scripted

*Volume 8, Issue 3, December 2011*

# INDIA'S NEW DATA PROTECTION LEGISLATION: DO THE GOVERNMENT'S CLARIFICATIONS SUFFICE?

*Raghunath Ananthapur*[*]

**Abstract**

After giving an introduction to data protection legislation in India, the author analyses the latest round of regulations to arise out of that country. This is important because India has started gaining prominence in the outsourcing business from European Union countries.

DOI: 10.2966/scrip.080311.317



[*] Raghunath Ananthapur, Lawyer, Tatva Legal, Bangalore, India. raghunath.ananthapur@tatvalegal.com. For a detailed analysis of India's Data Protection Legislation in its previous form see R Ananthapur, "India's New Data Protection Legislation" (2011) 8:2 *SCRIPTed* 192 available at http://www.law.ed.ac.uk/ahrc/script-ed/vol8-2/ananthapur.asp.

## 1. Background

An introduction of data protection legislation in India has been long awaited, particularly after India started gaining prominence in the outsourcing business from European Union countries.

On 11 April 2011, the Indian Ministry of Communications and Technology published rules implementing certain provisions of the *Information Technology (Amendment) Act 2008* (IT Amendment Act 2008) dealing with protection of sensitive personal data or information (Sensitive Data), and security practices and procedures that must be followed by organisations dealing with Sensitive Data (Data Privacy Rules).[2]

The Data Privacy Rules define Sensitive Data as a subset of "personal information". "Personal information" is defined as any information that relates to a natural person, which either directly or indirectly, in combination with other information available or likely to be available within a body corporate, is capable of identifying that person.[3] Sensitive Data[4] is defined as personal information that relates to:

a) passwords;
b) financial information such as bank account or credit card or debit card or other payment instrument details;
c) physical, psychological and mental health conditions;
d) sexual orientation;
e) medical records and history;
f) biometric information;
g) any detail relating to (a) – (f) above received by the corporate body for provision of services; or
h) any information relating to (a) – (g) that is received, stored or processed by the body corporate under a lawful contract or otherwise.

Sensitive Data is broadly defined to include data obtained by any method, including lawful contract. Information that is freely available, accessible in the public domain, or furnished under the *Right to Information Act 2005*,[5] is excluded from the ambit of the above definition.[6]

Following the introduction of the Data Privacy Rules, there was confusion amongst the Indian outsource service providers regarding compliance with certain provisions of the Data Privacy Rules, particularly the consent requirements.

Applicability of the Data Privacy Rules was established on merely using computer equipment in India, by a body corporate, to perform the functions of collection, processing or transfer of Sensitive Data of individuals residing in any jurisdiction.

---

[2] Notification no GSR 313(E), 11 April 2011, Gazette of India, Extraordinary, pt II, s 3(i).

[3] *Data Privacy Rules*, Rule 2(i).

[4] *Data Privacy Rules*, Rule 3.

[5] Government of India, *Right to Information Act 2005,* No 22 of 2005.

[6] *Data Privacy Rules*, Rule 3.

The application of the Data Privacy Rules was not limited to sensitive data belonging to Indian residents. The body corporate was not restricted to body corporate established in India, but included foreign corporations.

Introduction of the Data Privacy Rules, seen as a boon to the Indian outsourcing industry, was turning out to be a bane, considering its far reaching scope and ambiguous provisions.[7] For example:

*(a) Data Centres:* A foreign body corporate operating a data centre in India that performs functions of collection, storage or processing of Sensitive Data of foreign body corporate customers was likely to be subject to the Data Privacy Rules, although in real sense the foreign body corporate would not be processing data in India.

*(b) Business Process Outsourcing Entities (BPOs):* Indian outsource service providers, performing solely the functions of processing of Sensitive Data of foreign individuals (e.g. loan or mortgage transactions, medical transcription), pursuant to a contract with a foreign body corporate and in most cases with no access to the individual whose Sensitive Data is processed, were required to comply with the statutory duties under the Data Privacy Rules, in addition to the contractual duties (based on mandatory local law of the foreign body corporate or foreign body corporate internal requirements) that they may have under a contract with the foreign body corporate.

*(c) Call Centre Entities:* Indian outsource service providers, providing call centre services, pursuant to a contract with a foreign body corporate, engaged in direct conversation with the foreign individuals whose Sensitive Data is being processed. Due to direct interaction with the foreign individuals whose Sensitive Data is being processed, there was strong basis to infer that a call centre may have to comply with the most contentious provision- consent requirements under the Data Privacy Rules (i.e. obtaining prior written consent from the individual whose Sensitive Data is processed), while it may have been argued otherwise in the case of BPOs that solely perform processing functions.

Broad scope and ambiguous provisions of the Data Privacy Rules had the potential to produce multiple interpretations of the provisions, thus making it difficult to the Indian outsource service providers to achieve compliance with the Data Privacy Rules. One of the provisions of the Data Privacy Rules that were extensively debated is the "consent requirement". The Data Privacy Rules in its previous form required the "body corporate",[8] prior to the collection of Sensitive Data, to obtain prior written consent (by letter, fax or email) from the individual whose Sensitive Data is processed, regarding the purpose of usage of such data. It was unclear whether an

---

[7] Harsimran Julka, "NASSCOM Says New IT Rules will Hurt BPOs", *The Economic Times* (23 May 2011) available at http://articles.economictimes.indiatimes.com/2011-05-23/news/29574167_1_indian-it-bpo-nasscom-data-security-council (accessed 15 Nov 2011). Also see ET Bureau, "Government Relents on New IT Security Rules, Exempts BPOs", *The Economic Times* (26 Aug 2011) available at http://articles.economictimes.indiatimes.com/2011-08-26/news/29931602_1_bpos-security-rules-clarification (accessed 15 Nov 2011).

[8] The term "body corporate" is defined as any company and includes firms, sole proprietorships or other associations of individuals engaged in commercial or professional activities. The term "body corporate" before the Department's clarifications was not restricted to "body corporate" established in India. See 2.1 of this paper for revised meaning. S 43A(i) of *Information Technology Act 2000* (No 21 of 2000).

Indian outsource service provider providing outsource services to a foreign corporation was required to comply with (or ensure that the foreign corporation complied with) the provisions of the Data Privacy Rules in relation to functions (e.g. collection of Sensitive Data) that were not performed in India. For example, in a loan processing transaction, a foreign corporation might obtain Sensitive Data directly from customers within its own jurisdiction and then send the application package to BPOs in India for further processing. In such case, is it the role of the BPOs to ensure that the foreign corporation has collected the Sensitive Data from its customers in accordance with the Data Privacy Rules? Or, are the Indian BPOs required to obtain fresh consents from each customer of the foreign corporation in accordance with the Data Privacy Rules prior to processing? Or, the Indian BPOs exempt from complying with the provisions of the Data Privacy Rules that relate to functions that are not performed in India (such as collection of Sensitive Data).

To address the concerns of the outsourcing industry, the Department of Information Technology, Ministry of Communications and Technology (the Department) published clarifications to the Data Privacy Rules on 24 August.[9]

## 2. Clarifications to Data Privacy Rules

### *2.1 Applicable to Indian Body Corporate*

The Data Privacy Rules apply only to sensitive data of any individual collected, processed, or stored in India via computer resource by a body corporate located in India (Indian Body Corporate).

The Department has clarified that if an Indian Body Corporate performs the functions of collection, storage, or processing of sensitive data directly pursuant to a contract with the individual whose Sensitive Data is being processed (residing in any jurisdiction); the Data Privacy Rules, become applicable in entirety to this Indian Body Corporate (Principal Indian Corporate Body). However, if an Indian Corporate body performs the functions of collection, storage, or processing of Sensitive Data under a contract with any organisation in India or outside India, Rules 5 and 6 of the Data Privacy Rules relating to consent and disclosure requirements, do not apply to such Indian Body Corporate (Processor Indian Corporate Body). The Processor Indian Body Corporate therefore would be primarily governed by the provisions of the contract that it has entered into with the Principal Indian Body Corporate or a foreign body corporate. While the consent and disclosure requirements are made inapplicable to Processor Indian Body Corporate, other obligations under the Data Privacy Rules, such as publication of privacy policy, transfer conditions, and implementation of security controls, appear to remain applicable to Processor Indian Body Corporate.

### *2.2 Provider of Information*

The term "provider of information" was not defined in the earlier Data Privacy Rules. The Department has clarified that the term "provider of information" as referred to in

---

[99] *Clarifications on Information Technology (Reasonable Security Practices and Procedures & Sensitive Personal Data or Information) Rules 2011* under s 43A of the *Information Technology Act 2000*, available at http://mit.gov.in/sites/upload_files/dit/files/PressNote_25811.pdf (last accessed 16 Nov 2011).

the Data Privacy Rules refers to natural persons who provide sensitive personal data to Indian Body Corporate (Provider).

### *2.3 Consent*

Previously, a body corporate was required to obtain the prior written consent of the Provider by letter, fax or email. The Department has now clarified that the consent may be obtained by "any mode of electronic communication", and not just by fax or email.[10] This means that the consent may now be obtained through sms and telephone.

### *2.4 Privacy Policy*

Previously, it appeared that the body corporate was required to provide information, on its website for viewing by the Providers, that is more than what is provided for general information purposes; the information could have been implied to contain specific details in each case, such as the type of Sensitive Data collected, purpose of use and disclosures to a third party. In certain types of business activity, these details may be different in each case, making it difficult to provide general information, and certainly such information would be Sensitive Data and confidential and therefore not appropriate for publication on a website with uncontrolled access.

The Department has now clarified that the privacy policy of the Indian Body Corporate should relate to a unique Indian Body Corporate and not with respect to any particular obligation under any contract. Essentially, Indian Body Corporate are required to publish privacy policy on their website, drafted in conformance with the Data Privacy Rules.

## 3. Need for Further Clarifications

While the Department has certainly allayed the concerns of Indian outsourcing industry to a great extent by providing clarifications to the Data Privacy Rules, the clarifications still leave possible interpretation issues open.

It is unclear why Rule 2 (publication of privacy policy), Rule 7 (transfer conditions), and Rule 8 (security controls) continue to be made applicable to Processor Indian Body Corporate, while the Processor Indian Body Corporate are excluded from compliance with the key conditions of the Data Privacy Rules (i.e. collection, consent, processing and disclosure), and thus, have no obligation towards the Provider with respect to the key conditions of the Data Privacy Rules. These conditions should be made inapplicable to Processor Indian Body Corporate which provides services pursuant to a contract with a foreign body corporate, since provision of services by such entities would be pursuant to a contract it would have with the foreign body corporate (based on mandatory local law of the foreign body corporate or the foreign body corporate internal requirements), and more so the Sensitive Data processed would relate only to foreign residents.

The Data Privacy Rules contain independent conditions for disclosure (Rule 6) and transfer of Sensitive Data, but fail to clarify which actions constitute "disclosure" and

---

[10] *Data Privacy Rules*, Rule 5.

which amount to "transfer"; disclosure of Sensitive Data also could qualify as "transfer" of Sensitive Data. Conditions for "transfer" of Sensitive Data are more stringent than conditions that apply to "disclosure" of Sensitive Data. The doubts will continue to remain regarding the circumstances in which the "disclosure" and "transfer" conditions will become applicable to Indian Body Corporate.

## 4. Conclusion

The Department has sent positive signals by reacting quickly to the Indian outsourcing industry's concerns by publishing clarifications to the Data Privacy Rules. The Department clarifications, while they will certainly benefit the Indian outsourcing industry, are half baked, and appear to have had, as the objective, exempting third party Indian outsource providers from the compliance with the most controversial provision –"consent conditions". Hopefully, as issues discussed above and other new issues appear with the compliance of the Data Privacy Rules, the Department will once again be fast to react to address them, but in a holistic manner.