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

Dated: 12.01.2018

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 suggest a data protection bill.

The 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, the MeitY has also decided to conduct stakeholders' consultation meetings in various cities and the first stakeholders' consultation meeting was held at the Civil Services Officers' Institute, Vinay Marg, Chanakyapuri, New Delhi on 5 January 2018. Several key stakeholders, such as, industry bodies, civil society organisations, industry representatives, academicians, law firms and citizens were present at the consultation who shared their views and opinions in relation to the various issues raised in the White Paper.

Some of the concerns raised by the participants are as follows:

A. Scope and Exemptions

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

- Need of demarcation between 'personal data' and 'sensitive personal data' under a data protection law.
- There was a discussion regarding what may be included within the purview of 'personal data' and 'sensitive personal data'. For instance, it was suggested that customer usage data (such as, locational data of an individual customer) and in certain instances, public data/data generated by Government authorities may be covered within the ambit of 'personal data'/'sensitive personal data'.

2. Entities to be defined in the law: Data Controller and Processor

- Need of distinction in law between data controllers and data processors.

3. Exemptions

- Disscussions regarding not providing any broad or blanket national security exemption.

- It was also argued by some stakeholders that certain types of sensitive personal data, such as medical records, may be made available for research purposes with consent/ or in any anonymized or pseudonymized form. However, it was argued by other stakeholders that such information should either not be collected or should not be made available as it would violate the right to privacy of the concerned individuals.

4. Data Localisation and Cross-Border Flow of Data

- There were differing opinions on the issue of data localisation.
- Certain stakeholders were of the view that data should be localized in India and cross border flow of data should be restricted to only those countries, which provide a similar level of protection as India. However, a concern was raised as to whether India has sufficient resources to assess which countries provide similar level of protection as India in relation to data.
- On the other hand, other stakeholders argued that data should not be localized in India as it will hamper innovation and growth. Further, it was argued that corporations/start-ups will incur significant costs in building local servers. In this context, it was suggested that instead of 'mandating' localization, incentives may be provided for entities to store data locally.
- Number of stakeholders highlighted that the risk of domestic surveillance may also increase if data localisation is mandated.
- It must be noted that certain stakeholders also argued that a binary approach to data localization may not be feasible; certain types of data elements (e.g. financial records) may be localized while other types of data elements need not be localized.

B. Grounds of Processing, Obligation on Entities and Individual Rights

5. Notice and Consent

- As a response to the issue of consent-fatigue, it was argued that consent as an idea should not be abandoned completely; the manner of obtaining consent may be simplified and re-designed.
- In this context, it was suggested that a layered approach to consent may be incorporated. There may be a gradation of consent depending on the degree of sensitivity of the personal data. However, it was also argued by some stakeholders that consent should always be express.
- Consent must be clear, concise and specific.
- The manner in which notice should be provided was discussed. In this context, the concept of a consent dashboard may be considered.
- Need of technical parameters to be defined which will ensure the integrity of the saved consent.
- It was suggested that the age after which parental consent may not be required for a child should be fixed at 13/15 years of age.

6. **Purpose Specification and Use Limitation**
   - While most stakeholders were of the view that data minimization should be adopted, there were concerns that conflicts between data minimization and innovation must be resolved.
   - In this regard, individuals must be apprised of the specific purpose for which their data is being collected. Moreover, the principle of purpose specification must be adopted.

7. **Individual Participation Rights**
   - There should not be a binding 'right to be forgotten'. In this context, it is important to draw a distinction between the 'right to erasure' and the 'right to be forgotten'.
   - It was suggested that there may be a fee mechanism put in place where an individual seeks to exercise a right in relation to her data (such as, right to portability, right to access, etc.) to offset the costs incurred by data controllers.

C. Regulation and Enforcement

1. It was argued by certain stakeholders that 'self-regulation' may be adopted and the law should only provide broad principles on data protection. However, it was argued that such a model may not be effective and consequently, it may be more beneficial to prescribe a 'command and control' approach to enforcement.
2. Requirements of creating codes of practices created by industry bodies in relation to various issues, such as, notice, consent, security safeguards, etc.
3. There was a discussion on the nature and type of enforcement body for data protection. It was suggested by stakeholders that the role of such a body may be that of a facilitator, or an ombudsman, or it may have powers similar to that of a privacy/information commissioner in foreign jurisdictions. It was also suggested that such a body must be involved in promoting awareness and education about data protection.
4. It was suggested that an exception may be carved out for smaller organizations/ start-ups from certain obligations under a data protection framework.
5. It was also suggested that there should be heavy fines for illegal data mining, and such matter may be adjudicated by independent data privacy tribunal .

D. Other Concerns

The following suggestions/views were also put forward:

1. The data protection legal framework may include provisions regarding encryption of data.
2. Algorithmic discrimination and bias should be appropriately addressed in such a framework.

3. Concerns were raised in relation to making the Aadhaar Act, 2016 in line with the obligations and measures (including security measures) prescribed under the data protection legal framework for India.
4. It was argued that personal data should not be equated to assets/property with the potential application of 'eminent domain' by the state.
5. The data protection legal framework should also cover the issue of 'surveillance'.
6. Concerns were raised in relation to the constitution of the Committee as not being inclusive of all relevant stakeholders.