The Indian framework on data protection

The Justice B.N. Srikrishna Committee, which has been constituted to recommend a data protection framework for the country, has come out with a White Paper for discussions. What are the similarities that exist in the White Paper and the provisions in GDPR? Shisham Priyadarshini, partner, and Shaily Soni, associate, at law firm Rajani Associates, outline the similarities. Excerpts from a note prepared by them:

Shisham Priyadarshini Shaily Soni

While privacy is considered as too amorphous for a precise definition, the term broadly connotes the right to be left alone, or freedom from intrusion. In the realm of information, privacy is the right to have some control over personal data like name, identification number, location, physical, physiological, genetic, mental, economic, cultural or social identity of any natural person.

Data security is sometimes confused for data privacy. To appreciate the difference, it is essential to understand that processing of personal or sensitive data can be categorized into collection, use and disclosure of the same. While security is necessary for protecting data, which has been collected in electronic form in any manner, privacy deals with unauthorized collection, arbitrary use and disclosure of the personal data.

In August 2017 a committee headed by Justice B. N. Srikrishna was constituted 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 presented a White Paper and has suggested a broad framework to protect data in the country.

7 PRINCIPLES

Besides raising several questions and bringing out certain pertinent points for the response of stakeholders across all fields, the White Paper lays down 7 principles on which data protection framework in India must be based. The committee is of the view that the laws need to applicable to both government and private sector entities with necessary exceptions and for all kinds of processing of data be it based in India or carried out by non-Indian entities which do not have any presence in India. It was conscious of the fact that the laws for data protection and data privacy should be flexible and should consider the changing technologies and standards of compliance, with emphasis on inexpensive to implement, and easier to enforce laws. The White Paper has also deliberated on consent as a validating mechanism for data processing and has emphasized on genuine, informed, and meaningful consent. The processing of data should be minimal and only for the purpose for which it is sought and the entities controlling the data should be accountable for any data processing.

HIGH-POWERED AUTHORITY

The committee has suggested that enforcement of the data protection framework must be by a high-powered statutory authority and any violation of obligations on part of data controller, civil penalty not merely as a sanction but as a deterrent may be imposed.

It has also analyzed the General Data Protection Regulation (GDPR) adopted by the 28-member European Union (EU). It has suggested that it is necessary to keep in mind the EU approach to protection of personal data alongside recognizing the right to privacy by the Supreme Court of India and such other legislative developments to make the Indian framework for data protection effective in the international context.

Compared to GDPR, the Information Technology Act, 2000 (IT Act) together with the Information Technology (Reasonable Security Practices and Sensitive Personal Data or Information) Rules, 2011 (Rules) are felt to be insufficient to address the issue of data privacy. Though the IT Act is being criticized, it is pertinent to note that the IT Act and Rules have few similarities to GDPR.

NEW RIGHTS TO INDIVIDUALS

GDPR introduces new rights for individuals, such as the right to data portability and also the right to be forgotten. Earlier, silence was conveniently taken as consent. The committee has highlighted that limited data portability has already been allowed in India in the context of the telecom industry but this concept needs to be applied to personal data of the individual stored with data controllers irrespective of the sector in order to provide control to the individuals over their data. The White Paper has spelled out requirement to seek genuine, informed and meaningful consent from individuals which is almost in line with the provisions of GDPR.

The White Paper also deliberates on purpose specification and use limitation but instead of putting a blanket ban on subsequent use, the use limitation principle may need to be modified on the basis of a contextual understanding of purposes and uses.

GDPR has extra territorial implication and is not only limited to the EU but extends to any entity in any country which collects, processes, manages and/ or stores personal data of data subject residing in EU. The White Paper also recognizes the borderless nature of the internet and the several jurisdictional issues in relation to data protection.

While India is on the verge of enacting a full-fledged privacy law, it has got a reference point in GDPR. The need of the hour is to ensure growth of the digital economy while keeping personal data of citizens secured and protected. This is a wake-up call for the Indian business entities. They need to be cautious while dealing with personal data not only of data subject residing in European Union but also generally.

mohan@bankingfrontiers.com