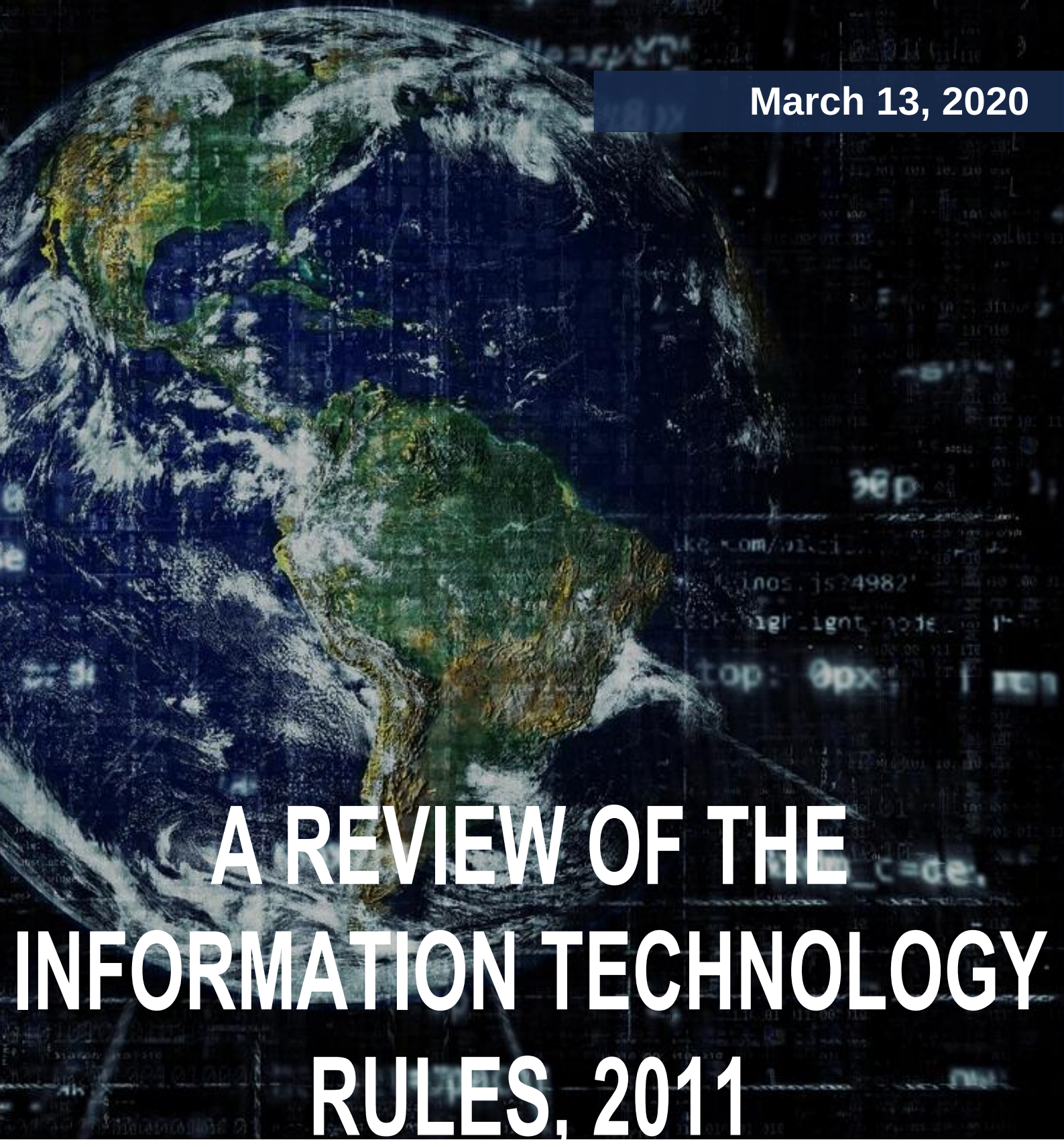

March 13, 2020

A REVIEW OF THE INFORMATION TECHNOLOGY RULES, 2011

REASONABLE SECURITY PRACTICES AND PROCEDURES AND SENSITIVE PERSONAL DATA OR INFORMATION

argus partners
SOLICITORS AND ADVOCATES

MUMBAI I DELHI I BENGALURU I KOLKATA I AHMEDABAD

Introduction

A new data protection law is on the anvil and all stakeholders are keenly awaiting the outcome of the consultation process for the draft Personal Data Protection Bill, 2019, recently initiated by the Joint Parliamentary Committee. Even after the new data privacy law is enacted, it is likely to take at least a year, if not more, for the infrastructure required to implement the new law to be put in place. Therefore, it will be an useful exercise to review and understand India's existing data privacy law which can be found in the form of the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 ("**2011 Rules**"). The 2011 Rules have been framed under Section 43A of the Information Technology Act, 2000 ("**IT Act**").

Advent of India's Data Privacy Regime

When the IT Act was enacted, its focus was on putting in place technology law fundamentals like digital signatures, providing legal recognition for electronic documents and the like. Its preamble states that its objective is to "*provide legal recognition for transactions carried out by means of electronic data interchange and other means of electronic communication, commonly referred to as 'electronic commerce', which involve the use of alternatives to paper-based methods of communication and storage of information, to facilitate electronic filing of documents with the Government agencies and further to amend the Indian Penal Code, the Indian Evidence Act, 1872, the Bankers' Books Evidence Act, 1891 and the Reserve Bank of India Act, 1934 and for matters connected therewith or incidental thereto.*"[1] It was only in 2008 that the IT Act was amended by the Information Technology (Amendment) Act, 2008, with effect from October 27, 2009 to incorporate Section 43A, which requires the *maintenance of reasonable security practices and procedures by bodies corporate that possess, deal or handle any sensitive personal data or information and* provides for *compensation for failure to protect such data*) and Section 72A, which penalises intentional personal data breach. The aforesaid amendment did not define either personal data or sensitive personal data, though Section 43A provided that "sensitive personal data or information" would mean such personal information as would be prescribed by the Central Government in consultation with such professional bodies or associations as it may deem fit.

Pursuant to the mandate given to the Central Government under Section 43A, the 2011 Rules were framed and for the first time, with effect from March 28, 2012[2], India had a legal regime for data privacy.

Do the 2011 Rules apply to all Types of Personal Data or only to Sensitive Personal Data?

Section 43A's stated objective is to stipulate that (i) a body corporate that processes sensitive personal data or information in a computer resource under its ownership or control must maintain reasonable security practices and procedures and (ii) if it is negligent in doing so and it causes wrongful loss to any person on account of such negligence, the body corporate shall be liable to pay damages by way of compensation to the person so affected. Since Section 43A refers only to 'sensitive personal data or information', one gets the impression that the 2011 Rules are meant to deal only with sensitive personal data and would not apply to non-sensitive personal data. Further, the phrase 'sensitive personal data or information' appears many times in the 2011 Rules, buttressing the feeling that the 2011 Rules deal only with sensitive personal data. However, on a careful reading of the 2011 Rules, one finds that the phrase 'personal information or sensitive personal data or Information' pops up in a few instances, though the phrase 'sensitive personal data or information' is a lot more common.

[1] http://meity.gov.in/content/preliminary

[2] The notification was issued on April 13, 2011

It could be argued that the phrase 'sensitive personal data or information' should be read as sensitive personal data and non-sensitive personal information. However, the better argument seems to be that the word 'sensitive' qualifies not only 'personal data', but also the word 'information'[3] and so 'sensitive personal data or information' should actually be read as 'sensitive personal data' or 'sensitive information'. The usage of the phrase 'personal information or sensitive personal data or Information' in a few places lends strength to the latter argument.

Sensitive Personal Data

What is Sensitive Personal Data?

Rule 3 of the 2011 Rules lists eight types of personal data as sensitive personal data, of which the first six are:

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;

After the six entries mentioned above, Rule 3 of the 2011 Rules has two more entries, which are as follows:

vii. any detail relating to the above clauses as provided to body corporate for providing service[4]
viii. any of the information received under above clauses by body corporate for processing, stored or processed under lawful contract or otherwise[5].

Thus, any document or other piece of data that captures the first six categories of sensitive personal data, that is provided to a body corporate for providing any service or performing under a contract would also be sensitive personal data.

The abovementioned eight types of sensitive personal data given in Rule 3 of the 2011 Rules is an exhaustive list, subject to the exception that, any information that is freely available or accessible in the public domain or furnished under the Right to Information Act, 2005 or any other law for the time being in force shall not be regarded as sensitive personal data or information for the purposes of the 2011 Rules.

Comparison with the Personal Data Protection Bill, 2019 ("PDP Bill 2019")

Passwords are not considered to be sensitive personal data under the PDP Bill, 2019, though the Personal Data Protection Bill, 2018 had included passwords in the list of sensitive personal data. The GDPR too does not consider passwords to be sensitive personal data. Other than passwords, all other categories of sensitive personal data provided for in Rule 3 of the 2011 Rules is covered by the definition of sensitive personal data given in the PDP Bill 2019. Instead of 'medical records and history' and 'physical, physiological and mental health condition', the PDP Bill 2019 has 'health data'. The PDP Bill 2019 also has the following additional categories of sensitive personal data,

[3] The IT Act defines 'information' as follows. Information includes data, message, text, images, sound, voice, codes, computer programmes, software and data bases or micro film or computer generated micro fiche. The 2011 Rules follow this definition.
[4] Sub-Rule (vii) of Rule 3 of the 2011 Rules
[5] Sub-Rule (viii) of Rule 3 of the 2011 Rules

which are not found in the 2011 Rules, namely, health data[6]; official identifier; sex life[7]; genetic data; transgender status; intersex status; caste or tribe; and religious or political belief or affiliation.

The "Commercial or Professional Activities" Requirement

The 2011 Rules protects personal data which is collected by an individual or a person who is involved in commercial or professional activities. This is because, all obligations under the 2011 Rules are incident only on bodies corporate. A 'body corporate' is defined under Section 43A of IT Act as "*any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities".* Therefore, an individual or a person who is not engaged in commercial or professional activities would fall outside the ambit of the 2011 Rules.

It is interesting to note that the 2011 Rules do not require personal data to be collected by a body corporate in the course of commercial or professional activities, for the 2011 Rules to apply. As long as a body corporate is engaged in any commercial or professional activity, such body corporate would be covered by the 2011 Rules. With the exception of young children, students and homemakers, there are very few individuals in this world who do not carry on any form of commercial or professional activity. A not-for-profit hospital cannot be said to be carrying on any commercial activity, though it processes large quantities of sensitive personal data. Can it be said that the not-for-profit hospital is carrying on professional activities? A doctor who works for charity would be carrying on professional activities and would be covered by the definition of body corporate. Would the word 'professional' extend to any work-related activity? Would a clerk working for a government owned or privately owned enterprise be called a "professional" for the purpose of the aforesaid definition of body corporate? A teacher is a professional and hence a teacher employed by a government owned school would be a body corporate and would be required to comply with the 2011 Rules in relation to any personal data processed by him/her, even in his/her personal capacity.

It is arguable that the drafters of the 2011 Rules intended to cover personal data and sensitive personal data which is collected in the course of commercial or professional activities, but a plain reading of the definition of 'body corporate' does not capture such an intent.

Do the 2011 Rules apply to Data which is not in an Electronic Format?

As mentioned above, the IT Act deals primarily with *electronic communication and electronic documents. In general, rules framed under the IT Act cannot apply to matters outside the purview of the IT Act.* The 2011 Rules state that they have been made by the Central Government under in exercise of the powers conferred by clause (ob) of subsection (2) of section 87 read with section 43A of the IT Act. *Section 87 of the IT Act provides that the Central Government may, by notification in the Official Gazette and in the Electronic Gazette, make rules to carry out the provisions of this Act.* The inclusive list of matters on which the Central Government may make rules includes *the reasonable security practices and procedures and sensitive personal data or information under section 43A*[8]*.* Section 43A of the IT Act states that it is applicable to sensitive personal data or information stored "in a computer resource".

Therefore, it is arguable that the 2011 Rules would apply only to personal data or information which is in an electronic format or in a computer resource and would not apply if any personal data is held in a non-electronic form, such as in a physical register or other hard copy document.

[6] The 2011 Rules classifies 'medical records and history' as sensitive personal data, but 'health data' is wider.

[7] The PDP Bill 2019 has a separate entry for 'sexual orientation'

[8] Sub-section(*ob*) of Section 87(2) of the IT Act

Privacy Policy

Rule 4 of the 2011 Rules requires everybody corporate (or any person who on behalf of the body corporate) that collects, receives, possess, stores, deals or handles information of the information provider, to provide a privacy policy. Such a privacy policy has to be available for viewing by those who have provided any information to the body corporate under lawful contract(s). The privacy policy also has to be published on the website of the body corporate. The privacy policy has to clearly set out the practices and policies of the body corporate for the collection, receipt, possession, storage, dealing or handling of information. It should also list out the types of personal data or sensitive personal data collected by the body corporate.

Obligations when collecting Personal Data

Rule 5 of the 2011 Rules contains a number of sub-rules relating to the collection of personal data. Of these, sub-rules 1, 2 and 4 relate only to sensitive personal data, whist the rest apply to all types of "information" (as defined in the IT Act and explained above).

When collecting sensitive personal data, the collector of such data has to obtain the prior consent of the provider of such sensitive personal data[9]. Further, sensitive personal data may be collected only for a lawful and necessary purpose[10]. A body corporate (or any person acting on behalf of a body corporate) holding sensitive personal data or information shall not retain that information for longer than is required for the purposes for which the information may lawfully be used or is otherwise required under any other law for the time being in force.[11]

Sub-rule 7 of Rule 5 states that the "provider of information" shall also be given the option to withdraw the consent given earlier to the body corporate. Since consent for collection of personal data is required only for sensitive personal data, it may be inferred that this provision applies only to sensitive personal data, even though sub-rule 7 ostensibly applies to all types of personal data. Withdrawal of the consent has to be communicated in writing to the body corporate which collected the information. The 2011 Rules are silent regarding the aftermath of withdrawal of consent. It may be argued that a body corporate holding personal data which was collected on the basis of consent, is required to erase such data when consent is withdrawn.

The sub-rules of Rule 5 which apply to all types of "information" (as defined in the IT Act, and explained above) are as follows:

While collecting information directly from the owner of such information, the person collecting such information has to ensure that the person concerned is informed that his personal information is being collected, (b) the purpose for which the information is being collected, the intended recipients of the information, and the name and address of the agency that is collecting the information and of the agency that will retain the information.[12] Any information that is collected shall be used only for the purpose for which it has been collected.[13]

A body corporate which has collected information is required to permit the providers of information, as and when requested by them, to review the information they had provided and ensure that any personal data found to be inaccurate or deficient is corrected or amended to the extent it is feasible.[14] However, it has been clarified that a body corporate shall not be responsible for the

[9] Rule 5(1) of the 2011 Rules.
[10] Rule 5(2) of the 2011 Rules.
[11] Rule 5(4) of the 2011 Rules.
[12] Rule 5(3) of the 2011 Rules.
[13] Rule 5(5) of the 2011 Rules.
[14] Rule 5(6) of the 2011 Rules.

authenticity of the personal information or sensitive personal data or information supplied to such body corporate.[15]

Prior to the collection of any information, the provider of such information should be given the option to not to provide the information sought to be collected.[16]

Anybody corporate who collects personal information is required to address any discrepancies and grievances (relating to processing of information in a time bound manner) of the providers of the information. For this purpose, the body corporate has to designate a grievance officer ("**Grievance Officer**") and publish his/her name and contact details on the body corporate's website. The Grievance Officer has to redress the grievances of the providers of information expeditiously and no later than one month from the date of receipt of grievance.[17]

Disclosure of Sensitive Personal Data

Rule 6(1) of the 2011 Rules provides that disclosure of sensitive personal data by a body corporate to any third party shall require the prior permission of the provider of such information. Such prior permission may be contained in the contract between the provider of sensitive personal data and the body corporate, in terms of which, the sensitive personal data was provided to the body corporate. The aforesaid Rule 6(1) applies only to sensitive personal data and does not apply to non-sensitive personal data.

There are a few exemptions to the rule regarding the need for prior permission before any sensitive personal data is disclosed, which are contained in Rules 6 and 7 of the 2011 Rules. These are:

- when disclosure is necessary for compliance with a "legal obligation". We presume that the "legal obligation", in the given context, implies a statutory obligation, as opposed to a contractual obligation;[18]
- if such sensitive personal data is sought in writing by Government agencies for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. The Government agency's request has to be accompanied by an undertaking to not to publish or share such sensitive personal data with any other person;[19]
- when disclosure is required by any third party by an order under the law for the time being in force;[20] and
- Rule 7 of the 2011 Rules provides that "sensitive personal data or information including any information" [sic] may be transferred to any person in India or abroad who ensures the same level of data protection that is adhered to by the transferor as provided for under the 2011 Rules, provided such transfer is necessary for the performance of a lawful contract between the transferor of personal data and the provider of personal data or where the provider of personal data has consented to such data transfer. Rule 7 uses the phrase "sensitive personal data or information including any information" and this could be interpreted to imply that it includes non-sensitive data. However, since Rule 7 is an exception to Rule 6 (which applies only to sensitive personal data), this point is moot.

Since Rule 6(1) applies only to sensitive personal data, can it be said that non-sensitive data can be disclosed or transferred without the need for any prior consent? The answer appears to be a yes. In such case, are there any restrictions for the disclosure or transfer of non-sensitive personal

[15] Proviso to Rule 5(6) of the 2011 Rules.
[16] Rule 5(7) of the 2011 Rules.
[17] Rule 5(9) of the 2011 Rules.
[18] Rule 6(1) of the 2011 Rules.
[19] Proviso to Rule 6(1) of the 2011 Rules.
[20] Rule 6(2) of the 2011 Rules.

data by the holder of such personal data? It may be argued that every person to whom non-sensitive personal data is transferred would be bound by the same restrictions which applied to the transferor of non-sensitive personal data. Since the transferor would have received the personal data with the consent of the provider of such personal data, the transferee must adhere to the terms under which the consent was given.

Reasonable Security Practices and Procedures

As mentioned above, Section 43A of the IT Act requires the maintenance of reasonable security practices and procedures by bodies corporate that possess, deal or handle any sensitive personal data or information. Rule 8 of the 2011 Rules provides 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. Rule 8(2) provides that the International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques - Information Security Management System - Requirements" meets the standards referred to above.

A body corporate may follow standards other than IS/ISO/IEC codes of best practices for data protection, provided such codes of best practices are (i) duly approved and notified by the Central Government and (ii) certified or audited on a regular basis by an independent auditor, who is duly approved by the Central Government. The audit of reasonable security practices and procedures shall be carried cut by an auditor at least once a year or as and when the body corporate undertakes significant upgradation of its process and computer resource.

A body corporate who has implemented either the IS/ISO/IEC 27001 standard or any codes of best practices for data protection which are approved and notified by the Central Government, shall be deemed to have complied with reasonable security practices and procedures. In other words, Rule 8 of the 2011 Rules creates a safe harbour so that in the event of an information security breach, the body corporate is able to demonstrate that it has have implemented security control measures as per their documented information security programme and information security policies.

Penalties for Breach of the 2011 Rules

The 2011 Rules do not contain any provision that prescribes a penalty for a breach of the 2011 Rules.

Section 72A of the IT Act punishes any person, including an intermediary, who discloses personal data without the consent of the person concerned, with the intention of causing loss to such person, with imprisonment for a term which may extend to three years, or with fine which may extend to five lakh rupees, or with both. The ingredients required to constitute an offence under Section 72A of the IT Act are (i) securing secured access to personal data when providing services under a lawful contract, (ii) disclosure of personal data with the intention to cause wrongful loss or wrongful gain, (iii) absence of consent from the concerned person or disclosure resulting in breach of the contract under which the personal data was secured. Please note that it is irrelevant for the purpose of Section 72A whether the disclosure of personal data, either without consent or in breach of the contract, actually resulted in loss or damage to the person to which such personal data relates. An intention to cause wrongful loss or wrongful gain is sufficient to pin liability on the person with such malafide intention.

As mentioned earlier, Section 43A stipulates the payment of compensation for any negligence by a body corporate in maintaining reasonable security practices and procedures, if such negligence

results in loss, but does not prescribe any criminal penalty, even if there is intentional failure in maintaining reasonable security practices and procedures.

Section 45 of the IT Act provides that when there is a contravention of any rules or regulations which have been made under the IT Act and no penalty has been separately provided for such contravention, the contravener shall be liable to pay a compensation not exceeding twenty-five thousand rupees to the affected person or a penalty not exceeding twenty-five thousand rupees. Therefore, contraventions of the 2011 Rules, which are not covered by Section 43A or Section 72A of the IT Act, shall fall under the aforesaid residuary Section 45. Thus, a body corporate's failure to obtain prior consent before collecting sensitive personal data or a failure to make available a privacy policy for viewing by those who have provided any information to the body corporate under a lawful contract, would be punished under Section 45 of the IT Act. Under Section 45, contravener shall be liable either to pay compensation to the affected person or a penalty to the government, but not both. On a plain reading of Section 45, it is unclear under what circumstances the contravener would be liable to pay a compensation to the affected person and when a penalty to the government would fall due.

This paper has been written by Vinod Joseph (Partner), Protiti Basu (Associate) and Ashwarya Bhargava (Associate).

DISCLAIMER

This document is merely intended as an update and is merely for informational purposes. This document should not be construed as a legal opinion. No person should rely on the contents of this document without first obtaining advice from a qualified professional person. This document is contributed on the understanding that the Firm, its employees and consultants are not responsible for the results of any actions taken on the basis of information in this document, or for any error in or omission from this document. Further, the Firm, its employees and consultants, expressly disclaim all and any liability and responsibility to any person who reads this document in respect of anything, and of the consequences of anything, done or omitted to be done by such person in reliance, whether wholly or partially, upon the whole or any part of the content of this document. Without limiting the generality of the above, no author, consultant or the Firm shall have any responsibility for any act or omission of any other author, consultant or the Firm. This document does not and is not intended to constitute solicitation, invitation, advertisement or inducement of any sort whatsoever from us or any of our members to solicit any work, in any manner, whether directly or indirectly.

You can send us your comments at:
argusknowledgecentre@argus-p.com

Mumbai I Delhi I Bengaluru I Kolkata I Ahmedabad

www.argus-p.com