

Notification of the Rules with respect to Protection of Sensitive Personal Data and Information under the Information Technology Act, 2000

Reema Patil¹

The Government of India recently notified the “*Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Information) Rules, 2011*” (the “**Rules**”) under Section 43-A of the Information Technology Act, 2000 (the “**IT Act**”). The Rules are in effect from April 11, 2011. The Rules have to be read with Section 43-A of the IT Act which deals with a body corporate possessing, dealing or handling sensitive personal data or information. With the notification of the Rules, we can see that India is slowly trying to draw certain principles from the European Union which follows two (2) main directives on data protection. What this note seeks to do is to compare EU’s Data Protection Directive (Directive 95/46/EC) (the “**EU Directive**”) to the Rules and see how far the Rules have followed the EU Directive.

Section 43-A of the IT Act deals states that “*where a body corporate possessing, dealing or handling any sensitive personal data or information in a computer resource which it owns, controls or operates, is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.*”

A body corporate under the IT Act has been defined as any company including a firm, sole proprietorship or other association of individuals which are engaged in commercial or professional activities. Section 43-A did not define what exactly constitutes “sensitive personal data or information.” The Rules define “Personal information” to mean any information that relates to a natural person, which, either directly or indirectly, in combination with other information available or likely to be available with a body corporate, which is capable of identifying such person. Further, “sensitive personal data or information” has been defined as personal information which consists of the following information:

- (i) password;
- (ii) user details as provided at the time of registration or thereafter;
- (iii) information related to financial information such as bank account /credit card / debit card / other payment instrument details of the users;
- (iv) physiological and mental health conditions;
- (v) medical records and history;
- (vi) Biometric Information; (defined term under the IT Act)
- (vii) information received by body corporate for processing, stored or processed under lawful contract or otherwise;
- (viii) Call Data Records (defined term under the IT Act).

The Rules specifically exclude from the definition of “sensitive personal data or information” any information that is freely available or accessible in public domain or accessible under the Right to Information Act, 2005.

The EU Directive applies to “*any operation or set of operations which is performed upon personal data,*” called “*processing*” of data. “Personal Data” has been defined to mean any information relating to an identified or identifiable natural person; an “identifiable natural person” is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. We can see that the definition of “Personal information” under the Rules and the definition of the “Personal Data” under the EU Directive mirror each other. The term “*processing of personal data*” under the EU Directive has been defined as any operation or set of operations which is performed upon personal data, whether or not by automatic means such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, discrimination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Privacy Policy

Rule 4 states that a body corporate has to provide a policy for privacy and disclosure of information. It states that a body corporate or any person who on behalf of a body corporate collects, receives, possesses, stores, deals or handles information of a provider of information, has to provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information and ensure that such privacy policy is available for view by such providers of information who have provided such information under lawful contract. The privacy policy has to be published on the website of the body corporate or any person on its behalf. The privacy policy has to provide for:

- (i) clear and easily accessible statements of its practices and policies;
- (ii) type of personal or sensitive personal data or information collected;
- (iii) purpose of collection and usage of such information;
- (iv) disclosure of information including sensitive personal data or information as provided in Rule 6; and
- (v) reasonable security practices and procedures as provided under Rule 8.

Collection of Information

Rule 5 deals with respect to the collection of sensitive personal data or information. It states *inter alia* that a body corporate has to first obtain consent in writing through letter or fax or email from the provider of such information regarding purpose of usage before collection of such information. Article 7(a) of the EU Directive reflects the same principle as it states that personal data may be processed only if the data subject has unambiguously given his consent to the same. Further, under Rule 5, there are certain rights given to the provider of information and certain obligations placed on the body corporate collecting such information. The provider of information should be allowed to modify such information as and when necessary and he must have the option to opt-in and opt-out of providing such information. While collecting such information, the body corporate:

- (i) has to ensure that there is a necessity and a lawful purpose for which information is being collected;

- (ii) has to ensure that the provider of information is aware that information is being collected, the purpose for which it being collected, the intended recipients, name and address of the agency collecting and holding the information;
- (iii) cannot hold information longer than necessary;
- (iv) has to ensure that information has to be used for the purpose it was collected;
- (v) has to keep information secure; and
- (vi) address discrepancies/grievances in a time bound manner.

The above obligations placed on the body corporate seem to have been derived from the obligations placed on member states of the EU while processing personal data. Similar obligations have been set out in Article 6 of the EU Directive which are summarized below:

Personal data must be:

- (i) processed fairly and lawfully;
- (ii) collected for specified, explicit and legitimate purposes and not further processed in a way incompatible with those purposes;
- (iii) adequate, relevant and not excessive in relation to the purposes for which they are collected and/or further processed;
- (iv) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that data which are inaccurate or incomplete, having regard to the purposes for which they were collected or for which they are further processed, are erased or rectified;
- (v) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the data were collected or for which they are further processed.

Article 8 of the EU Directive states that processing of personal data which reveals racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership and the processing of data concerning health or sex life is prohibited except under certain specific circumstances. However, the Rules do not distinguish such information and has also included physiological, mental health conditions and medical records under the definition of sensitive personal data or information.

Disclosure of Information

Rule 6 states that prior permission of the provider of information has to be obtained by the body corporate before disclosure is made to a third party and any third party receiving such information is not entitled to disclose it further. This Rule is in line with Article 6(b) of the EU Directive which states that personal data collected for specified, explicit and legitimate purposes and *not further processed* in a way incompatible with the purpose for which such information was gathered.

Rule 6 also states that body corporates however shall be obliged to share such information without obtaining prior consent from provider of information, with Government agencies mandated under the law to obtain information including sensitive personal data or information for the purpose of verification of identity, or for prevention, detection, investigation

including cyber incidents, prosecution, and punishment of offences. Further, the Government agency has to send a request in writing to the body corporate possessing such sensitive personal data or information stating clearly the purpose of seeking such information. The Government agency is also under an obligation to state that the information so obtained will not be published or shared with any other person. Rule 6 further states that any sensitive personal data or information shall be disclosed to *any* third party by *an order under the law for the time being in force*. The EU Directive also lays down exemptions which restrict the rights provided under the EU Directive to data subjects. The circumstances under which these exemptions can be exercised are far more restrictive and specific when compared the Rules which allows for a disclosure by “an order under the law for the time being in force”. The EU Directive, under Article 13, states that Member States have been granted the right to restrict the scope of the obligations and rights provided when such restrictions constitute necessary measures to safeguard:

- (i) national security;
- (ii) defence;
- (iii) public security;
- (iv) the prevention, investigation, detection and prosecution of criminal offences, or of breaches of ethics for regulated professions;
- (v) an important economic or financial interest of a Member State or of the European Union, including monetary, budgetary and taxation matters;
- (vi) a monitoring, inspection or regulatory function connected, even occasionally, with the exercise of official authority in cases referred to in (iii), (iv) and (v);
- (vii) the protection of the data subject or of the rights and freedoms of others.

Transfer of Information

The EU Directive, under Article 25 allows for the transfer of personal data to third countries, *provided however that*, such third country to whom such personal data is being transferred to also ensures an adequate level of data protection. What would be considered as an “adequate level of protection” would be assessed in the light of all the circumstances surrounding a data transfer operation or set of data transfer operations; particular consideration being given to the nature of the data, the purpose and the duration of the proposed processing operation or operations, the country of origin and the country of final destination, the rules of law, both general and sectoral, in force in such third country in question and the professional rules and security measures which are complied within that country.

A similar provision has been provided for under the Rule 7 with regard to transfer of data within India or outside. A body corporate or any person on its behalf may transfer sensitive personal data or information including any information, to any other body corporate or a person in India, or located in any other country, that ensures the same level of data protection that is adhered to by the body corporate as provided for under Rule 7. This provision lays an obligation on the transferor of the information to ensure that the recipient of such information also adheres to data protection levels as set out in the Rules. Rule 7 also states that the transfer may be allowed only if it is necessary for the performance of the lawful contract between the body corporate or any person on its behalf and provider of information or where such person has consented to data transfer.

Reasonable Security Practices and Procedures

Rule 8 states that a body corporate or a person on its behalf shall be considered to have complied with *reasonable security practices and procedures*, if they have implemented such security practices and standards and have a comprehensive documented information security programme and information security policies that contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business. “Reasonable security practices and procedures” has been defined in the explanation of Section 43-A to mean “security practices and procedures designed to protect such information from unauthorized access, damage, use, modification, disclosure or impairment, as may be specified in an agreement between the parties, or as may be specified in any law for the time being in force, and in the absence of such agreement or any law, such reasonable security practices and procedures, as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.”

Rule 8 further states that the international Standard IS/ISO/IEC 27001 on “Information Technology - Security Techniques - Information Security Management System – Requirements” is one such standard referred to in sub-rule (1). However, the parties are free follow any other best code practices other than IS/ISO/IEC 27001, but the same needs to be approved by the Central Government through any industry body or entity formed by such an association, whose members are self regulating. A body corporate or a person on its behalf who has implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified under sub-rule (3) shall be deemed to have complied with reasonable security practices and procedures provided that such standard or the codes of best practices have been certified or audited on a regular basis by entities through independent auditor, duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried out by an auditor at least once a year or as and when the body corporate or a person on its behalf undertake significant upgradation of its process and computer resource.

Consequences of Non-compliance

Civil Remedy:

Section 43-A lays down that a body corporate who is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such body corporate shall be liable to pay damages by way of compensation to the person so affected.

Criminal Proceedings:

In addition to being liable under Section 43-A, a body corporate will be liable under Section 72-A of the IT Act which provides for punishment for disclosure of information in breach of lawful contract. Section 72-A provides that any person, while providing services under

the terms of a lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to another person, shall be punished with imprisonment for a term which may extend to three (3) years, or with fine which may extend to five (5) lakh rupees, or with both.

Conclusion

With the coming into force of the Rules, India now has legislation that governs the protection of sensitive personal data and information. Interestingly however, while the Rules are in force, there is no prescribed period within which body corporates need to implement the prescribed security practices and procedures with respect to protecting sensitive personal data and information. While it is commendable that India is trying to keep its pace with the rest of the world in respect to its data protection laws, body corporates will now have to establish security procedures to be in compliance with these Rules, keeping in mind the costs that will be incurred in the process of establishing the same.

ⁱ *Reema Patil is an Associate at Narasappa, Doraswamy & Raja, an Indian law firm that specializes in corporate and commercial laws. The views of the author are personal and do not reflect the views of the firm.*