

Privacy Law in India- New Era

Unlike the EU, the US and other developed countries, Indian legal system did not place much premium on the issue of privacy and data security until recently. While the Indian judiciary had recognized that right to privacy is embodied within the right to life and liberty as enshrined in the Constitution of India, no substantive legislation was in place dealing with these issues until about a decade ago. In 2000, the Indian Parliament enacted the Information Technology Act, which inter alia provided for data safety/security measures. However, the issue of dealing with personal data (and therefore the larger issue of privacy) was largely left untouched

With the growth in India's economy over the last few years, concerns have been raised repeatedly about the absence of a proper regulatory framework governing privacy issues in India. In recent times, instances of data theft, misuse of sensitive personal data (“**SPD**”), etc have been on the rise and corporate bodies, media and activist groups have strongly advocated the need for a legislative framework. To address these concerns, the Government introduced amendments to the Information Technology Act in 2008 to protect SPD. The framework for protection of such data was further codified in the form of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (“**Rules**”) which were brought into effect on April 11, 2011.

Salient Features of the Rules

These Rules define SPD elaborately to include passwords, financial information, information pertaining to physical, psychological and mental health condition, medical records, sexual orientation, biometric information, etc. However, SPD does not include any information which is freely available or accessible in public domain.

The Rules provide for elaborate mechanism concerning collection, storage, usage and distribution of SPD. For instance, SPD may not be collected unless a prior consent of the provider of the information is obtained. A written consent has to be obtained from the provider by letter, fax or email. Prior to the collection of information, the corporate entity must also give an option to the provider to not provide the information. Prior consent is also required for disclosure of the information to any party other than the government unless the provider of the information consents to such disclosure.

The Rules make it mandatory for a corporate entity dealing with personal information of an individual, to publish a privacy policy on its website explaining its practices and policies. The corporate entity is also required to appoint a Grievance officer to enable peaceful resolution of disputes pertaining to data privacy.

The corporate entity should also ensure that the provider of the information is aware that the information is being collected, the purpose of use of the information, the recipients of the

information and the name and address of any third party agency either collecting and/or dealing with such information.

The personal information can be used only for the purpose for which it is collected. Also, it cannot be retained by the corporate entity for longer than is required and only for lawful purposes.

The Rules also impose restrictions on transfer and disclosure of SPD by the corporate entity. Transfer of SPD can be done only if the transferee company has the same level of data protection. Further, such transfer is permitted only if it is necessary for the performance of a lawful contract between the corporate entity and the provider of information or where the provider consents to such transfer.

Under these Rules, a corporate entity is considered to have complied with reasonable security practices if they have implemented a program having comprehensive documented information that ensures data protection. The Rules state that the corporate entity can have the International Standard IS/ISO/IEC 27001 as its data security program. Any other security program would have to be approved by a Government-appointed agency which is yet to be appointed. An audit of the security program has to be undertaken through an independent auditor annually and on each occasion of upgradation.

A Critical Analysis

By implementation of the Rules, India has taken a step in the right direction in so far as privacy issues are concerned. As stated above, the Rules seek to provide for elaborate mechanism for collection, use, etc of SPD. It is however, pertinent to note that the Rules fall short on certain critical aspects. By way of illustration, the Rules are silent regarding the procedure to be followed in the event a complainant is not satisfied with the decision of the Grievance Officer. On the basic issue of the SPD, the Rules do not address a situation where data collected by a corporate entity may not be by itself sufficient to identify the provider of information although the said provider can be identified by using another set of data in conjunction with the SPD. For instance, in case of a clinical trial, the information of the patients received by the investigator is in a codified form in order to conduct an unbiased trial. Thus, the investigator cannot track the information of the patient unless required in specific scenarios. The Rules do not address a situation like this.

In context of data security program, the provision in the Rules is somewhat ambiguous. Firstly, the language does not seem to suggest that a corporate entity is mandatorily required to have its data security program certified either under the ISO standard or by the Government-appointed agency. Secondly, even assuming that if it is mandatory to have such program duly certified, it is not clear whether besides the options mentioned in the Rules (ISO standard or approval by Government-appointed agency), the corporate entity can opt for any third party method of certification.

Regarding the issue of transfer of SPD, the Rules provide that the transferee company must have the same level of data protection as that of the transferor company. From a practical perspective, such standard could be onerous and also difficult to monitor specially in the context of a cross-border transfer of SPD.

These Rules will have an impact on all businesses, most particularly on multinational companies. Multinational companies tend to maintain centralized databases of information about their businesses all over the world including information about employees, third party contractors and their customers. Thus, multinational companies holding such centralized databases would have to adhere to these Rules. Additionally, these Rules shall also have an impact on the outsourcing industry. Entities in India to which SPD is outsourced may have to adhere to these Rules.

Conclusion

As a major player in today's world economy and an IT hub, India needs more than ever before a comprehensive strategy for protection of privacy, sensitive personal data and its use. While the introduction of Rules is clearly laudable, the legal regime has a long way to go before adequate standards are in place for privacy and data security. It seems that the Government is sensitive enough to this issue and the Right to Privacy Bill 2011 is currently under consideration. Corporates and the legal fraternity are therefore looking forward to emerging issues on privacy laws in India with much anticipation.

In case of any queries please send them to:-

Rajarshi Chakrabarti

rajarshi@mumbai.kochhar.com

Ankita Wagle

ankita@mumbai.kochhar.com