Morgan Lewis

outsourcing lawflash

alert

www.morganlewis.com

Recent Issuance of Privacy Rules in India May Impact Outsourcing Transactions

June 15, 2011

India has been under pressure from the outsourcing community for some time to implement standard rules regarding the protection of personal information. On April 13, India quietly issued final rules under its Information Technology (Amendment) Act, 2008 (the IT Act) regarding the protection of personal information (collectively, referred to as the "Privacy Rules"). The Privacy Rules include the following:

- Information Technology (Electronic Service Delivery) Rules, 2011
- Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (the Security Rules)
- Information Technology (Intermediaries Guidelines) Rules, 2011

Observers now are questioning whether the Privacy Rules have gone too far and will have unintended implications on outsourcing suppliers and customers, imposing in many cases more stringent requirements on the collection of personal information in India (for example, by India-based call centers) than those imposed by the home country of the individual from whom the data is being collected. Outsourcing suppliers and customers are in the process of analyzing the impact of the Privacy Rules on existing and new transactions where India service locations are used, including potential changes that are required to the infrastructure, standards, and processes used to support such outsourcing transactions.

This LawFlash is intended to highlight several key provisions of the Privacy Rules and their potential impact on outsourcing transactions.

Highlights of the Privacy Rules

As a general matter, the Privacy Rules apply broadly to the collection and use of personal information by an organization in India, regardless of whether the information is from or concerns individuals who are outside of India. Providers of outsourcing services appear to be subject to the Privacy Rules, with

liability exceptions in certain instances for "intermediaries" (such as network providers) that handle but do not process personal information.[1]

The Privacy Rules impose obligations regarding "personal information," with additional requirements applicable to personal information that falls within the definition of "sensitive personal data." "Personal information" is defined to include any information that is capable (separately or in combination with other information) of identifying any natural person.[2] "Sensitive personal data" means personal information which consists of information relating to the following:

- Password
- Financial information (e.g., bank account or credit/debit card details)
- Physical, physiological, and mental health conditions
- Sexual orientation
- Medical records and history
- Biometric information
- Any detail relating to the above items as provided to an organization for providing services
- Any of the information received under the above items by an organization for processing or stored or processed under a lawful contract or otherwise[3]

Key requirements of the Privacy Rules for personal information generally include the following:

- Policy requirements:
  - An organization that collects, receives, possesses, stores, deals, or handles any personal information must establish a privacy policy and make the policy available to individuals that provide personal information.[4]
  - The privacy policy must contain an explanation of the organization's reasonable security practices and procedures used to maintain the security of the personal information collected.[5] According to the Privacy Rules, an organization is deemed 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 commensurate with the information assets being protected with the nature of the business."[6] IS/ISO/IEC 27001 is specifically mentioned as one such standard.[7]
- Collection requirements:

1. Section 79 of the IT Act states that intermediaries (such as network providers) are not liable under the IT Act in certain cases. Under the IT Act, an "intermediary" is defined as any person who, on behalf of another person, receives, stores, or transmits an electronic record or "provides any service with respect to that record and includes telecom service providers, network service providers, internet service providers, web-hosting service providers, search engines, online payment sites, online-auction sites, online-market places and cyber cafes." Section 2(w) of the IT Act. It is unclear if this definition would be expanded to apply to all service providers or just a limited subset of service providers.

2. Section 2(i) of the Security Rules.

3. Section 3 of the Security Rules.

4. Section 4(1) of the Security Rules.

5. Section 4(1)(v) of the Security Rules.

6. Section 8 of the Security Rules.

7. Section 8 of the Security Rules.

- An organization that collects information must take steps to ensure that the person providing the information is aware that his or her information is being collected, the purpose for the collection, the intended recipients of the information, and the name and address of the organization collecting the information, as well as the organization retaining the information.[8]
- Prior to the collection of information, an organization that collects information must allow the provider of the information the option not to provide the requested data or information and the right to withdraw any consent previously given.[9]
- An organization that has collected information must provide individuals the right to access and correct personal information.[10]
- An organization that has collected information must designate a "Grievance Officer" for the purpose of addressing any discrepancies and grievances of the provider of information with respect to processing of information. The Grievance Officer must resolve grievances "expeditiously but within one month from the date of receipt of [the] grievance."[11]

In addition to the obligations highlighted above, with respect to any sensitive personal data, the Privacy Rules requires the following:

- An organization must obtain consent in writing through letter, fax, or email from the provider of the sensitive personal data prior to the collection of any such data.[12]
- Sensitive personal data may not be disclosed to any third party without the prior permission from the provider unless such disclosure has been agreed to in a contract or where the disclosure is necessary for compliance with a legal obligation.[13]
- Sensitive personal data may only be transferred to another organization or person in India or another country that ensures the same level of data protection as provided by the Privacy Rules.[14]
- Sensitive personal data may only be transferred if such transfer is necessary for the performance of the contract between the organization and the provider of the information or where the person has consented to the transfer.[15]

If an organization possessing, dealing, or handling any sensitive personal data or information in a computer resource that it owns, controls, or operates is negligent in implementing and maintaining reasonable security practices and procedures and thereby causes wrongful loss or wrongful gain to any person, such organization is liable to pay damages by way of compensation to the person so affected.[16]

---

8. Section 5(3) of the Security Rules.

9. Section 5(7) of the Security Rules. In the event the provider of information does not provide consent or later withdraws his/her consent, the organization does have the option not to provide the goods or services for which the information was sought.

10. Section 5(6) of the Security Rules.

11. Section 5(9) of the Security Rules.

12. Section 5(1) of the Security Rules.

13. Section 6(1) of the Security Rules. The Security Rules also prohibit further disclosure of the sensitive personal data by any third party once it has been disclosed under Section 6(1). See Section 6(4) of the Security Rules.

14. Section 7 of the Security Rules.

15. Section 7 of the Security Rules.

16. Section 43A of the IT Act.

Additionally, other failures to comply with the Privacy Rules are subject to fines and up to three years' imprisonment depending on the nature of the offense.[17]

Implications

Given the importance of outsourcing services to India and the potential impact that the Privacy Rules may have on the industry, many observers are questioning whether the burdensome requirements of the Privacy Rules will be relaxed, go unenforced, or be superseded by subsequent legislation. Clearly some clarifications and guidance will be required to allow organizations to comply with the Privacy Rules. For example, the prohibition on transfers of sensitive personal data are so broad that, while they would apply to data collected from a person in the United States, they may prohibit the transfer of such data back to an organization within the United States because the United States does not ensure "the same level of data protection that is . . . provided for under [the Privacy Rules]."[18] That would appear to be an unintended result of the current version of the Privacy Rules.

Until there is additional clarification on the Privacy Rules from the Indian government, customers and potential customers of Indian-based outsourcing suppliers must proceed on the basis that the Privacy Rules will be enforced as written. Accordingly, when negotiating an agreement with an outsourcing supplier that has operations in India, customers should account for the vendor's compliance with the Privacy Rules in the outsourcing agreement. Similarly, customers that have already contracted with an outsourcing supplier with operations in India should engage their vendors to determine how the outsourcing suppliers intend to comply with the Privacy Rules and should consider whether their own practices need to be changed to match the requirements created by the Privacy Rules.

If you have any questions or would like more information on the issues discussed in this LawFlash, please contact any of the following Morgan Lewis attorneys:

New York
Vito Petretti 212.309.6755 vpetretti@morganlewis.com

Palo Alto
Rahul Kapoor 650.843.7580 rkapoor@morganlewis.com

Philadelphia
Barbara Murphy Melby 215.963.5053 bmelby@morganlewis.com
Michael L. Pillion 215.963.5554 mpillion@morganlewis.com

Pittsburgh
Peter M. Watt-Morse 412.560.3320 pwatt-morse@morganlewis.com

17. Sections 72 and 72A of the IT Act. Section 72 of the IT Act provides that a person who secures "access to any electronic record, book, register, correspondence, information, document or other material without the consent of the person concerned discloses such electronic record, book, register, correspondence, information, document or other material to any other person shall be punished with imprisonment for a term which may extend to two years, or with fine which may extend to one lakh rupees [approximately, US$2,200], or with both." Further, Section 72A provides for harsher penalties for certain intentional conduct. ("[A]ny person including an intermediary who, while providing services under the terms of lawful contract, has secured access to any material containing personal information about another person, with the intent to cause or knowing that he is likely to cause wrongful loss or wrongful gain discloses, without the consent of the person concerned, or in breach of a lawful contract, such material to any other person shall be punished with imprisonment for a term which may extend to three years, or with a fine which may extend to five lakh rupees [approximately, US$11,100], or with both.").

18. Section 7 of the Security Rules.

About Morgan, Lewis & Bockius LLP

With 22 offices in the United States, Europe, and Asia, Morgan Lewis provides comprehensive transactional, litigation, labor and employment, regulatory, and intellectual property legal services to clients of all sizes—from global Fortune 100 companies to just-conceived startups—across all major industries. Our international team of attorneys, patent agents, employee benefits advisors, regulatory scientists, and other specialists—nearly 3,000 professionals total—serves clients from locations in Beijing, Boston, Brussels, Chicago, Dallas, Frankfurt, Harrisburg, Houston, Irvine, London, Los Angeles, Miami, New York, Palo Alto, Paris, Philadelphia, Pittsburgh, Princeton, San Francisco, Tokyo, Washington, D.C., and Wilmington. For more information about Morgan Lewis or its practices, please visit us online at www.morganlewis.com.