scripted

*Volume 8, Issue 2, August 2011*

# INDIA'S NEW DATA PROTECTION LEGISLATION

*Raghunath Ananthapur*[*]

**Abstract**

With the increase in importance of the outsourcing business in India, there has been extensive discussion regarding the absence of Indian data protection legislation, and how this may impact the flow of business from European Union companies. India has, in the past, attempted to enact data protection legislation, but for some reason it has never seen the light of day.

India has recently notified regulations relating to protection of sensitive personal data. This article examines the Indian regulations, contrasting their provisions, at certain points, with the *UK Data Protection Act 1998*.

DOI: 10.2966/scrip.080211.192



[*] Raghunath Ananthapur, Lawyer, *Tatva Legal*, Bangalore, India. raghunath.ananthapur@tatvalegal.com.

## 1. Background

From the moment the Indian information technology industry began to play a major role in the outsourcing business, there have been extensive discussions regarding the lack of data protection legislation in India and how this may impact upon the flow of outsourcing business from European Union countries. The delay in Indian enactment of data protection legislation raised concerns that this might divert outsourcing business within the European Union to the new Eastern European Member States, or to other countries that provide adequate levels of protection for personal data via legislative or other means.

The importation of personal data from EU countries thus appears to be the driving force behind the Indian data protection debate, and earlier attempts to introduce data protection legislation.

Protection of personal data in the European Union (and European Economic Area) is based on the *EU Data Protection Directive*.[1] Transfer of personal data to locations outside the European Union is restricted unless the importing country ensures adequate levels of protection for personal data through its domestic legislation or international commitments. The European Commission is empowered by the *EU Data Protection Directive* to determine whether a third country ensures adequate levels of protection to personal data. The Commission has identified a limited number of countries that provide levels of data protection considered to be adequate and comparable to those in the European Union. These include: Andorra, Argentina, Australia, Canada, Switzerland, Faeroe Islands, Guernsey, Israel, Isle of Man and Jersey. The United States of America is not recognised as providing adequate levels of protection via legislation, but the European Commission and US Department of Commerce have entered into a "safe harbour" self-regulatory arrangement, whereby US companies become eligible to receive personal data from the EU by agreeing to adhere to the EU data protection principles.[2] The *EU Data Protection Directive* contains exemptions from the prohibition on transfer of personal data to non-EU countries that provide inadequate protection. These exemptions are, however, difficult to apply if the only reason for the transfer is to access low processing costs in the country of the data processor. The European Commission has, since 2001, authorised EU organisations to use standard clauses in their contractual arrangements with organisations located outside the European Union.[3]

---

[1] *Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data*, OJ L 281, 23 November 1995, 31–50.

[2] *Commission decisions on the adequacy of the protection of personal data in third countries* (2011) available at http://ec.europa.eu/justice/policies/privacy/thridcountries/ (accessed July 26 2011).

[3] *Model Contracts for the transfer of personal data to third countries* (2011) available at http://ec.europa.eu/justice/policies/privacy/modelcontracts/index_en.htm (accessed July 26 2011). The Information Commissioner under the *UK Data Protection Act 1998* has also authorised the use of model contract clauses: ICO, *International Transfers/Transborder Data Flows* available at http://www.ico.gov.uk/upload/documents/library/data_protection/practical_application/model_contracts_for_data_processors_processing_personal_information_on_their_behalf001001.pdf (accessed 26 July 2011).

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: (a) protection of sensitive personal data: security practices and procedures that must be followed by organisations dealing with sensitive personal data (Data Privacy Rules);[4] (b) due diligence to be observed by intermediaries; and (c) guidelines for cybercafés.

The last data protection bill, *The Personal Data Protection Bill 2006*,[5] introduced in Parliament on 8 December 2006, has now lapsed.[6] On 18 October 2010, the Department of Personnel and Training, Government of India, published an approach paper for legislation on privacy.[7] More recently, there have been news reports suggesting that a 'Right to Privacy' Bill will be introduced in Parliament in the upcoming monsoon session.[8] From the extracts of the Bill reproduced in the newspapers, it appears that it will be a data protection and privacy law. In the wake of all these developments, India will have data protection legislation dealing with protection of sensitive personal data. This development could, to some extent work in favour of India, especially when the British banks appear to be moving their call centres back to the UK.[9]

This paper discusses the Data Privacy Rules and at certain places also contrasts the concepts under the Data Privacy Rules with the *UK Data Protection Act 1998*[10] (UK Act).

## 2. Data Privacy Rules

### *2.1 Personal Information and Sensitive Personal Data*

The overall scheme of the Data Privacy Rules - including the brief description in the preamble, and the provision of *The Information Technology Act 2000*[11] (IT Act) under which they are enacted - appears to seek to protect Sensitive Data. The Data Privacy Rules refer consistently to 'sensitive personal data or information' (Sensitive Data) as the subject of protection, but also refer, with respect to certain obligations, to 'personal information'. Sensitive Data is defined as a subset of 'personal information'. The use of the terms 'information' and 'personal information' are general usages and are thus not intended to expand the scope of the Data Privacy

---

[4] Notification no. G.S.R. 313(E), 11 April 2011, Gazette of India, Extraordinary, Part II, Section 3(i).

[5] Bill No. XCI of 2006, *The Personal Data Protection Bill*, 2006 (2006) available at http://164.100.24.219/BillsTexts/RSBillTexts/asintroduced/XCI_2006.pdf (accessed 15 June 2011).

[6] Search of the Parliamentary Bills Information System reveals the status as 'lapsed'.

[7] Government of India, *Approach paper for a legislation on privacy* (2010) available at: http://persmin.gov.in/WriteReadData/RTI/aproach_paper.pdf (accessed 26 July 2011).

[8] J Venkatesan, "Bill on 'right to privacy' in monsoon session: Moily", *The Hindu Times* (7 June 2011) available at http://www.thehindu.com/news/national/article2082643.ece (accessed 15 June 2011).

[9] J Treanor, "Santander axes Indian call centers", *The Guardian*, (8 July 2011) available at http://www.guardian.co.uk/business/2011/jul/08/santander-axes-indian-call-centre (accessed 23 July 2011).

[10] UK *Data Protection Act 1998* c. 29 (hereafter UK Act).

[11] Government of India, *The Information Technology Act 2000* (No. 21 of 2000) (hereafter IT Act).

Rules. 'Personal information' is 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 such person.[12]

Sensitive Data[13] 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 condition;
d) sexual orientation;
e) medical records and history;
f) biometric information;
g) any detail relating to (a) – (f) above received by the body corporate 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*[14], is excluded from the ambit of the above definition.[15]

In contrast to the Data Privacy Rules, the UK Act addresses two distinct types of data: 'personal data' and 'sensitive personal data.'[16] The processing of 'sensitive personal data' is subject to conditions that are stricter than those applied to 'personal data'.[17]

Further, the Data Privacy Rules do not cover Sensitive Data that are available in non-digital form. This is possibly because the data protection rules are not stand-alone legislation being incorporated into the IT Act. The UK Act, however, includes within its ambit manual data that are structured and readily accessible.[18]

### *2.2 Key Terms in the Data Privacy Rules*

#### *2.2.1 Body corporate*

The term 'body corporate' is defined as any company and includes a firm, sole proprietorship or other association of individuals engaged in commercial or

---

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

[13] Data Privacy Rules, Rule 3.

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

[15] Data Privacy Rules, Rule 3.

[16] UK Act, s 1.

[17] UK Act, Sch 2 and Sch 3.

[18] UK Act, s 1(c); *Durant v FSA* [2003] EWCA Civ 1746.

professional activities.[19] The term 'body corporate' is not restricted to a 'body corporate' established in India.

*2.2.2 Any person on behalf of body corporate*

'Any person on behalf of body corporate' is not defined, but is used throughout the Data Privacy Rules in conjunction with the term 'body corporate.' It most likely refers to an organisation that collects, stores or processes Sensitive Data on behalf of a body corporate (Data Processor).

*2.2.3 Provider of information*

The term 'provider of information' is not defined in the Data Privacy Rules but it is understood to refer to an individual whose Sensitive Data is being collected (Provider). The equivalent term in the UK legislation would be 'data subject'.

The consequences of extending this definition of Provider to include a body corporate that discloses Sensitive Data to a third party are discussed at paragraph 2.9 of this paper.

### *2.3 Applicability*

The Data Privacy Rules appear to apply to Sensitive Data of any individual collected, processed or stored in India via computer resources by any entity, whether established in India or not. The application of the Rules is not limited to Sensitive Data belonging to Indian residents. Neither is 'body corporate' restricted to a 'body corporate' established in India, but includes a foreign body corporate.

Unlike the UK Act, the Data Privacy Rules do not distinguish between a data controller and a data processor. In the UK Act these terms are defined: a data controller (Data Controller) is a person who determines the purposes and the manner in which the data is to be processed. A data processor (Data Processor) is a person who processes the data on behalf of the 'data controller'. Under the UK Act, legal responsibility to the Provider rests with the Data Controller, unless decisions regarding control over the data are taken jointly by the Data Controller and the Data Processor. In that case, both organisations may be regarded as co-controllers.[20]

Under the Data Privacy Rules, legal responsibility in relation to consent requirements and Provider access requests does not lie solely with the corporation in question but appears to extend to the Data Processor. Both a body corporate and a Data Processor performing functions of collecting, storing or processing the Sensitive Data might be responsible for compliance with the obligations of the Data Privacy Rules.

For example, a foreign corporation using computer equipment in India that collects, processes, stores or transfers Sensitive Data must comply with the Data Privacy

---

[19] IT Act, s 43A(i).

[20] Data controllers who share personal data on data subjects for different purposes are often referred to as 'data controllers in common'. Each data controller remains individually responsible for the processing they have carried out on the personal data. Data controllers who share personal data on data subjects for the same purpose, and who would be jointly liable for any breach under the UK Act, are often referred to as joint data controllers'.

Rules. To illustrate further, a UK bank operating a data centre in India - that undertakes such functions in relation to the financial information of its UK customers – would appear to be subject to the Data Privacy Rules.

In another example, an Indian entity performing the functions of collection, processing or transfer of Sensitive Data of individuals residing in any jurisdiction, would be required to comply with statutory duties under the Data Privacy Rules, in addition to the contractual duties (based on local law or the requirements of the organisation) that it may have under a contract with the foreign body corporate. This is regardless of whether the Indian entity is in a position to determine the purposes and the manner in which the Sensitive Data is to be processed.

It is unclear however, whether an Indian organisation providing services to a foreign corporation is required to comply with (or ensure that the foreign corporation complies with) provisions of the Data Privacy Rules in relation to functions (eg collection of Sensitive Data) that are 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 its Indian service provider for further processing. In such case, is it the role of the Indian service provider to ensure that the non-Indian corporation modifies its data collection standards to comply with those imposed by the Data Privacy Rules? Is the Indian organisation required to obtain consents from each customer of the foreign corporation in accordance with the Data Privacy Rules? The answer to each of these questions should be 'no', since the collection function is not performed in India.

Until clarifications are issued, these questions will remain contentious, and as a result several interpretations will be applied.

### *2.4 Collection of Sensitive Data*

#### *2.4.1 Consent*

Prior to collection of Sensitive Data, the body corporate or the Data Processor must obtain prior written consent (by letter, fax or email) from the prospective Provider, regarding the purpose of usage of such data.[21]

#### *2.4.2 Conditions for collection of Sensitive Data*

Sensitive Data must not be collected unless it is for lawful purpose connected with a function of the body corporate, or the Data Processor, and the collection is necessary for that purpose.[22]

#### *2.4.3 Information*

While collecting Sensitive Data directly from the Provider, the body corporate or the Data Processor must ensure that the Provider is informed about: the fact that Sensitive Data is being collected; the purpose for which it will be used; who the intended

[21] Data Privacy Rules, Rule 5.

[22] Data Privacy Rules, Rule 5(2).

recipients are; which agency is collecting, and which agency will be retaining, the Sensitive Data.[23]

The Data Privacy Rules do not contemplate that Sensitive Data will be obtained other than directly from the Provider. The firm or Data Processor will not therefore be justified in disclosing Sensitive Data to a third party (even if such disclosure is necessary for the purpose for which the Sensitive Data is obtained) unless the corporation or Data Processor has obtained prior written consent of the Provider. A further exception, discussed below, involves circumstances in which the disclosure is necessary for compliance of a legal obligation.

*2.4.4 Opt out and withdrawal of consent*

Prior to collection of Sensitive Data, the corporation or the Data Processor must ensure that the Provider is given the option of declining to provide the Sensitive Data. A Provider who has already consented to the collection of the Sensitive Data must be able to communicate a withdrawal of consent, in writing, at any time.[24]

### *2.5 Processing and Retention*

Sensitive Data must not be used for purposes other than for which it is collected.[25]

The Data Privacy Rules do not specify any timeframes for retention of Sensitive Data. The body corporate or Data Processor must not retain the Sensitive Data for longer than is required for the purposes for which the Sensitive Data may lawfully be used.

The Data Privacy Rules do not override provisions of other laws that may specify a maximum period of retention for Sensitive Data.[26] For example, telecom licenses require licensees to maintain, for security reasons, for scrutiny by the Department of Telecommunication, all commercial records related to communications exchanged on the network for at least one year.

Section 67C of the IT Act requires an intermediary to retain such information, and for such period of time, as shall be prescribed by the Central Government. 'Intermediary' includes telecom service providers, network service providers, Internet service providers, web-hosting service providers, search engines, online-auction sites, online market places and cyber cafes. The Central Government has yet to frame rules implementing the retention provision. Therefore, the nature of data that is to be preserved and retained by the intermediary, and duration of retention, is not known.

### *2.6 Access*

A Provider has right of access to information about himself that is being held, and to review such information. If any of the retained information is found to be inaccurate

---

[23] Data Privacy Rules, Rule 5(3).

[24] Data Privacy Rules, Rule 5(7).

[25] Data Privacy Rules, Rule 5(5).

[26] Data Privacy Rules, Rule 5(4).

or deficient, the Provider has a right to require the body corporate or Data Processor to correct or amend such inaccuracy or deficiency.[27]

The Data Privacy Rules do not detail procedures to be followed by the Provider in exercising his right to access the data. Neither does it stipulate the time period within which the body corporate or Data Processor must comply with the request.

### *2.7 Disclosure of Information*

The disclosure of Sensitive Data requires the prior consent of the Provider, unless the disclosure is:

a) a provision of a contract between the body corporate and Provider; or

b) made to Government agencies mandated by law to obtain Sensitive Data for the purposes of verification of identity, or for the prevention, detection, investigation, prosecution and punishment of offences, including cyber incidents; or

c) pursuant to an order under the law.[28]

Neither the body corporate nor the Data Processor are permitted to publish Sensitive Data.[29] A third party that receives Sensitive Data from any body corporate or Data Processor is prohibited from disclosing it further.[30]

Where a disclosure is made to Government agencies mandated under the law, the body corporate should have received a request in writing from the Government agency stating clearly the purpose of use and containing an undertaking that it will not publish or share any information so received.[31] This means that an Indian Data Processor processing Sensitive Data of a foreign individual may be required to disclose such information to Government agencies in India. Foreign corporations exporting Sensitive Data to India should be aware of this condition; they may have to include consent provisions in their contractual arrangements with the Provider allowing them to make such disclosure if requested by an Indian Government agency.

### *2.8 Third party transfers*

A body corporate or Data Processor ('Transferor') may transfer Sensitive Data to a third party in India or outside India, provided:

a) the third party affords the same level of data protection that is adhered to by the Transferor under the Data Privacy Rules; and

b) transfer is necessary for the performance of the lawful contract between the Transferor and the Provider; or

---

[27] Data Privacy Rules, Rule 5(6).

[28] Data Privacy Rules, Rule 6(1).

[29] Data Privacy Rules, Rule 6(3).

[30] Data Privacy Rules, Rule 6(4).

[31] *Ibid.*

c) the Provider has consented to such transfer.[32]

While the UK Act and the *EU Data Protection Directive* appear to require that the transferee country provide adequate protection for processing of personal data through domestic legislation, the Data Privacy Rules appear to achieve protection in cases of transfer of Sensitive Data outside India, through a contract at the organisational level.

### *2.9 Overlap of Disclosure and Transfer conditions*

As indicated above, the Data Privacy Rules contain independent conditions for disclosure and transfer of Sensitive Data, but fail to clarify which actions constitute 'disclosure' and which amount to 'transfer'. Conditions for 'transfer' of Sensitive Data are more stringent than conditions that apply to 'disclosure' of Sensitive Data.

A corporation or Data Processor is permitted to disclose Sensitive Data to a third party if the Provider has consented to such disclosure in its respective contractual arrangements with them. Apart from compliance with a prohibition on publication of the Sensitive Data that is received, the third party has no further obligation with respect to the information; neither is the body corporate required to ensure that the third party at least take security measures to prevent misuse of Sensitive Data. For the sake of argument, the third party could be a person (including a person outside India) who does not provide adequate levels of protection to Sensitive Data.

On the other hand, a body corporate or Data Processor transferring Sensitive Data to another body corporate (whether in India or outside India) is required to ensure that the transferee firm affords the same level of protection to Sensitive Data that is adhered to by the transferor firm under the Data Privacy Rules. This will ensure that the transferee takes appropriate security measures to prevent misuse of Sensitive Data, does not retain the Sensitive Data longer than necessary etc.

If the definition of Provider is extended (beyond the meaning adopted in paragraph 2.2.3 of this paper) to include a corporation that discloses Sensitive Data to a third party, then the third party will be placed in the position of a body corporate under the Data Privacy Rules. The obligations of a body corporate with respect to collection, storage and processing of Sensitive Data, including obligations to implement security measures, will become applicable to such third party. The effect of such interpretation would be to impose legal responsibilities under the Data Privacy Rules on all persons who receive Sensitive Data (including transferee foreign firms under the transfer provision above). It is to be noted that the IT Act provides for extraterritorial application.[33]

### *2.10 Publication of Privacy Policy*

A body corporate and a Data Processor are required to publish on their respective websites a privacy policy in regard to the processing of Sensitive Data. It must contain the following information:

---

[32] Data Privacy Rules, Rule 7.

[33] The IT Act, s 1(2) provides: "It shall extend to the whole of India and, save as otherwise provided in this Act, it applies also to any offence or contravention thereunder committed outside India by any person."

a) clear and accessible statements of its practices and policies;

b) type of Sensitive Data collected;

c) purpose of use;

d) any disclosures to third party; and

e) security measures implemented.[34]

It appears that the information to be published by a body corporate or Data Processor may not be the information that is provided for general information purposes; the information may need to contain case specific details 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, and certainly such information would be Sensitive Data and confidential. If this obligation is to be strictly complied with, the corporation or Data Processor may have to provide such information to the Providers under restricted access to their website and not as public information. This interpretation appears too far-fetched, given that the consent of the Provider will have been obtained and that the Provider will therefore be informed of all the details that are required to be published as part of the privacy policy. Nevertheless, it cannot be ruled out without further clarifications.

### *2.11 Security measures*

The Data Privacy Rules require that the body corporate and the Data Processor implement reasonable security practices and standards; have a comprehensively documented information security program, and security policies. These must contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected and with the nature of business.[35]

The International Standard IS/ISO/IEC 27001 on 'Information Technology - Security Techniques - Information Security Management System - Requirements' is recognised as an approved security practices standard that the body corporate or the Data Processor could implement to comply with security measures under the Data Privacy Rules. Any other security standard approved by the Central Government may also be adopted by the body corporate or the Data Processor in compliance with the security measures under the Data Privacy Rules.[36]

The security standards adopted by the body corporate and the Data Processor should be audited by an auditor approved by the Central Government. The audit must be carried out at least once every year, or at such times as the body corporate or the Data Processor undertakes a significant upgrade of its process or computer resource.[37]

If there is an information security breach, the body corporate or the Data Processor will be required, upon request from a governmental agency, to demonstrate that it has

---

[34] Data Privacy Rules, Rule 4.

[35] Data Privacy Rules, Rule 8(1).

[36] Data Privacy Rules, Rule 5(3).

[37] Data Privacy Rules, Rule 5(4).

implemented the security control measures as per its documented information security program and information security policies.[38]

A corporation is required to designate a Grievance Officer to address the grievances of the Provider. The name and contact details of the Grievance Officer must be published on the website of the body corporate. The Grievance Officer must address the grievances within 1 month from the date of receipt of grievance.[39]

### *2.12 Penalties*

The Data Privacy Rules implement s 43A of the IT Act (s 22 of the *IT Amendment Act 2008*). Under s 43A, a body corporate that possesses, deals or handles Sensitive Data in a computer resource is liable to pay compensation if it is negligent in implementing and maintaining reasonable security practices and procedures, and such negligence results in wrongful loss or wrongful gain to any person.[40]

Section 43A fixes liability on a body corporate that is negligent in implementing security measures prescribed under the Data Privacy Rules if such negligence results in wrongful loss or wrongful gain to any person. The IT Act does not provide for specific penalties for breach of obligations under the Data Privacy Rules relating to collection, processing, disclosure or transfer of Sensitive Data.

Under s 72A of the IT Act (introduced by *IT Amendment Act 2008*), a person who is providing services under a lawful contract, may be liable to imprisonment for a term of up to 3 years or a fine up to Rs. 5,00,000 (Rupees Five Lakhs) for disclosure of personal information of any individual: (a) with the intent to cause, or knowing that he is likely to cause, wrongful loss or wrongful gain; and (b) without the consent of such individual, or in breach of lawful contract.

The IT Act does not define 'personal information'. It is however defined in the context of Sensitive Data under the Data Privacy Rules (that implement s 43A of the IT Act). There is confusion, therefore, as to whether the meaning of 'personal information' under the Data Privacy Rules can be attributed to the term 'personal information' under s 72A of the IT Act, and as a result bring within its purview the protection of Sensitive Data that forms a subset of 'personal information'. While s 72A may be relied upon to some extent for protection of 'personal information', it has its own limitations. Section 72A limits its application to 'personal information' obtained under a lawful contract. Further, while s 72A provides for criminal liability, it provides no compensation to the Provider.

Until clarity is achieved, recourse is available under a residuary provision[41] in the IT Act that requires any person contravening any provision of the rules or regulations under the IT Act to pay compensation of Rs. 25,000 (Rupees Twenty Five Thousand). Considering that the Data Privacy Rules seek to protect Sensitive Data Rs. 25,000 compensation is really minimal and of limited deterrent effect.

---

[38] Data Privacy Rules, Rule 8(1).

[39] Data Privacy Rules, Rule 5(9).

[40] IT Act, s 43A.

[41] IT Act, s 45.

## 3. Conclusion

Comprehensive data protection legislation that seeks to install a data protection regime covering both personal and data privacy is in the pipeline. A social movement to protect personal privacy of individuals, arising from the recent telephone tapping controversies in the Government, should act as an impetus for bringing into force the proposed data protection bill. Until then, there is an urgent need for clarification of the Data Privacy Rules in order to avoid the possibility of the application of several interpretations, resulting in complete confusion.