STAKEHOLDER CONSULTATION ON THE PERSONAL DATA PROTECTION BILL 2019: THE DIALOGUE AND PSA

INTRODUCTION

The Dialogue and **PSA** organized a stakeholder consultation on ***The Personal Data Protection Bill 2019*** on **January 10, 2020**. The event was held at the Regency IV and V, The Lalit, New Delhi.

The introduction of the EU GDPR (General Data Protection Regulation) has set the ball rolling regarding strengthening of legal provisions to protect personal data across the world. The enforcement of the law has begun a huge global shift for data privacy. In the ***KS Puttuswamy v. Union of India***, the Supreme Court held that each individual had the fundamental right to information privacy and recognised the need for the Government to put in place a legal regime that protects individual's privacy right.. In its aftermath, the Government of India took the first step by setting up a committee to discuss data protection and regulation. The Committee submitted its report a year later analysing the issue and making recommendations for a data protection law. The Government since has released its own draft bills, the second of which has been sent to a Joint Parliamentary Committee (**JPC**) for deliberation. The JPC is expected to submit its report before the end of the upcoming Parliamentary session.

The discussion at the event was aimed at analysing the Personal Data Protection Bill, 2019 (**Bill**) 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 Mr. Dhruv Suri, Partner at Delhi based law firm, PSA. Amongst the people who attended, there were eminent members of the tech policy space from different organizations such as MasterCard, Microsoft, IBM, Albright Stone Bridge Group, Twitter, International Association of Privacy Professionals to name a few. Representatives of the offices of Members of Parliament and members of the media were also present at the event.

Based on extensive stakeholder consultation, this report seeks to draw JPC member's attention to certain fundamental aspects of the proposed law which need closer review and revision:

1. Cross-border Data Flow and Data Localization

At the event, impact of the Bill's provisions (Clauses 33 & 34) relating to cross-border data flows were discussed extensively. Data localization is the act of storing data on any device physically present within the boundaries of a country. The term can also be used to describe any sort of restrictions on cross-border data flows. Bearing this localization scope, please see below certain key points worth JPC's consideration:

- Many attendees believe that restrictive provisions in this regard could have a negative impact on the 135 billion worth IT sector of the Indian economy. The Bill contemplates localisation of sensitive personal data and prohibits processing of critical data outside India. Sensitive personal data (Clause 2(36)) is personal data which may reveal, be related to, or constitutes financial, genetic, biometric, health, or any other category of listed out sensitive data. Literal interpretation suggests that where a personal data has the potential of disclosing sensitive data, the personal data may also qualify. For instance, a person's name and address when combined with other data can disclose her financial data such as bank accounts, credit score; and where it so happens, name and address can be argued as sensitive data. Owing to the large scope of sensitive personal data, it is possible that all personal data can be classified as sensitive data, and consequently, stored in India. Further, the Bill does not indicate what kind of data will qualify as critical data. Thus, while the Bill seems to relax the localization requirements, there is ambiguity on what data will eventually be classified as sensitive or critical data. In absence of limiting criteria for classifying further categories of sensitive and critical data, businesses will be severely impacted as they will have to constantly review data life cycle management practices and processes.

- Further, there is concern around how foreigner's data will be treated. Foreigner's data in the given context could mean personal data of a non-resident which is received in India. It is unclear if organizations will have to comply with localization requirements for such data pool. This aspect must be clarified.

- As per the present draft of the Bill, the Data Protection Authority is required to vet each individual contract that contains a clause relating to cross border data flow. Stakeholders raised concerns that if this provision is retained it would place immense pressure on the Data Protection Authority considering the amount of applications it will receive in this regard. It would also be inconvenient for companies to procure approval for each individual contract. Accordingly, it is in best interest that Data Protection Authority promulgates certain mandatory standard contractual clauses and intra-group schemes that organizations can follow for cross-border data transfer, and only in certain situations, where the organizations seek deviation, prior approval should be mandated.

- It was also recommended that provisions relating to restrictions on data flow should be applied in a tiered manner and vary based on the size of companies and their operations. Such a system would provide relief from onerous storage requirements for smaller companies such as start-ups and other SMEs.

- With regard to inclusion of financial data as sensitive personal data, it was noted that storage of financial data in India could be a red flag for many companies in the payment sector, thereby discouraging them from investing within the Indian market. It was also highlighted that other progressive jurisdictions like EU (GDPR) and Australia (Privacy Act) do not include financial data as sensitive data, but provide for separate regulations that only cater to processing of financial data. It may be worthwhile for JPC to consider excluding financial data from the Bill, and recommending its regulation as subject matter of another law.

2. Government Access to Data

The stakeholders observed that far reaching exemptions have been carved out where personal data is to be processed by state or any agency in discharge of state functions. While informational privacy is not an absolute right, it can only be curtailed by following due process of law (substantive and procedural) circumscribed by the test of proportionality. All stakeholders acknowledged that legitimate situations may arise, such as those concerning national security and integrity; however, a well-defined process with checks and balances must be laid down. Based on the present version of the Bill, if access is allowed in such a manner for the Government, the issue of privatization of surveillance may arise. With this underlying requirement, some of the Bill's provisions need to be evaluated thoroughly:

- The Bill contains a provision (Clause 35) that allows the Government or agencies authorized by it to be exempted from the provisions of this Act if it is satisfied that such exemption is "necessary or expedient" in the interest of sovereignty and integrity of India, security of State, friendly relation with foreign states, public order, and prevention of incitement or commission of offence related thereto. This proposed clause was substantially different under the 2018 bill, where it was required that such exemption for State should be authorised by law and proportionate to the objectives sought to be achieved. Without such limitation, many concerns arise as it provides the Government with unfettered access to personal data without laying down a procedure or any form of judicial oversight for the same. Stakeholders pointed out that in the absence of well-defined checks and balances this provision may be held to be unconstitutional as being violative of an individual's right to informational privacy. As such, please note that in light of *KS Puttuswamy v. Union of India* judgement, informational privacy can only be curtailed if the limitation satisfies the tests of proportionality, legality and legitimate interest. At present, there are no such procedures or rules and hence, it is imperative that Clause 35 is revised suitably to subject it to authorization under law and proportionality tests.

- The Bill also allows state and private parties to process personal data without obtaining consent or providing notice to data principal (Clause 12) where processing is in discharge of state function for provision of goods/services or grant of license and permits, compliance with any law made by the Parliament or State Legislature, or compliance with court order. The 2018 draft in the least mandated that while processing personal data under the above mentioned grounds, detailed *apriori* notice or notice within reasonable time must be provided to the data principal. This in a way ensured that the individual was informed about processing undertaken on her personal data, and this also provided the basis for her to exercise rights of confirmation and access. It is unclear why the requirement for providing notice has been done away with, and it is strongly recommended that any form of processing should be subject to notice requirement, failing which transparency and accountability cannot be ensured.

3. Processing basis

The stakeholders were concerned about consent being the primary basis of processing (Clause 11). Ample statistics and evidence suggests that "consent fatigue" or "click fatigue" is a real phenomenon where an individual does not read consent terms before giving consent. Further, it makes organization's processing cycle completely dependent on an individual's consent, which means that once consent is withdrawn, businesses do not have any right to

continue processing data. This could be extremely cumbersome and practically difficult to comply with. Stakeholders highlighted that other jurisdictions allow additional grounds for processing personal data. For instance, EU GDPR allows data controller to process personal data for (i) performance of lawful contract or carrying out steps for entering into a contract with the data subject, (ii) controller's or third party's legitimate interests, as long as such interest does not circumvent data subject's interest, freedom and rights, and (ii) processing where new purpose is compatible with the original purpose for which consent had been obtained. Due to these additional grounds, it is not always necessary to go back to the data subject for consent renewal when processing takes place. The Bill should provide for these and similar additional grounds for processing personal data.

4. Data Protection Authority

The structure, functions and composition of the Data Protection Authority as envisaged by the Bill was discussed numerous times. The change in the composition of selection committee that appoints members to the Data Protection Authority was noted as a point of concern. It replaces judicial members with those from the executive, raising concerns over the independence of the Authority and the issue of increased Governmental interference. Certain stakeholders pointed out that the DPA may inherently be toothless in its present form. Accordingly, the stakeholders believe that judicial members should be included in the selection committee. Further, it was considered that an ombudsman model should be considered to bring impartial and faster adjudication of matters under data protection laws.

5. Definition of Personal Data to include inferences

As per the Bill, the definition of personal data (Clause 2(28)) has been expanded to include inferences derived from data for the purposes of profiling. Profiling is also widely defined to mean any form of processing that analyses or predicts aspects concerning the behaviour, attributes or interests of a data principal (Clause 2(32)). Stakeholders raised concerns regarding the broad scope of personal data and profiling, which in effect could include opinions whether true of false, any analytics finding that often forms the basis for improvising provision of goods/services and many more. They raised the issue of how inferences on data are derived after investing time and capital and companies also possess intellectual property rights over such inferences. Sometimes entire business models are based on these inferences. There is also a possibility that inferences are stored in anonymised formats, in which case the regime on personal data protection should not apply. To this effect, it was observed that EU GDPR provides for a limited scope for inferences as personal data, and profiling. Profiling under EU GDPR means processing by automated mean which is done with the objective of evaluating certain personal aspects of a natural person, in particular, analyse or predict aspects concerning natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements. Thus, it is important that processing is through complete automation. Such requirement is missing in the Bill's definition. In the larger scheme, including inferences for the purposes of profiling as personal data may lead to a situation where organizations are required to store such inference in India if the government notifies them as additional categories of sensitive personal data. Therefore, it is unclear why inferences should be included and what is the harm posed to informational privacy if they are excluded. It may be prudent to exclude inferences from the scope of personal data.

6. Non Personal Data

Stakeholders acknowledged that a lot of confusion has been created by inclusion of "non-personal data" in the Bill (Clause 91). The Bill in its application clause (Clause 3) states that Bill will not apply to anonymised data, except data processed under Clause 91. Clause 91 states that Government in consultation with Data Protection Authority ca direct any fiduciary or processor to provide any anonymised data or non-personal data for better targeting and delivery of services as well as formulation of evidence-based policies. Non-personal data is defined as any data that is not personal data. Thus, in reality there is no difference between anonymised data and non-personal data. Reading it with applicability section, it appears that fiduciaries and processors may have to continue complying with the data protection requirements even after anonymisation takes place. Further, the stakeholders believe that since a special committee has been formed by the Government to deliberate on the regulation on non-personal data and the consultation process has not been completed, it was premature to place a provision that regulates non-personal data in this Bill. It was expressed that such a system would make India a hostile destination for companies that work with and capitalize on data. We firmly recommend removal of Clause 91, which should ideally be dealt under a separate law.

7. Right to be forgotten

The Bill enables a data principal to require the fiduciary to erase personal data which is no longer necessary for the purpose of processing (Clause 18(1)(d)). The right to seek erasure where necessary is a fundamental facet of data principal's autonomy over her own personal data and should be retained. This is internationally also recognised as right to be forgotten. However, the Bill seems to treat right to erasure and right to be forgotten differently. As per the Bill (Clause 20), right to be forgotten means the right to limit subsequent disclosure of data subject to prior approval of the Data Protection Authority's adjudicating officers. This in essence is a right to limit disclosure and stakeholders believe that the nomenclature should be changed suitable so as to avoid interpretation issues. In reality, it is ambiguous as to why prior approval must be obtained when a data principal wants to limit disclosure when the purpose has been achieved. It may create a situation where data principal prefers exercising right to erasure over limiting future disclosures. Bearing in mind this practicality, it is worthwhile to consider revising the right to limit disclosure.

8. Age Limit for children

As per the Bill (Clause 16), a child is considered to be a data principal below the age of 18 and there are different regulations for the same. Stakeholders felt that the age limit of 18 is rather high and inconsistent with the practices followed in other jurisdictions. As there are restrictions and conditions placed on how the data of children are to be dealt with, placing such a high age limit would make compliance cumbersome and in many cases not feasible. Stakeholders urged the Government must recognise that teenagers are a huge audience and base for many apps in the market, and such conditions would adversely affect the status quo. It is also not possible for parents to provide consent for the child at each instance.

9. Transition provision

The Bill does not provide for transition mechanism. Contrary to this, the 2018 draft provided for an elaborate timeline as to how different provisions will be notified and implemented. Please refer to Clause 97 of the 2018 draft. It was strongly urged that such timeline and transition provision should be reincorporated in the 2019 Bill.

CONCLUSION

Stakeholders welcomed the move of the Bill being sent to JPC for further consideration before passing it. They all acknowledged the importance of putting in place a sound framework that regulates and protects the data of individuals, informational privacy, interests of the industry while balancing the needs of national security. It is urged that JPC conducts an interactive consultation process, inviting comments from across the board on the 2019 Bill, as it affects a large number of stakeholders, both small and large. We at The Dialogue and PSA would be keen to work with JPC for further analysing the Bill in detail.