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

19.01.2018

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 second stakeholders' consultation meeting was held at the Dr. Marri Channa Reddy HRD Institute of Telangana on 12 January 2018 in Hyderabad. Several key stakeholders, such as industry bodies, civil society organisations, industry representatives, 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.

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'

- There was an opinion that "foreign data", *i.e.* data relating to non-Indian citizens should not be included within the purview of a data protection law in India. The justification provided was that numerous foreign companies outsource certain back-office processing activities to India (usually involving only data collation and software development and no processing of personal data). It was argued that the security of this data is sufficiently protected *via* contractual obligation and provisions of foreign law, such as the Gramm Leach Bliley Act. Requiring these companies to additionally comply with an Indian data protection law would raise compliance and operation costs.
- It was suggested that damage caused by unauthorised access to biometric information could be minimised by utilising technological solutions which provide for different manifestations/distortions of the biometric information to mask user identity (cancellable biometrics).
- There was a query raised as to whether individuals' names should also be included within the purview of "personal data".
- With respect to "sensitive personal data", the following was suggested:
  - Political views and caste of an individual not be included in the definition of "sensitive personal data".
  - The definition of "sensitive personal data" and the obligations pertaining to its processing should be done in a circumspect manner.

- The existing definition of "sensitive personal data or information", as per Rule 3 of the Information Technology (Reasonable security practices and procedures and sensitive personal data or information) Rules, 2011 ("SPDI Rules") should be retained within the new data protection law.
- There was a counter view that the definition of "personal data" and "sensitive personal data" are nebulous under the current SPDI Rules and efforts should be made to clarify the existing list.
- Obligations imposed on data controllers and processors must be proportional to the purpose for which sensitive personal data is collected. For instance, an employer who collects an employee's medical information only for providing insurance should not be held to the same level of accountability as a hospital which holds and processes medical information of individuals on a regular basis.
- Unless the collection of sensitive personal information is core/integral to the primary purpose of the data controller, individuals should be given the option to choose whether such information may be collected.
- As an alternative to having a defined list of "sensitive personal information", the individual should be given the option to choose for herself the categories of information which are sensitive to her, and are therefore deserving of higher levels of protection within the data protection law. This was countered by the argument that objective standards as to what amounts to sensitive personal data are necessary for smooth enforcement of the data protection law.

2. Anonymised and Pseudonymised Data

- Anonymised data must be exempted from the purview of the data protection law. However, pseudonymised data must be included.
- There was a suggestion that any unauthorised attempt to de-anonymise data should be made punishable. This was countered by arguments made by security researchers, who claim that in certain instances, it is necessary to attempt to de-anonymise data to demonstrate that current encryption techniques/data safeguard methods are inadequate. This view is reflected in the latest amendments to the UK Data Protection Bill, 2017.
- If attempts to de-anonymise data are made punishable under the data protection law, penalties should be proportional to the attempts made to de-anonymise the data, as well as the purpose for such de-anonymisation.
- A clear definition of "encryption" and "encrypted data" must be included in the data protection law.

3. Classifying Data

- All data must be classified into appropriate categories (such as public data, confidential data, highly confidential data etc.), and tagged accordingly. This is to be done presumably with the intention of determining the levels of protection which must be accorded to the different types of data.
- The data protection law should recognise and differentiate between government use of personal data and private use of personal data.

4. Data Controllers and Data Processors

- Greater accountability must be placed on the data controller. The data processor's accountability should be limited to the terms of the contract between the data controller and processor. This suggestion was made in the light of reducing compliance burdens on smaller companies.

5. Exemptions

- Journalistic practices must be clearly defined within the data protection law.
- A specific exemption for "security researchers" must be provided (as per the UK Data Protection Bill, 2017).
- A query was raised whether independent researchers are exempt from the purview of the data protection law.
- A blanket exemption for national security should not be provided. Processing data required for national security purposes should not be exempt from audit, and should be subject to a transparent review process.

6. Data Localisation and Cross-Border Flow of Data

- Some stakeholders argued that data localisation might not be a practical approach as many companies rely on storage of data on cloud servers, which are located outside India.
- There was a view that making data localisation mandatory would make it very difficult for smaller companies to comply.

7. Retrospective application of the data protection law

- Existing data should fall within the purview of the data protection law.
- A concern was raised as to whether fresh consent would need to be obtained for data already collected.
- There was a suggestion that like the EU GDPR, a transition period of 1.5 years be granted to allow data controllers and data processors to make necessary arrangements to be able to comply with the provisions of the new data protection law.

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

8. Notice and Consent

- One view was that the level of consent required prior to collection of personal data should be made proportional to the type of data being collected (sensitive or non-sensitive). For instance, express consent ought to be obtained prior to collection of sensitive data, however less sensitive data could perhaps be collected with less stringent requirements of obtaining consent.
- With respect to improving notices, several suggestions were put forth:
  - The data protection law itself could provide samples of standard forms of notices, which could be adapted and utilised by app creators and other data controllers.
  - To improve accessibility; notices should be translated/made available in local languages. There was a counter-view that notices mandated to be available in local languages could pose

compliance burdens on companies. Options to make notices available in audio format and in pictorial format/graphical images could also be considered.

- To prevent critical terms and conditions from being obscured by legalese in notices, the most important terms and conditions should pop-up at the beginning of the notice.
- Notices should be easily readable and understandable.
- Newer methods of making notice more effective would include incorporating: (i) just-in-time notices; (ii) nutrition-label form of notices.
- At present, many apps and service providers employ a "take it or leave it" approach when it comes to obtaining consent. There was a suggestion that the data protection law could include a provision which allows the individual the option to opt-out from giving consent, while the controller continues to provide services.

9. Purpose Specification and Use Limitation

- Data protection law should specifically deal with the collection of data by mobile applications.
- The data collected by these applications exceeds what is necessary to satisfy the purpose for which it is collected. Specific written submissions have been made to this effect.

10. Data Retention

- Service providers such as LPG and telecom often collect physical documents for providing services and then digitise records. The data protection law must specify that these physical documents must be destroyed after the purpose for which they are collected is satisfied.

11. Individual Participation Rights

- Individuals should be informed once their personal data has been destroyed by the data controller/processor after its intended use is satisfied.

C. <u>Regulation and Enforcement</u>

1. It was suggested that every time an individual parts with personal data to an entity/agency, a unique ID be assigned. These unique IDs could be accessible on a common platform, to enable individuals to trace every point at which personal data has been provided to the collecting entity. This would facilitate easier tracking of data breaches, as well as assist in data governance measures.
2. Business houses could consider simplifying their codes of conduct to make them more palatable to the ordinary user.
3. Adopting the co-regulation model would be difficult and it would result in higher overheads. It would be necessary to provide tools within the law to facilitate its implementation.
4. It was recognised that ensuring that safety security safeguards in networked devices would be a difficult task for data controllers.
5. Data Breaches Reporting and Notification
   - A protocol for reporting data breaches should be followed. Data controllers must be provided a specific channel and time period through which data breaches may be addressed.
   - Data controllers and processors must be required to make mandatory disclosures of hardware and software security issues.

- It was suggested if the data breach is very minor and unlikely to cause much harm, then such breaches need not be reported immediately, to avoid panic among individuals.
- Views were sought on how to handle inadvertent data breaches. The general view was that where the data controller/processor can demonstrate that the breach took place despite taking necessary security safeguards, then the liability assigned to the organisation would be lower.

6. A point was raised that when it comes to enforcement, it is difficult to distinguish to whom data belongs (in the context of the data protection law applying to Indian citizens' data and not to foreign citizens' data).
7. The difficulty of enforcing the data protection law on companies who have no physical presence in India was recognised. It was suggested that it would be perhaps necessary to enter multilateral treaties to ensure enforcement. Another suggestion was to make some of the offences under the data protection law criminal in nature so that extradition treaties could be utilised to provide legal recourse.
8. The importance of conducting data audits was stressed upon. It was suggested that the data audit measures elaborated in United Kingdom's data protection law be examined.

D. <u>Key Residual Issues</u>

The following suggestions/views were also put forward:

1. The concept of "data ownership" is not dealt within the White Paper.
2. The White Paper only makes limited mention of "meta-data", and does not address other forms of data such as "community data" sources such as Wikipedia and whether the data protection law would apply to such data.
3. Concerns relating to surveillance and mass storage of personal data by the government in an unsecured manner were raised.
4. A query was raised as to whether personal data stored on smart devices would come within the purview of the data protection law.