Technology Law Analysis

June 18, 2011

GOVERNMENT NOTIFIES RULES WITH RESPECT TO PROTECTION OF DATA UNDER THE INFORMATION TECHNOLOGY ACT, 2000

The Government of India recently notified the "*Reasonable security practices and procedures and sensitive personal data or information Rules, 2011"* ("**Rules**") under Section 43A of the Information Technology Act, 2000 ("**ITA**"). These Rules have been made effective from **April 11, 2011**. Earlier, in October 27, 2009 the Parliament inserted Section 43A in the ITA, which addressed issues in relation to data security and privacy but its implementation was not effective till the notification of the current Rules.

Section 43A of the ITA *inter alia* deals with protection of data in electronic medium[1] by providing that when an body corporate[2] is negligent in implementing and maintaining *'reasonable security practices and procedures'* in relation to any '*sensitive personal data or information'* which it possesses, deals or handles in a computer resource which it owns, controls or operates and such negligence causes wrongful loss or wrongful gain to any person, **such entity shall be liable to pay damages by way of compensation to the person so affected**.

The expressions '*sensitive personal data or information'* and '*reasonable security practices and procedures'* were not defined in the ITA, but are now defined in the Rules.

Thus, going forward, outsourcing companies / banks / business captives and any other companies who deal, posses or handle personal information and/ or sensitive personal data shall need to adhere to these Rules.

In the below analysis, we have discussed the nature of information the Rules intend to protect and the mechanism contemplated by the Government for the same.

THE SCOPE OF THE RULES

Section 43A applies to data or information "in a computer resource". The Rules do not apply to information in the purely physical domain e.g. when information (whether or not such information is sensitive or personal) is collected in physical form and is not processed in / stored in / transmitted through an electronic/ computer media.

The Rules define "Personal Information and "Sensitive personal data or information" to mean as follows:

· "Personal Information" means 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, is capable of identifying such person

· "Sensitive personal data or information" means such personal information which consists of information relating to;—

(i) password;

(ii) financial information such as Bank account or credit card or debit card or other payment instrument details ;

(iii) physical, physiological and mental health condition;

(iv) sexual orientation;

(v) medical records and history;

(vi) Biometric information;

(vii) any detail relating to the above clauses as provided to body corporate for providing service; and

(viii) any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise.

Any information that is freely available or accessible in public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force is not to be regarded as sensitive personal data or information.

ANALYSIS:

The definition of 'personal information' is wider than 'sensitive personal data or information' (SPDI). The definition of SPDI is in the nature of an exhaustive list of items. Hence, no other information apart from the one listed above, would be considered as SPDI. It is interesting to note that Section 43A only included SPDI within its ambit, but some of its provisions of the Rules have been made applicable to 'Personal Information'.

It is pertinent to note that these Rules apply to personal information irrespective of the nationality of the provider of the information; thus information provided not only by Indian nationals but also by nationals in different jurisdictions, whose information is stored, dealt or handled by a corporate entity in a computer resource in India would attract the provisions

Research Papers

FAQs on Setting Up of Offices in India
December 13, 2024

FAQs on Downstream Investment
December 13, 2024

Gaming Law 2024
December 12, 2024

Research Articles

The Revolution Realized: Bitcoin's Triumph
December 05, 2024

The Bitcoin Effect
November 14, 2024

Acquirers Beware: Indian Merger Control Regime Revamped!
September 15, 2024

Audio

Securities Market Regulator's Continued Quest Against "Unfiltered" Financial Advice
December 18, 2024

Digital Lending - Part 1 - What's New with NBFC P2Ps
November 19, 2024

Renewable Roadmap: Budget 2024 and Beyond - Part I
August 26, 2024

NDA Connect

Connect with us at events, conferences and seminars.

NDA Hotline

Click here to view Hotline archives.

Video

"Investment return is not enough" Nishith Desai with Nikunj Dalmia (ET Now) at FII8 event in Riyadh
October 31, 2024

Analysing SEBI's Consultation Paper on Simplification of registration for FPIs

of the ITA. The applicability is driven by the location of computer resource in India, as can be seen from the wording of Section 43A of the ITA read with the Rules.

These Rules will also be applicable in circumstances where the information is collected in India and is transferred to any computer resource outside India and also in cases where the information is neither collected nor stored in India, but is dealt with or handled in India e.g. even accessed from India. Thus, typical outsourcing businesses where *personal information* of foreign nationals is transferred to Indian entity(ies) who deal or handle such information, would henceforth attract the provisions of the ITA.

MECHANISM FOR PROTECTION OF PERSONAL INFORMATION AND SENSITIVE PERSONAL DATA OR INFORMATION.

Type of Data	Applicability / Requirement	Analysis
· Personal Information · Sensitive Personal Data Or Information	***PRIVACY POLICY*** [3] The body corporate or a person who on the behalf of the body corporate collects, store, deals, or handles *Personal Information and SPDI* is required to have a privacy policy in place to protect such information. Such privacy policy should be available for review by the provider of the information and should be accessible on the website of the body corporate or the person who is acting on its behalf. The privacy policy should clearly state the following: 1. Clear and accessible statement relating to practices and procedure; 2. If Sensitive Personal Information or Data is collected; 3. Purpose and usage of collection of such information; 4. Disclosure of information to third parties; 5. Reasonable security practices or procedures.	Though the drafting of the provision is slightly vague, it appears that the intention is to apply to the requirement of having the privacy policy only in situations where Personal Information and SPDI are collected. The entities that collect, store, deal or handle such information would have to adhere to these Rules, if the computer resource that is involved is located in India. Thus, outsourcing entities that deal or handle the data that is collected abroad will also have to adhere to this Rule.
· Sensitive Personal Data Or Information	***COLLECTION OF INFORMATION*** [4] **I. Option:** A body corporate before collecting SPDI is required to provide an option to the provider to provide such information **II. Consent**: The body corporate is required to obtain a ***written consent*** from the provider via a letter, fax or email. **III. Right to withdraw**: The provider has the discretion to withdraw his consent through a written letter at any time while availing the services of the body	Though not specified, we believe that in keeping with the spirit of the IT Act, written consent and the written withdrawal obtained through a click through mechanism in the electronic medium should be construed as letter for the purpose of this Rule.

September 26, 2024

Scope of judicial interference and inquiry in an application for appointment of arbitrator under the (Indian) Arbitration and Conciliation Act, 1996

September 22, 2024

corporate. However, in case of withdrawal, the body corporate has the discretion to withdraw the services for which the SDPI was sought.	
IV. Knowledge to be Provided to Users: A body corporate while collecting information, should take such steps as are, in the circumstances, reasonable to ensure that the provider has the knowledge of: (a) the fact that the information is being collected; (b) the purpose for which the information is being collected; (c) the intended recipients of the information; and (d) the name and address of — · the agency that is collecting the information; · the agency that will retain the information	The Rules do not lay down what would be considered to be reasonable steps which a company should undertake. We believe that, compliance of this provision may be accomplished if the information is made part of the Privacy Policy (discussed earlier) and the same is made known to the provider at the time he discloses such information. For the purpose of the same, companies would need to maintain the information in such a manner / medium which is easily retraceable as and when desired by the provider.
V. Use of Information: Body corporate can only use the SPDI for the purpose for which it was collected and retain such information only till such SPDI is necessary for the purpose sought.	
VI. Review: Body corporate would need to permit the provider, as and when requested by them, to review the information they had provided and ensure that any such information found to be inaccurate or deficient shall be corrected or amended as feasible	
VII. Authenticity of User Information*:* Body corporate is not be responsible for the authenticity of the SPDI supplied by the provider. **VIII. Grievance:** Body corporate would need to address any discrepancies and grievances of the provider with respect to processing of information in a time bound manner. For this purpose, body corporate would have to designate a Grievance Officer and publish his name and contact details on its website. The Grievance Officer needs to redress the grievances expeditiously but within one month from the date of receipt of grievance.	Henceforth, not only would there be a requirement of a designated Grievance Officer but the company would also need to provide his / her name and contact details. Moreover, the company would need to provide an immediate replacement in the event the designated Grievance Officer leaves the employment of the company or is substituted by the company.

General Analysis of Rule 5 - *The Rules lay down a higher degree of care and liability for collection of SPDI. It should be noted that under Rule 5, the terms 'information*[5]*, 'Personal Information' and 'SPDI' have been used in different sub clauses; these three terms have different meanings and implications. It is not clear whether the legislature indeed intended to make distinction in application of various sub-rules of Rule 5 to different set of information. Keeping in mind the fact that the requirements and compliances under Rule 5 are considerably onerous, it is possible that it was the intent of the legislature to apply the provisions of Rule 5 to only SPDI. Having said that, as the Rules have only been recently been notified, they are still untested and we await any further clarification from the Government of India* *In case of outsourcing arrangements, where the data is collected abroad and is delivered to or accessed through computer resource in India, this provision will have to be adhered to. It is not clear how this Rule will be applicable when the data was collected before April 11, 2011 but delivered in India post that date.*		
· Sensitive Personal Data Or Information	***DISCLOSURE AND TRANSFER OF SENSITIVE PERSONAL DATA OR INFORMATION***[6] Disclosure of SPDI to a third party shall require prior written approval of the provider unless such disclosure has been agreed to in the contract between the body corporate and provider of information. The exception(s) where prior permission shall not be required before disclosure are - (a) Where disclosure is necessary to be in compliance with law; or (b) where disclosure is necessary for government agencies mandated under law to procure such information. A body corporate may transfer SPDI to any other body corporate or a person in India or abroad that ensures the same level of data protection that is adhered to by the body corporate as provided for under the Rules. 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.	In most contracts where it is likely that SPDI may be transferred, it is typical to have detailed provisions regarding the standard of confidentiality to be maintained and the exceptions thereto. What is relevant about this provision is the *necessity of ensuring* that an entity to whom SPDI is being transferred adheres to data protection levels as set out in the Rules. While the use of the term 'ensure' is important in that it casts an absolute obligation. The Rules do not specify how this obligation is to be satisfied and whether there are any safe harbours. For e.g: it is not clear whether taking a contractual; representation to this effect from the transferee would suffice or if the transferor has to undertake a detailed due diligence exercise to ensure compliance with this provision.
· Personal Information · Sensitive Personal Data Or Information	***REASONABLE SECURITY PRACTICES AND PROCEDURES***[7] Body corporate needs to comply with 'reasonable security practices and procedures' Section 43A defined	Section 43A was very clear in providing that if the agreement between the parties specify the security policies and procedures, then the same would govern. However, the wording of Rule 8 brings in ambiguity as . It is not clear whether despite having security guidelines agreed to in a contract between the contracting parties, it now becomes necessary to also have and

	"*Reasonable security practices and procedures*" to mean security practices designed to protect 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 · In the absence of such agreement or law, such reasonable security practice as may be prescribed by the Central Government. Through the Rules the Government has (a) Stated that an entity shall be deemed to have complied with the reasonable security practices and procedures where it implements such practices and procedures and has a comprehensive documented information security programme and information security policies that contain managerial, technical operational and physical security measures that are commensurate with the assets being protected. (b) Prescribed the International Standard IS/ISO/IEC 27001 on "*Information Technology - Security Techniques - Information Security Management System - Requirements*" as one of the standards which may be followed by entities in implementing security practices and procedures. However, the parties can follow any other best code practices other than IS/ISO/IEC 27001, but the same which needs to be approved by the Central Government through any industry body or entity formed by such an association, whose members are self regulating. (c) Prescribed that entities that implement IS/ISO/IEC 27001 or similar best practices are to be audited on a regular basis by an independent auditor approved by the Central Government, such a audit should be carried out at least once a year.	implement the security programme referred to in point (a) or whether such security programme is in lieu of a contractual arrangement. · It is not clear whether the IS/ISO/IEC 27001 is intended to be a minimum threshold for security standards to be adopted by entities.

CONCLUSION

Being the only Indian statute which specifically addresses personal information/data security, the industry had welcomed the progressive amendments made to the IT Act in the year 2009, which introduced Section 43A. After notification of the Rules however, concerns have been raised about their implementation.

Section 43A of the Act punishes a body corporate that is negligent in implementing / maintaining reasonable security practices while possessing, dealing or handling sensitive personal data or information in a computer resource which it owns, controls or operates and whereby such negligence causes wrongful loss or wrongful gain to any person.

The Rules, apart from specifying reasonable security practices and procedures, have also specified additional compliance requirements. It may be argued that these additional compliances are beyond the purview of Section 43A and therefore, for non-compliance penalty under Section 43A should not apply. Further, the operative part of Section 43A is linked with a negligent act which causes wrongful loss or wrongful gain to any person. Thus unless there is any wrongful loss or wrongful gain to any person, sanction under Section 43A would not get attracted.

Although the Rules are reformatory, they leave certain room for interpretation and it is hoped that the Government will soon come out with some clarification(s) to throw light on the existing discrepancies as discussed in the above analysis.

- Tech Team

_____

1 Section 43A of ITA. Compensation for failure to protect data 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, not exceeding five crore rupees, to the person so affected.

Explanation: For the purposes of this section

(i) "body corporate" means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities

(ii) "reasonable security practices and procedures" means security practices and procedures designed to protect such information from unauthorised 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.

(iii) "sensitive personal data or information" means such personal information as may be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

2 A company includes a firm, sole proprietorship, association of individuals engaged in commercial or professional activities. The definition of body corporate specifically excludes

3 Part 4 of the Data Protection Rules

4 Part 5 of the Data Protection Rules

5 Information is defined under the IT Act as : *"information" includes data, message, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche"*

6 Part 6 and 7 of the Data Protection Rules

7 Part 8 of the Data Protection Rules