Government of India
Ministry of Electronics & Information Technology (MeitY)

29.01.2018

The Government of India has constituted an Expert Committee under the Chairmanship of Justice B.N. Srikrishna, Former Judge, Supreme Court of India comprising members from the Government, academia, and industry to identify and study the key issues relating to data protection in India; make specific suggestions on principles underlying a data protection framework in India; and to suggest a data protection bill.

The Expert Committee has put out a White Paper on a data protection framework for India and has sought comments from the public. Submissions of responses to the White Paper will be received till 31 January 2018, preferably through the website https://innovate.mygov.in/data-protection-in-India/.

In this regard, MeitY has also decided to conduct stakeholders' consultation meetings in various cities. The fourth stakeholders' consultation meeting was held at the Victor Menezes Convention Centre Building, IIT Bombay Campus, Powai on 23 January 2018 in Mumbai. Several key stakeholders, such as industry representatives, civil society organisations, law firms and citizens were present at this consultation, where they shared their views and opinions in relation to the various issues raised in the White Paper.

The primary concerns raised at the consultation have been summarised below:

A. Scope and Exemptions

1. Nature and Scope of 'Personal Data' and 'Sensitive Personal Data'

- A participant found traditional definition of 'personal data' involving tests of whether the data is identifiable to a person to be the only reasonable recourse. However, they did not find the classification of sensitive personal data to be meaningful as they considered it considerably easy to extrapolate sensitive personal data out of personal data. It was instead suggested that all data should be protected with adequately rigorous standards.
- In relation with concerns on corporate espionage and the enforcement of laws like insider trading rules, it was argued that the data of juristic person should also be protected.
- A suggestion was made that societal conditions in India had to be examined before determining what could be considered sensitive personal data.
- It was also argued that thorough examination was needed to assess whether financial information should be included within the purview of sensitive personal data as done under the rules under the Information Technology Act, 2000 (IT Act). It was also urged that the test for sensitive personal data should be in relation to the human body.
- It was suggested that information such as passwords were becoming increasingly irrelevant with time and that access information has been replaced with different methods for achieving access to online services.

- It was suggested that appropriate definitions for anonymized data should be put in place and that such data should not be subjected to general obligations.
- The example of location based data in market research regarding movement of persons indoors and outdoors was also discussed. Concerns were raised regarding how it could be ensured that the processing of such location based data could be permitted as long as there was no identification of the specific person. Reference was made to the use of 'hash functions' and the potential of using wi-fi addresses and computer IDs to identify a person. Another participant argued that unique machine characteristics should not be removed from the scope of personal data.
- In line with the principle of technology-neutral application of the law, it was argued that the law would have to encourage routine checks and audits to ensure that controllers/processors addressed data that could become identifiable to a person over time even if it was not so at the time of collection.
- A general suggestion came forward that apart from traditional classifications of personal and sensitive personal data, a broader examination must be undertaken to identify databases of national importance, similar to such classifications under the IT Act.

2. Data Controllers and Data Processors

- It was suggested that intermediaries as a third class of entities be recognized under a data protection law in addition to data controllers/processors.
- A suggestion was made that the law should primarily make controllers liable and should not interfere with the contractual relation between controller and processor.
- A scheme of classification of data controllers was suggested at three levels according to low, medium and high-risk. In relation with high-risk controllers, it was suggested that the means of identification of such controllers proceed on similar lines as the Basel Committee on Banking Supervision, with appropriate stress on the "interconnectedness" of databases. The effect of failure of one database on other databases was pointed to as one criteria for classification apart from general considerations like volume of data processed.

3. Exemptions

- In relation with such exemptions as national security, a participant urged that there would have to be greater transparency regarding processing by the government for surveillance purposes.
- It was argued that exemptions should not be broadly worded but that there should be, for example, more detailed explanation as to the meaning of "household" purposes. An example was given of databases created and shared within communities for matrimonial purposes and how these could be easily misused. It was urged that minimum obligations should continue to apply even in such situations.

4. Extraterritoriality, Data Localisation and Cross-Border Flow of Data

- Some participants showed general support for treaty based solutions to issues of cross-border flow of data. A few participants argued that there should not be blanket localization and particularly sensitive data alone should be localized. It was argued that if every country responds in a protectionist manner, there would be considerable

issues. It was suggested that the Committee look into the possibility of an international agreement as the appropriate solution.

- For the purposes of extraterritorial jurisdiction, one suggestion was that the link should be in relation with the citizenship of the person whose data is being processed.
- As against the above solution, a participant pointed out that it is particularly difficult to identify citizenship at the time of processing and that it would be necessary to proceed on principles of territoriality. Thus, applicability of the law should be to persons in the territory of India and enterprises conducting business in India. This would cover data collected in India but processed outside.
- Privacy framework developed by the Asia-Pacific Economic Cooperation (APEC) organization cited in relation with its discussion of cross-border flows.
- It was highlighted by one participant that data localization is a patently protectionist stance and that India should not pursue it. Another participant pointed out that global/cloud hosting enhanced competition in the industry and that data localization would prove anti-competitive.
- A participant suggested attempts to better the MLATs process instead of going for localization. In this regard, it was urged that the timelines involved in responding to requests for data should be reduced.

5. Retrospective Application of the Data Protection Law

- Doubts were raised regarding how the retrospective application of the law would function and what it would mean for the data that had already been processed or simply collected through various modes. In this regard, reference was made to the example of the one-year period provided in South African law.
- Support was generally shown for retrospective application with adequate time for compliance of previously collected data.

B. <u>Grounds of Processing, Obligation on Entities and Individual Rights</u>

A general suggestion was made that the relevant obligations of parties involved in processing activities should be listed in detail and not broadly outlined.

1. **Notice and Consent**

- Some participants suggested that consent should not be the primary ground for processing as it was not effective in ensuring effective data flow throughout society. One participant found that consent based processing was presently limited only to the giving of notice.
- Existing industry practices involving standard form collection of consent was criticised as ineffective. A suggestion was made that the solution to such issues involved better legal regulation and recognition of online agreements generally.
- It was urged that adequate guidance be provided regarding model notices. It was argued that the existence of model notices would promote predictability and those receiving such notices would be aware of what they were signing up for.
- It was suggested that issues related to consent had to be solved by unbundling consent forms such that different parts of services and different services could be negotiated separately. Similarly, another participant urged that consent would have to

be taken on the basis of different functions sought to be used (in an application, say). The example of Android's Play Store was given.

- Problems related to the bundling of consent were further highlighted and it was pointed out that a broadly applicable test on purpose specification and necessity of data could partially address this issue if applied even in situations involving consensual processing.
- Principles based on harm were argued to be more useful than consent based grounds for processing. In this regard, some participants urged examination of the APEC framework.
- It was also suggested that the law should deal with presumptions such that the default setting should be that a data subject does not want to part with data ("opt-in" framework).
- It was suggested that the "life" of consent had to be examined and consent would have to be taken regularly for continued processing if necessary (more so in the context of KYC).
- A participant highlighted practices undertaken by e-commerce businesses to enhance customer experience. It was pointed out that e-commerce websites though having the consumer and e-commerce player as the main parties, the manufacturer was also involved in the business transaction. Such manufacturers may also require information about consumers to enhance the quality of goods supplied/consumer experience. Consent to provide data onwards to manufacturers should be facilitated so that interlinkages of data in such markets can be allowed.
- Simplification of notices also suggested as a solution to relevant issues.
- A participant urged the Committee to consider practices in which a person is requested for information on dependents (wife, children etc.). It was argued that in such situations, consent obligations were difficult and that provision for the same would have to be made.

2. **Child's Consent**

- Concerns were raised regarding the ease with which the pictures of children could be collected and processed and the ubiquity of such processing e.g. for school IDs, social network registration etc.
- It was suggested that there should be a three-fold classification of children according to age ranges and differential rules should be in place regarding the consent of children in these ranges.

3. **Purpose Specification and Use Limitation**

- Highlighting concerns regarding burdens on start-ups and the like, a participant suggested that use limitation was a difficult principle to implement.
- Another participant argued that market research was an extremely beneficial objective for society and pointed out the benefits of such practices such as "mass customization" which required that market researchers and businesses returned to customers from time to time track how usage of goods and services had proceeded and gauge trends in the same. This was pointed out as different from analysis of aggregated data for useful trends and shown to require identifiability of the customer being tracked. Participant referred to this as "re-contactability".

- It was urged by some that data minimization principles should be replaced with harm based principles. This was disputed by others who felt that data minimization should be made the foundation of the law.
- It was argued by a participant that a law that was too strict could kill innovation whereas data-driven innovation was compatible with privacy as it empowered users and facilitated trust in the use of digital modes.

4. **Other Grounds of Processing**

- One suggestion was made that a general ground for processing be developed in the form of a "legitimate purpose" test and would be based on the legality, necessity and proportionality of the processing.
- Highlighting concerns regarding grounds of processing for investigation purposes, a DSCI manual on digital investigation was referred to. It was suggested that the law should adequately address the sensitivity of the data handled by police officers and the means by which it had to be secured from misuse.
- It was argued that grounds of processing (and accompanying obligations) for the government should be stricter than those for private organisations.
- Direct marketing purposes came up for discussion and it was urged that some mechanism should be in place to allow for the communication of offers to customers with the option to opt out of such further offers. Discussion was also made as to the sourcing of contact information from the public domain and such registers as club diaries.

5. **Data Retention**

- "Purging" of data when it is illegally possessed was seen to be very difficult due to the ease of flow and storage of data in the modern world. In this context, it was suggested that a 3-5 year period may be a reasonable retention duration.
- A participant sought to draw the attention of the Committee towards the data of dead persons and potential retention obligations related to the same. Another participant urged that all such situations should be dealt with through a system of nomination or automatic designation of an "heir".

6. **Individual Participation Rights**

- In relation with the right to be forgotten, it was argued by some participants that the same should be available only in relation with such issues as identity theft and the availability of sensitive personal data online. One participant argued that apart from these limited situations, deletion should only be obligatory under a court order for the same.
- A participant urged that data portability should be facilitated through a self-regulatory framework.
- The exceptions to right to access had to be clarified in the law to ensure that frivolous requests for access could be curbed. It would have to be made clear to controllers as to when requests for access could be denied.
- In contrast, another participant argued that a fee for access and rectification rights would be prohibitive and would unfairly disincentivise low-income individuals from utilizing their rights.

C. Regulation and Enforcement

1. Regulation Model, Organisational Measures and Informal Guidance

- A participant showed wholesome support for co-regulation and suggested that there should be a pyramid scheme of enforcement involving systematic escalation of disputes. Similarly, another participant argued that the law should be principles-based and further details should be fleshed out through co-regulatory development. A further participant argued that co-regulation and self-regulation models should be opted for if a command-and-control model with adequate teeth was not adopted. Yet another participant argued that a command-and-control model would be the only effective one.
- A participant argued in favour of "light-touch" regulation to allow for the slow development of rules appropriate to an evolving technology landscape. This was disputed by another participant who felt that there was enough precedent regarding the need for such principles as data minimization and that they should be adopted immediately.
- A participant suggested that in the context of data processing and obligations surrounding the same, it was essential for effective enforcement that mandatory rules be coupled with informal guidance from relevant authorities. Another participant referred to practices of providing advanced rulings.
- As part of obligations on data processors to carry out data audits, it was argued that such audits and related practices should be carried out with adequate transparency to ensure public participation and checks on the same.
- It was suggested that obligations to retain Data Protection Officers were too burdensome and costly. It was argued that there should be permission to contract with independent professionals (by a group of data controllers) for such matters instead of employing an officer. The example of chartered accountants was raised. It was urged that such an obligation should only be for high-risk processing.
- In contrast with the above, it was pointed out that digitization and automation processes have meant that various activities are becoming mechanized with no responsible person in place to ensure the protection of rights and interests. The participant urged that the law should ensure that some individuals are put in place within the framework to ensure that processes go forward responsibly instead of simply discounting liability by blaming machines.

2. Regulatory and Adjudicatory Bodies

- Existing adjudicatory framework under the IT Act was criticised as ineffective especially in relation to ensuring that compensation is made. Critics proposed greater usage of online dispute resolution mechanisms with the recognition and involvement of state authorities. This mechanism was proposed as a first-order means for resolution before other offline resolution mechanisms could be proceeded to. In relation with the question of compensation, another participant argued that a data protection fund should be put in place statutorily to ensure that there was adequate disbursal of compensation.
- On the same subject, a participant argued that it was essential for the Committee to learn from lessons from the functioning of the IT Act. This would mean that

enforcement authorities would have to be given teeth and awareness generation would have to be recognized as an important function.

- A participant argued that bodies such as MEITY should not be involved in regulation and that TDSAT would not serve as a good appellate body.
- It was argued that since the law sought to create whole new ecosystem of professionals and entities, the effectiveness of the law may depend substantially on efforts to raise awareness regarding the same.
- One participant argued that sectoral regulators should not determine granular rules.
- A participant urged the use of regulatory technology in the identification of unusual/uncharacteristic processing trends so that breaches can be better identified.

3. **Data Breaches Reporting and Notification**

- A participant argued that data breaches should be responded to with obligations for immediate measures to mitigate harm and immediate notification of data subjects.

4. **Penalties and Liability Models**

- It was argued that strict penalties were necessary to ensure compliance.
- It was urged that penalties should not be turnover based but should in fact be harm-based to be fair.
- In relation with liability for obligations, a participant discussed ex-ante and ex-post liability models. It was argued that if preventing harm was made the objective, then there could be more ex-post liability with appropriate consideration of insurance as a solution for heavy liabilities. However, it was argued that a regulatory body should have adequate ex-ante supervisory tools so as to prevent data breaches before they can happen.

D. Key Residual Issues

The following suggestions/views were also put forward:

1. A suggestion pointed towards addressing questions of privacy generally in the law instead of limiting it to personal data and informational privacy.
2. In relation with allied laws that would have to be examined, the rules on cyber cafes under the IT Act and the provisions relating to the Mental Health Act, 2017 were highlighted.
3. It was otherwise argued that the Committee should only make principle-based suggestions regarding allied laws and should not enter into a detailed examination of the same.
4. A participant argued that while processors would encrypt data to ensure privacy, the management of private keys was not done properly.
5. Though a data protection law must be technology agnostic, a participant urged statutory requirements to review rules and regulations regularly so as to keep up with changing technology.