Report Summary

White Paper on Data Protection Framework for India

- The Committee of Experts on a Data Protection Framework for India (Chair: Justice B. N. Srikrishna) released a white paper on November 27, 2017. The Committee was constituted in August 2017 to examine issues related to data protection, recommend methods to address them, and draft a data protection law. The objective was to ensure growth of the digital economy while keeping personal data of citizens secure and protected. The Committee sought comments on certain questions raised by it till December 31, 2017. It will draft a law for data protection in India based on the feedback it receives.
- **Principles:** The Committee suggested that a framework to protect data in the country should be based on seven principles: (i) law should be flexible to take into account changing technologies, (ii) law must apply to both government and private sector entities, (iii) consent should be genuine, informed, and meaningful, (iv) processing of data should be minimal and only for the purpose for which it is sought, (v) entities controlling the data should be accountable for any data processing, (vi) enforcement of the data protection framework should be by a high-powered statutory authority, and (vii) penalties should be adequate to discourage any wrongful acts.

Scope and exemptions under the framework

- **Applicability:** The Committee observed that countries can enforce laws within their jurisdiction. However, a single act of data processing could take place across different countries and jurisdictions. Some of the questions asked by the Committee relate to: (i) territorial applicability of the law, (ii) extent to which the law should apply outside India, and (iii) measures that should be included in the law to ensure compliance by foreign entities.
- **Definition of personal data:** The Committee noted that it is important to define what constitutes personal information. This is critical to determine the extent to which privacy of information will be guaranteed under a data protection law. It sought comments on some questions which relate to: (i) what kind of information qualifies as personal data, (ii) should the definition focus on whether a person can be identified based on the data, and (iii) treatment of sensitive personal data. Sensitive data is related to intimate matters where there is a higher expectation of privacy (e.g., caste, religion, and sexual orientation).
- **Exemptions:** The Committee noted that entities under the data protection framework may be exempt from certain obligations (e.g., certain actions taken by the state). It sought comments on the categories of exemptions that should be included under the law, and the basic safeguards that should be ensured when processing data in these categories.

Grounds for data processing, obligation on entities and rights of individuals

- **Consent:** The Committee noted that consent is treated as one of the grounds for processing personal data. However, consent is often not informed or meaningful. In this context, it sought comments on the conditions that determine valid consent. Further, it noted that one in three internet users across the world is a child under the age of 18. A data protection law must sufficiently protect their interests, while considering their vulnerability, and exposure to risks online.
- **Purpose of collection:** The Committee discussed the principle where personal data must be collected for a specified purpose, and such data should not be processed for any other purpose. Further, a related principle requires that personal data be erased once the purpose for collecting it has been met.
- **Participation rights:** The Committee noted that one of the principles of data protection is that a person whose data is being processed should be able to influence the processing. This includes the right to confirm, access, and rectify the data. The Committee observed that regulations of the European Union have recognised other rights such as the right to object to data processing. Incorporation of such rights in the Indian law requires further assessment. It also noted that the right to be forgotten has emerged as a contentious issue in data protection laws.

Regulation and enforcement

- **Enforcement models:** The Committee noted that once the provisions of the law are formalised, enforcement mechanisms must be structured to ensure compliance. In this context, it sought comments on the enforcement tools to be used for: (i) code of conduct, (ii) breach of personal data, (iii) categorisation of different data controllers, and (iv) creation of a separate data protection authority. The authority may be responsible for: (i) monitoring, enforcement and investigation, (ii) setting standards, and (iii) generating awareness.
- **Penalty and compensation:** The Committee discussed penalties for offences under the proposed law, and the authority which should have the power to hear and adjudicate complaints. Further, it noted that awarding compensation to an individual who has incurred a loss or damage due to the data controller's failure is an important remedy to be specified under the law.

Vatsal Khullar
vatsal@prsindia.org

December 1, 2017