deal with the various duties assigned to it such as formulation of rules, regulations, best practice guidelines and other powers of oversight for a smooth functioning of the data framework in India. The main concerns of the stakeholders with respect to this was that very little time has been devoted to create systems to carry out such functions. Stakeholders believed that in a such a situation, the DPA will not be cohesive and functional organisation by the time that the regulation comes into force, which could prove to be a huge hurdle for the entire framework.

Non-Personal Data

An issue that resonated with almost all stakeholders across the board, was the inclusion of regulation of non-personal data within the ambit of the Personal Data Protection Bill, 2019. There was consensus around the point that since the aspect of regulation of non-personal data is currently being debated by a committee, chaired

by Mr. Kris Gopalkrishnan, under the aegis of the MeitY, no decision regarding its regulation must be taken until a report is submitted. Due to the nature and uses of non-personal data hasty regulation could be detrimental to the economy and the rights of individuals.

Regarding the manner in which the legislation regulates personal data, concerns were raised regarding the safety of data vis-à-vis maintaining the anonymity of data. Stakeholders expressed their concerns over how at present it is not possible to ensure the anonymised data cannot be deanonymized easily. They pointed out how there are umpteen examples in daily life where data that can be used to de-anonymize data sets fall into the wrong hands. For example, there are regular reports of data breaches wherein the passwords of users are accessed by hackers. The inability to understand technical processes serves as a major limitation to regulate issues such as anonymization was pointed out as a major hurdle by stakeholders. They believed that regulation of such a technical process requires nuanced and thorough policy making and re-iterated that hasty regulation could be harmful. Stakeholders stressed on the fact that as technology itself at present cannot guarantee complete anonymisation of data, the prescription of anonymisation standards to ensure safety would be difficult to arrive at.

Another aspect that was raised was Clause 91 of the Bill, which deals with the access to non-personal data of any entity by the Government of India for the purpose of aiding in the process of digital policy making. Stakeholders raised concerns of the mandatory nature of the process. Certain stakeholders spoke regarding how non-personal data, that is held and owned by companies is a form of meta-data and is covered by intellectual property protections, the form of access proposed by the Bill for the Government of India, would ideally violate WIPO protections for intellectual

property. Protection and regulation of IP form a huge part of trade agreements and such callous regulation could lead consequences for India with respect to its trade relations with other nations and make India a less favourable destination.

However, all stakeholders were of the opinion that the regulation of non-personal data is required, but they also stressed on how we must consider the large amount of data that has already been collected, monetised and used while making such decisions. The approach of the Government must not disrupt models to the extent that many players will be forced to exit. There is a need to evaluate existing systems, identify specific issues and build solutions for the same. A pertinent point made was that India is home to a vast amount of intellectual property and has a lot of potential which can be tapped into by creating a framework that is suitable to all the stakeholders involved. Stakeholders recommended that an approach that addresses specific use of data rather than blanket regulation would be ideal in such situations.

Penalties

A major concern of stakeholders from the industry were regarding the nature of penalties imposed through the legislation. The first issue regarding penalties was the irregularity in penalties for the Government as compared to other entities. As the Government has an equal duty to the citizens to protect their data, such a provision sends across a wrong message. Secondly, concerns regarding how penalties are calculated based on the annual turnover of companies was addressed. Stakeholders believe that such a system would place an immense hardship on all players, especially the smaller ones. They suggested that the Government re-assess this requirement to take into consideration the volume of business in each jurisdiction. Another suggestion was regarding having different slabs of penalties for companies

of varying prosperity. Thirdly, concerns regarding the criminal penalties of jail terms were raised, stakeholders were of the opinion that the penalties prescribed were too severe in nature. They also believed that in light of the Government's recent decision to remove jail terms as a penalty for the violation of a host of civil offences across legislations such a move would be unfair to the technology community.