APPLICABILITY – THE RULES APPLY TO ALL BODY CORPORATES

May 2011

Applicability

The Rules apply to all body corporates that collect and use personal data and information in India, including the intermediaries acting on their behalf. Section 2(w) of the Act defines intermediary as a person that receives, stores or transmits electronic records on behalf of another person and includes telecom/network/internet/web-hosting service provider, the search engines, online payment, online auction and online market places, and cyber cafes. It does not apply only to Indian citizens or residents or body corporate, but to any personal information collected within or outside India by body corporates.

Data

The Act in section 2(o) defines "data" as information, knowledge, facts, concepts or restrictions prepared and processed in a computer system/network in any form, including computer printouts, magnetic or optical storage media, punched cards, punched tapes or stored internally in the memory of the computer. The Rules, however, provide an inclusive definition of "sensitive personal data or information." These are the personal information relating to password, finance, physical, physiological and mental health condition, sexual orientation, medical records and history and biometric information. It also includes the information received by a body corporate for providing service, and/or processing, storing under a lawful contract or otherwise. This definition has exempted all information freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law.

Obligations of body corporates

The various obligations of body corporates are as under:

1. To provide a policy for privacy and disclosure of information. This policy should be clear, easily accessible, and complete, prominently published on their website and provide for the type of personal information to be collected, its purposes and usage. The reasonable security practices and procedures should also be outlined.

2. To procure consent in writing (through letter, fax or e-mail) from the provider of information ("Provider") and ensure that the Provider is also given an option to not provide the information. As consent is

the basis of collecting information, Provider has the option to opt-in or opt-out at any time along with the option to review and modify the information, whenever necessary.

3. To collect sensitive personal information only when it is to be used for lawful purpose and considered necessary for the purpose for which it is collected. The process of collection should be transparent and the necessity of collection be stated. Provider should be given the details of the intended recipients and name and address of agency collecting and/or retaining the information.

4. To not retain information longer than required for the purpose for which it is collected.

5. To address any discrepancy and grievance of the Provider and designate a grievance officer within one month of the receipt of any grievance. It is essential to note here that the body corporate shall not be responsible for the authenticity of the information supplied by the Provider.

6. To share, without obtaining prior consent from the Provider, with government agencies mandated under the law and to any third party by an order under the law. The third party receiving information has the obligation to not disclose it further. The Information Technology (Procedure and Safeguards for Interception, Monitoring and Decryption of Information) Rules, 2009 also provides for a comprehensive framework for the disclosure of information.

7. To transfer sensitive personal data to any other body corporate or person in any country that ensures the same level of data protection as provided under Rules provided it is necessary for the performance of the lawful contract between the body corporate and Provider or where such person has consented to data transfer.

8. To comply with reasonable security practices and implement standards containing managerial, technical, operational and physical security control measures commensurate to the information assets protected with the nature of business. The Rules prescribes to follow either – (i) international standard IS/ISO/IEC 27001 on “Information Technology – Security Techniques – Information Security Management System – Requirements.”; (ii) code of best practices by industry association for self-regulated industries; and (iii) a certified standard implemented by the body corporate. This must have been certified or audited on a regular basis by entities through independent auditors, approved by the government, at least once a year or as and when the body corporate is upgrading its processes and computer resource.

Indeed, corporations have the highest incentives for securing and protecting data as breach will impact their brand image and lead to loss of trust. Notable mentioning here is the national encryption policy being developed by the Department of Information Technology[1]which will ensure more protection to data by providing encryption limits for private entities and even industry-wise. However, it will also raise the concern regarding the government depository of decryption keys as it involves huge confidence issues between the government, private parties and end users.

Penalties

Any failure to implement the Rules will be construed as negligence on part of the body corporate making it liable under section 43A of the Act. In the event of a security breach, a body corporate has to demonstrate that it complied with the Rules and the data security practices were commensurate with the assets being

protected. The Act provides for a penalty of up to 2 years imprisonment or a fine up to INR 100,000 (US$2,200 approx where 1 US$ = INR 44.8) or both for breach of confidentiality and privacy as under sections 72 and 72A of the Act. Even the directors can be held liable unless they can prove that breach was without their knowledge and/or they acted to prevent the breach. Service providers who disclose information in breach of a lawful contract are subject to penalties that include up to 3 years imprisonment or a fine of up to INR 200,000 (US$4,400 approx) or both.

Intermediaries Guidelines

An intermediary has to observe certain due diligence while discharging its duties. Like a corporation is required to publish the rules and regulations and privacy policy and user agreement. Intermediary is prohibited to host, display, upload, modify, publish, transmit, update or share any information that is harmful, obscene, harm minors, infringes IPRs, violates law, impersonates any person, contains viruses, threatens unity, integrity or defence or security of India, among others. This covers extremely broad area without giving proper clarifications regarding each of the specific words or phrases being used. If such information is stored, hosted or published in an intermediary's computer system and the affected person writes about such information, it has to act within 36 hours and disable such information. Apart from maintaining records, an intermediary has to strictly abide by the Act and assist government agencies in any investigation, protection or cyber security activity. Furthermore, the intermediary must report the cyber security incidents with the Indian Computer Emergency Response Team (CERT-In) as provided for under section 70B of the Act and publish the mechanism to notify complaints to the grievance officer who must redress the complaints within one month.

PSA view – One of the most crucial aspects in the Rules is the dissemination of information to third parties. In the Peoples Union for Civil Liberties v. Union of India,[2] the Supreme Court had provided guidelines for telephone tapping which led to the insertion of Rule 419A in the Telegraph Rules. The Interception Rules of 2009 was based on this Rule 419A. The Rules has widened the scope of sharing information and has eliminated limitations under the Interception Rules as it contemplates information sharing with government agency and the reciprocal prohibitions for unauthorized disclosures are missing.

In any event, pursuant to the Rules, while handling sensitive personal information, corporations and intermediaries have to ensure that they conform to the Rules. In cases of a contractual relationship with the Provider, they should additionally observe the restrictions of the contract. To follow reasonable security obligation, they can also adopt the Information Technology Security Guidelines set out in Schedule II of the Information Technology (Certifying Authorities) Rules, 2000 which is amenable to Indian situations. They should have in place reasonable security practices requiring protection of sensitive personal information from unauthorized access, damage, use, modification, and disclosure or impairment. The crucial point to be noted here is the applicability of the Act to any violation committed outside India by any person, which imposes stringent obligations upon corporations to ensure protection of data.

By:

Priti Suri
Neeraj Dubey

SITEMAP | CONTACT US