SPDI Rules 2011: Taking a step towards securing Data

Ravi Singhania
Managing Partner
E: ravi@singhania.in

Data Protection and Privacy is of high importance in the contemporary world. It shields an organisation's information against fraud, hacking, phishing and identity theft. Any business that wishes to function efficiently must create a data protection plan to secure its data. Nowadays, data protection and privacy have turned into issues of individual rights.

Ensuring Privacy through Protecting Data

According to Article 21 of the Indian Constitution, which was upheld by the Supreme Court in the landmark case of *Justice KS Puttaswamy v. Union of India*, the right to privacy was recognised as a fundamental right. One of the most important legislations in this domain is The Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules 2011 (SPDI Rules).

Issued on 13th April 2011, the SPDI Rules impose strict security requirements on organisations that retain sensitive user personal information. These Rules apply to any corporate body or person located in India.

According to the Security Practices Rules, sensitive personal information must be given to the government entities. As per Rule 3 of the regulations, the following forms of data or information are to be regarded as sensitive personal data:

- Bank Account Details,
- Present and past health records,
- Passwords,
- Sexual orientation,
- Biometric data,
- Credit/debit card details,

A person who provides information to a body corporate is known as an information provider. 'Body Corporate' has been defined as a company under Clause 11 of Section 2 of the Companies Act, 2013.

It states, "body corporate or corporation includes a company incorporated outside India, but does not include -

(i) a co-operative society registered under any law relating to co-operative societies; and

(ii) any other body corporate (not being a company as defined in this Act), which the Central Government may, by notification, specify in this behalf;

According to these rules, information providers have certain rights over sensitive personal information. This information cannot be collected without the providers' consent, and providers have the right to refuse to give consent or to withdraw consent by writing to the body corporate.

A body corporate is prohibited by Rule 6 from publishing or disclosing such data or information to any third party without the approval of the information source. There are two exceptions to this rule, though:

- The contract between the body corporate and the information supplier stipulates that disclosure will take place.
- Adherence to a legal requirement.

The information provider has the right to check the data at any time and to update it if it turns out to be wrong. The body corporate may not keep the information for any longer than is necessary to fulfill the authorised purpose for which it was obtained, and may only use the information for the purpose for which it was gathered.

Furthermore, there exists a requirement for "Commercial or Professional activities" which essentially states that all personal data that may be collected by an individual or a person who is considered to be engaged in commercial or professional activities, (no distinction as to scope of commercial activity). The 2011 Rules are applicable only on 'bodies corporate' which has been defined under Section 43A of IT Act 2000.

Some features of the Body Corporate:

- The body corporate must respond to any complaints or inconsistencies of the information provider within one month through the grievance officer of the body, whose contact information must be made available on the website.
- Only when it is required for the fulfillment of the contract or the provider has given their consent may a body corporate transmit sensitive personal data or information to any other body corporate or a person in or outside of India that provides the same degree of data protection under these regulations.
- The body corporate in charge of SPDI need to implement "reasonable security practises and procedures in relation to SPDI," which includes establishing a privacy policy outlining the

kinds of information collected, the reasons behind collection, the disclosure policy, the security practises and procedures used, etc. The said policy must also be published on the body corporate's website.

Conclusion

Rules to ensure data privacy, especially in the present, are the need of the hour. That's why nearly a decade later, a fresh set of rules were introduced to govern the developing cyberspace - The Information Technology (Intermediary Guidelines and Digital Media Ethics Code) Rules, 2021, which shall be discussed next.