Unit 3: Body Corporate Responsibilities for Data Protection

3

UNIT STRUCTURE

1.1 LEARNING OBJECTIVES

After going through this chapter, you should be able to understand:

- What is meant by 'Reasonable Security Practices and Procedures'
- What are the responsibilities which need to be discharged by Body Corporates
- Can Body Corporates be held liable if the information given isn't authentic

1.2 INTRODUCTION

With the rampant use of the internet, there is an undeniable need for the protection of data that the people put up or share over the internet. This has been more firmly established by the pronouncement of judgment by the Honorable Supreme Court in the case of ***Justice K.S. Puttaswamy (Retd.) & Anr. v Union of India & Ors,***[171] which accorded the right of privacy as a fundamental right. Further, it is a recognized and a well-recognized jurisprudential principle that where there is a right, there is a duty. So in this situation, where the individuals have the right to privacy, the bodies or agencies which have the data of the individuals are under a duty to protect and restrain from the using or allowing the data to be used for any purpose other than that

[171] *Justice K.S. Puttaswamy (Retd) & Anr v Union of India & Ors* W P (Civil) No 494 of [2012]

permitted by law. In this chapter, we will focus on those duties of a body corporate that has been imposed upon them by the law with respect to the protection of electronic data.

1.3 LEGAL DEFINITION OF CERTAIN IMPORTANT TERMS

The term ***'body corporate'*** has neither been defined under the Information Technology Act, 2000 nor under any of the Rules issued from time to time by the competent authorities which draw its validity and legal backing from the Information Technology Act 2000 (hereinafter referred to as 'the IT Act, 2000'). However, in the year 2008, certain provisions of the IT Act, 2002, were amended and amongst other provisions, ***Section 43A*** was brought in, which prescribed that the compensation has to be paid, to the provider of information, by the body corporate which possesses, deals or handles sensitive personal data or information who has a duty to implement and maintain reasonable security practices and procedures so as to prevent the information from unauthorized use, access, sharing, alteration or damage and which has failed to do so and, as a result of the unauthorized access or disclosure, certain loss has been caused. It is in the explanation part of this provision, certain terms have been defined, which sets out their meaning for the purpose of the section. It is in this part of this provision that body corporate has been defined. It states that 'body corporate' means any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities.

The term also defines ***'reasonable security practices and procedures'*** as those 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. Now, as the definition mentions the reasonable security practices and procedures as those practices as procedures as may be specified in law, the Central Government has framed certain Rules to regulate on these security practices and procedures drawing its validity under ***Section 43A and clause (ob) subsection (2) of Section 87 of the IT Act 2000.*** The Central Government notified these Rules in the year 2011, and they are ***called Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information)***

Rules, 2011 (hereinafter referred to as 'the 2011 Rules'). Now we will look into the important amongst those guidelines. In the previous Chapter, those guidelines were discussed from the viewpoint of the provider of the information, but in this chapter, the discussion will follow the viewpoint of an organization that is collecting such information.

1.4 RESPONSIBILITIES TO BE DISCHARGED BY BODY CORPORATE

1. Responsibility of Body Corporate to provide a policy for privacy and disclosure of information.

   Under the 2011 Rules, ***Rule 4*** provides that the body corporate or any person, who on its behalf collects, receives, possess, stores, deals or handle information of provider of information, has to provide a privacy policy for handling of or dealing in personal information including sensitive personal data or information. Such body corporate or any person on its behalf shall ensure that such policy is available for seeing to such providers of information who has provided the concerned information under a lawful contract, and such policy shall be published online on the website of the body corporate. The policy shall have following things among others:-

   i. Clear and easily accessible statements of its practices and policies; and
   ii. Type of personal or sensitive personal data or information collected under Rule 3 of the 2011 Rules; and
   iii. Purpose of collection and usage of such information; and
   iv. Disclosure of information including sensitive personal data or information as provided in Rule 6 of the 2011 Rules;
   v. Reasonable security practices and procedures as provided under Rule 8 of the 2011 Rules.

2. As mentioned under ***Rule 5 of the 2011 Rules,*** it is duty or responsibility of the Body Corporate or the person working on its behalf to obtain the consent of the provider of the sensitive personal information or data. Such consent must be regarding the purpose of usage and must be obtained before the collection of such information.
3. It is also the responsibility of the body corporate or the person working on its behalf to endure that the provider of the sensitive personal information is aware that such information is being collected, and the purpose for which the information is being collected, and the intended recipients of the information sought to be collected, along with the name and

address of the agencies collecting the information and of those who will be retaining the information.[172]

4. The body corporate is also under an obligation to collect information only for a lawful purpose, which is connected with any activity or function of such body corporate and when the collection of information is necessary for that purpose.
5. The body corporate or the person acting on its behalf which is holding such sensitive personal information or data is under an obligation to not retain the information retained for any time longer than what is required for the lawful purpose for which the information was retained or than the period which is permitted under any law for the time being in force.
6. One of the most important and basic responsibilities of the body corporate or the person who is working on its behalf is that the information shall be used only for the purpose for which it was collected and nothing more. This responsibility restricts the body corporate from the misuse of the data collected and this is a very big onus being placed on the body corporate.
7. It is the duty of the body corporate to enable the data or information providers to correct or amend the data or information given by them, when they request for the same, and so far as this is feasible. The point worth noticing here is that the body corporate or the person working on its behalf isn't responsible for the correctness or the genuineness of the data or information given or corrected, as the case may be.
8. Another important obligation of the body corporate is that before collecting the information, it or any person working on its behalf shall provide the provider of the information with an option to not provide the concerned data or information.
9. The obligation mentioned in the point above is also available at a later stage, whereby the consent is given can be withdrawn at a later stage, and thereby the body corporate or any person working on its behalf shall be duty-bound not to use such data or information in respect of which the consent has been withdrawn.
10. Under sub-rule 5 of Rule 5 of the 2011 Rules, another responsibility of the body corporate has been encapsulated. This obligation or responsibility is that of grievance redressal of establishing an authority for the said purpose. The Rule states that the body corporate shall address any discrepancies and grievances of their provider of the information with respect to the processing of information in a time-bound manner. The Rule also mandates the body

[172] <https://digitalindia.gov.in/writereaddata/files/6.Data%20Protection%20in%20India.pdf>

corporate to designate a Grievance Officer, and to ensure that this is known to the people, it is obligated to publish his name and contact details online on its website. The Rule also prescribes a timeframe within which the grievances must be taken care of and mentions that the Grievance Officer shall redress the grievances or provider of information expeditiously but within 1 month from the date of receipt of the grievance.

11. Another obligation on the body corporate is mentioned in sub-rule 8 of rule 5 of 2011 Rules. It states that the body corporate or any person working on its behalf shall keep the information secure as provided in rule 8. In relation to the same, rule 8 talks about 'Reasonable Security Practices and Procedures.'

    Rule 8 talks about presumption, in favour of body corporate or person acting on its behalf, in respect of security practices and procedures provided that they have implemented such security practices and standards and have a comprehensively documented information security program and information security policies. The requirement of such policies shall contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected with the nature of business.[173]

    The rule further lists down certain standards which, if complied with, are sufficient to raise the presumption above mentioned.

    - One such standard is: The International Standard IS/ISO/IEC 27001 on "Information Technology - Security Techniques - Information Security Management System – Requirements."
    - Any industry association or its entity, whose members are self-regulating by following any standard other than IS/ISO/IEC codes of best practices for data protection as per sub-rule(1) of Rule 8, needs to get its codes of best practices duly approved and notified by the Central Government for effective implementation.[174]

    The rule further mentions that the body corporate or a person on its behalf who have implemented either IS/ISO/IEC 27001 standard or the codes of best practices for data protection as approved and notified (abovementioned) shall be deemed to have complied with reasonable security practices and procedures provided that such

[173] Rule 8: Reasonable Security Practices and Procedures <https://www.itlaw.in/rule-8-reasonable-security-practices-and-procedures/>

[174] <https://induslaw.com/app/webroot/publications/pdf/alerts-2018/Personal_Data_Protection_Bill_2018.pdf>

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 undertakes significant upgradation of its process and computer resource.

12. Regarding disclosure of information by the body corporate or any person working on its behalf, as the body corporate is responsible not to disclose the data or information to any other person or entity without the prior permission of the provider of the information, but this doesn't apply where the disclosure is a legal obligation of the body corporate.
13. In continuance of the obligation to not to disclose the information or data to any third party, another important yet interesting obligation of the body corporate is to disclose the data to the Government Agencies which are mandated under the law to obtain information which is covered under the 2011 Rules on certain grounds, and this has to be done by the body corporate without the prior permission of the provider of the information. So this rule is, in a way, an exception to the general rule that the disclosure of information can be made only after the prior permission of the provider. The grounds on which such disclosure is to be made by the body corporate to the Government Agencies include: for the purpose of verification of identity, or for prevention, detection, investigation including cyber incidents, prosecution, and punishment of offences. This rule, as mentioned in the one of the previous chapters is similar to one of the provisions under the IT Act which provides for similar grounds on which the governmental agencies can seek information from the entities retaining them and the latter are under an obligation to disclose the same to the concerned agencies on the orders of the authorities mentioned therein.[175]
14. Also, the disclosure of the information is mandatory for the body corporate in compliance with an order under the law for the time being in force (as per Sub-rule 2 of Rule 6 of 2011 Rules).[176]

[175] How to deal with Section 43A in a Company <https://www.naavi.org/cl_editorial_12/edit_dec_2_sec43A_compliance_framework.html>
[176] Data Protected India | Insights | Linklaters <https://www.linklaters.com/en/insights/data-protected/data-protected---india>

So these were the major responsibilities or obligations of the body corporate in respect of data protection, which can be ascertained from the legal regime which is existing at present.

1.5 LET'S SUM UP

In this chapter, we have studied the meaning of reasonable security practices and procedures along with certain important terms related to data protection. Finally, we have ended our discussion with the responsibilities to be discharged by body corporate.

1.6 FURTHER READING

- Privacyinternational.org (2019), https://privacyinternational.org/sites/default/files/2018-09/Data%20Protection%20COMPLETE.pdf (last visited Nov 21, 2019).
- Ghosh, Dr. Jayanta. (2016). 'Privacy and Data Protection Laws in India: A Right-Based Analysis.
- India: Data Protection & Cyber Security - AZB & Partners, AZB & Partners (2019), https://www.azbpartners.com/bank/india-data-protection-cyber-security/ (last visited Nov 21, 2019).
- Thelawreviews.co.uk (2019), https://thelawreviews.co.uk/digital_assets/25776d4c-702f-41bb-82a0-cb3e18240506/Privacy.pdf (last visited Nov 21, 2019).

1.7 CHECK YOUR PROGRESS: POSSIBLE ANSWERS

1. **Was 'body corporate' originally defined in the Information Technology Act, 2000?**
   No. However, Section 43A was inserted by Information Technology (Amended) Act, 2008, in the explanation of which the term 'body corporate' was defined for the first time in the law relating Information Technology.

2. **Can body corporate obtain information on the assumption that the provider of the information is aware of the purpose for which the information is to be used?**
   No, it has been mentioned under "Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011", that it is the responsibility of the body corporate to make sure that the provider of the information is aware of certain things, one of which is the purpose for which the information is being collected. And therefore the body corporate can't record the information or data on presuming the knowledge of the provider.

3. **Does body corporate need to obtain the prior permission of the provider of information if it is ordered to disclose the concerned information by a court's order?**

   In the situation mentioned above, since disclosing the concerned information becomes the legal obligation on the body corporate due to it coming from the court's order, hence the prior permission isn't necessary for such a situation.

4. **If the information is provided by a person with his free consent for a particular purpose, can such information be used for any other purpose for which he hasn't consented specifically?**

   The obligations as mentioned under the 2011 Rules, specify that the consent which is necessary must be for the specific purpose for which the information is to be used. Thus the information can't be used for any purpose other than that for which it was consented to.

5. **If the provider of the information has any grievance against any body corporate, whom does he need to approach, and by when shall the grievance be resolved?**

   The Body Corporate has to appoint a Grievance Officer for resolving such grievances, and it has to be done within one month.

1.8 ACTIVITY

Mention all the situations (covered under IT Act, 2000, and Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011) under which the information or data can be disclosed to third parties. (800 Words)