SUTHERLAND

LEGAL ALERT

August 9, 2011

Outsourcing: India Adopts New Privacy and Security Rules for Personal Information

Effective with their publication on April 11, 2011,[1] the Central Government of India (GOI) adopted the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Data or Information) Rules, 2011 (Rules), under Section 43A of The Information Technology Act, 2000, as amended by The Information Technology (Amendment) Act, 2008 (IT Act). The Rules define certain key, previously undefined, terms used in that Section and otherwise impose India's first significant personal information privacy and data security regime.

These Rules have spawned widespread concern and debate regarding their interpretation. As discussed in this Legal Alert, literally read, the Rules impose extremely burdensome obligations relating to the collection of personal information by companies with no other contacts with India other than the utilization of outsourcing services provided from inside India. It has been recently reported that the CEO of the Data Security Council of India[2] has stated that they have discussed these concerns with the GOI and expect that the GOI will clarify their interpretation of the rules in the near future.

Sutherland does not advise on Indian law, but has been in contact with legal advisers in India regarding the Rules and does regularly advise clients engaging service providers in India under various outsourcing arrangements.

New Rules Present Potential Compliance Challenges to Outsourcing Customers

As written, the Rules are more restrictive than those prescribed by the Gramm-Leach-Bliley Act and the EU Privacy Directive and can extend beyond India to any contravention of the IT Act committed outside of India by any person if a computer, computer system or computer network located in India is involved.[3] There is no transition period for implementing the Rules, nor is there any "grandfathering" of prior practices with respect to the personal information collected prior to the date the Rules became effective.

The Rules apply not only to companies collecting and handling personal information in India, but also potentially to companies collecting personal information outside of India and either sending it to India for hosting, processing or other handling or permitting it to be accessed by computer systems located in India. Where "sensitive personal data or information" (as defined by the Rules and discussed further below) is involved, enhanced notice and consent safeguards are required. The mandates of the Rules fall into the categories of: (1) providing notice to and obtaining consent from the information provider regarding (a) the fact that the information is being collected,(b) the purposes for which the information is

---

[1] *The Gazette of India, Extraordinary*, Part II, Section 3, Sub-section (i), dated 11 April 2011, and Rules, Sec. 1(2).

[2] The Data Security Council of India is a not-for-profit company, established by NASSCOM to promote data protection and to develop security and privacy codes and standards for the IT/BPO sector. NASSCOM is the premier trade body and chamber of commerce for the IT-BPO industries in India.

[3] IT Act, Secs. 1(2) and 75.

being collected, (c) the intended use of the information, and (d) the disclosure and/or transfer of the information to third parties; (2) establishment of and compliance with grievance resolution procedures; and (3) compliance with prescribed security practices and procedures to protect personal information. The consequences of the failure to comply with the Rules at present appear to be those prescribed under the IT Act. The "teeth" under the IT Act are contained in Sections 43A, 72 and 72A, which are described in greater detail below. These sections provide for a private cause of action for damages resulting from the negligent failure to maintain "reasonable security practices and procedures" to protect "sensitive personal data or information" (Section 43A) and penalties (fines and/or imprisonment) for unauthorized disclosure of personal information (Sections 72 and 72A).

Pending clarification of the Rules by the GOI, it would be prudent for all outsourcing customers utilizing Indian service providers to process, otherwise handle or access personal information (wherever that information was collected) to undertake an analysis of the following: (1) how the Rules might impact the services being provided to the customer in or from India and/or the provider of the services; (2) whether the existing outsourcing agreement with the Indian service provider adequately protects the customer from violation of the Rules by the service provider; (3) how the Rules might impact the personal information collection and handling activities of the customer outside of India; (4) whether it is practical or even possible for the customer to modify its personal information collection practices and procedures in a way that would enable it to comply with the Rules; (5) the potential financial and/or reputational risks posed by the Rules to the customer; and (6) options for alternative service provider arrangements, if the application of the Rules is not satisfactorily limited by the GOI.

Since a broad, yet not unreasonably expansive, reading of the Rules would have an adverse impact on two of India's most important industry sectors (IT-BPO), by not only imposing burdensome and expensive requirements on the India-based service providers, but also on their offshore customers, it is generally assumed that the Rules will be "clarified" by the GOI to substantially narrow their potential scope.

If the customary process in India for working through new laws, rules and regulations is followed in the case of the Rules, it would be expected that there will be future pronouncements by the GOI providing "clarification," either through further rulemaking or other clarifying interpretations. Depending on the severity of the reaction to the Rules, conceivably the Indian Parliament could take action.[4] Consequently, a prudent course of action for companies outsourcing to India is to take a "wait and see" approach. Changes in practices and procedures that can be implemented without significant expense should be considered, but otherwise it is premature to implement significant or otherwise expensive changes in policies, processes and procedures, as later they may prove to have been unnecessary or not the optimal solutions.

Relevant Provisions of the IT Act

Failure to Implement/Maintain Reasonable Security. Section 43A of the IT Act provides, in summary, that where a body corporate[5] 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

[4] The Personal Data Protection Bill, 2006, has been pending before the Indian Parliament since its introduction in 2006.

[5] The IT Act defines a "*body corporate*" as "any company and includes a firm, sole proprietorship or other association or individuals engaged in commercial or professional activities."

reasonable security practices and procedures" and thereby causes wrongful loss or wrongful gain to any person, such body corporate can be held liable to pay damages to the person affected.[6]

Unauthorized Disclosure. Section 72 of the IT Act provides for a fine and/or imprisonment of any person who discloses any lawfully obtained confidential or private information without the consent of the person concerned. Section 72A of the IT Act provides for fines and/or imprisonment of any person who discloses personal information acquired while providing services under the terms of a lawful contract without the consent of the person concerned or in breach of a lawful contract, where such actions were taken with the intent to cause, or with the knowledge that the action is likely to cause, wrongful loss or wrongful gain. The penalties under Section 72A are more severe than those under Section 72 due to the added requirement under Section 72A of the element of an actual intent to cause harm.

Significant Requirements of Rules Highlighted

The following is a summary of some of the more significant requirements of the Rules.

A. *All Personal Information*

1. Privacy policies must be adopted and published, on the websites of the collector of personal information, as well as by any other entity that receives, possesses, stores, deals or handles the information, that comply with the requirements of the Rules as to content. Additionally, the Rules require that the information collector and the service provider ensure that these policies "are available for view" by the information provider. The Rules do not explain what actions are sufficient to satisfy this additional requirement. This requirement must be considered in the context of the customer's collection of personal information outside of India, as well as collection of personal information by the service provider on behalf of the customer in India.

2. During the collection of any personal information, reasonable steps must be taken to ensure that the information provider knows: (i) that the information is being collected; (ii) the purpose for which the information is being collected; (iii) the intended recipients of the information; and (iv) the name and address of the agency collecting the information and the agency that will retain the information. The Rules do not provide guidance on what constitutes such reasonable steps.

3. Personal information can be used only for the purpose for which it has been collected.

4. Providers of all personal information must be afforded the right to review and correct inaccuracies and deficiencies and a grievance procedure must be implemented that complies with the Rules, including resolving all grievances within one month of receipt.

5. Personal information must be secured in accordance with the requirements of the Rules.

[6] The measure of damages resulting from a wrongful loss or a wrongful gain remains subject to clarification.

B. *"Sensitive Personal Data or Information"*

1. Before collecting "sensitive personal data or information," written consent from the information provider in the form of a letter or fax or email regarding the purpose and usage of the information must be obtained.

2. "Sensitive personal data or information" may be collected only for a lawful purpose that is necessary for the activity conducted by the collector of the information.

3. Any transfers or disclosures of "sensitive personal data or information" require the consent of the provider.

4. The provider of "sensitive personal data or information" must be advised of the option not to provide the information, and consent to collection previously given may be later withdrawn in writing. Provision of services to the provider of the "sensitive personal data or information" can be conditioned on the information provider's continuing consent to provide the information.

Key Terms of Section 43A Defined by Rules

The Rules define the previously undefined key terms in Section 43A as follows:

> "*Personal information*" is defined as any information that relates to a natural person that alone or together with other information available with a corporate body is capable of identifying such person.[7]
>
> "*Sensitive personal data or information*" is defined as personal information that consists of information relating to: (1) password; (2) financial information such as bank account or credit card or debit card or other payment instrument details; (3) physical, physiological and mental health condition; (4) sexual orientation; (5) medical records or history; (6) Biometric (as defined) information; (7) any detail relating to the foregoing as provided to a body corporate for providing a service; and (8) any of the foregoing information received by a body corporate for processing or stored or processed under contract or otherwise. Excluded from this definition is information "furnished under the Right to Information Act, 2005 or any other law for the time being in force."
>
> *"Reasonable security practices and procedures*" shall be considered to have been complied with by a body corporate or a person acting on behalf of a body corporate "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 that are commensurate with the information assets being protected with the nature of business."[8] The Rules appear to provide a "safe harbor" to the extent the body corporate, or person acting on its behalf, possessing or processing the information: (1)(a) implements security control measures prescribed by the International Standard IS/ISO/IEC 27001 on "Information Technology – Security Techniques – Information Security

---

[7] The term "*information*" is defined in the IT Act as "data, text, images, sound, voice, codes, computer programmes, software and databases or micro film or computer generated micro fiche."

[8] Rules, Sec. 8(4).

Management System – Requirements"[9] or (b) best practices prescribed by an industry association and approved by the GOI; and (2) obtains an annual audit certifying such compliance.

Published Privacy Policy Required for Collectors/Handlers of Personal Information

The body corporate or person acting on its behalf that collects, receives, possesses, stores, deals or handles any personal information of a provider must: (1) provide a privacy policy for handling or dealing in personal information; (2) ensure that the same is available for view by the provider of the information; and (3) publish its privacy policy on its website. The principal contents required for the privacy policy are set out in the Rules.[10]

Notification Obligations Applicable to Personal Information

When collecting information directly from a person, the body corporate or person acting on its behalf must take reasonable steps to ensure that the person concerned has knowledge that the information is being collected and of the details regarding the purpose for collection, the intended recipients, and the name and address of the collecting agency and agency who will retain the information.[11]

Consent Required to Collect "Sensitive Personal Data or Information"

The body corporate or person acting on its behalf must obtain consent in writing of the provider of "sensitive personal data or information" regarding the purpose and usage of the information in the form of a letter, fax or email.[12]

Prior to the collection of any "sensitive personal data or information," the collecting body corporate or person acting on its behalf must provide an option to the provider of the information not to provide the data. At any time after having provided the "sensitive personal data or information," the provider of the information can withdraw consent to collection of the information in writing. The collecting corporate body may condition providing goods or services upon the provider continuing to provide the information.[13]

---

[9] This is an Information Security Management System (ISMS) standard published in October 2005 by the International Organization for Standardization and the International Electrotechnical Commission. The standard specifies the requirements for establishing, implementing, operating, maintaining and improving a documented ISMS within the context of an organization's overall business risks. A company's ISMS may be certified as compliant with this standard by an Accredited Registrar or other accredited certification body.

[10] Rules, Sec. 4(1). The Privacy Policy must contain: (1) clear and easily accessible statements of its practices and policies; (2) the type of personal or sensitive personal data or information collected; (3) the purpose of collection and usage of such information; (4) the intended disclosure of information including sensitive personal data or information; and (5) the reasonable security practices and procedures as required under the Rules.

[11] Rules, Sec. 5(3).

[12] Rules, Sec. 5(1).

[13] Rules, Sec. 5(7). The Rules do not explain the actions required of the holder of the information once consent previously given has been withdrawn. Presumably, the information must be removed from the records of the entity holding the information, although this answer must await further clarification from the GOI.

Limitations on Use of "Sensitive Personal Data or Information"

No body corporate or person acting on its behalf is permitted to collect "sensitive personal data or information" unless: (1) it is for a lawful purpose connected with a function/activity of the collecting body corporate; and (2) collection of the information is considered necessary for that purpose.[14] Any information collected must be used only for the purpose collected.[15] The body corporate or person acting on its behalf must not retain "sensitive personal data or information" longer than is required for the permitted use or as otherwise required by law.[16]

Obligation to Correct Inaccuracies and Address Grievances Relating to Personal Information

The body corporate or entity acting on its behalf must permit the providers of personal information to review the information they have provided and must correct any inaccuracies and deficiencies in personal information.[17] The body corporate must address any discrepancies and grievances of the provider of the information within one month of receipt of the grievance and must appoint a "Grievance Officer" to handle grievances and publish that officer's name and contact information on the body corporate website.[18]

Consent Required for Disclosure of "Sensitive Personal Data or Information"

Disclosure of "sensitive personal data or information" requires the prior permission of the provider, except in the case of disclosure to a Government agency upon proper written request or order under any law in force. Prior permission for disclosure can be given by the provider in a contract with the corporate body. The "sensitive personal data or information" cannot be published by the corporate body or person acting on its behalf[19] and any third party to whom the information is provided pursuant to the permission of the information provider is not permitted to disclose the information further.[20]

Consent Required for Transfer of Sensitive Personal Data or Information

A body corporate or person acting on its behalf may transfer "sensitive personal data or information" to another body corporate or person in or outside of India, so long as that entity/person ensures the same level of data protection as required by the Rules. The transfer must be necessary for the performance of a

---

[14] Rules, Sec. 5(2).

[15] Rules, Sec. 5(5).

[16] Rules, Sec. 5(4).

[17] Rules, Sec. 5(6).

[18] Rules, Sec. 5(9). No other details are provided by the Rules as to how grievances are to be addressed.

[19] Rules, Sec. 6(3).

[20] Rules, Sec. 6(4). The prohibition on the third party receiving the information from disclosing it further would appear to restrict further downstream distribution of the information.

contract between the corporate body and the provider of the information or the provider must have consented to the transfer.[21]

Data Security Requirements

Personal information must be kept secure by the body corporate or person acting on its behalf holding the information in accordance with "reasonable security practices and procedures" (see discussion above).[22]

What the Rules Mean for Customers Utilizing Service Providers in India

Clearly the Rules may potentially complicate the decision by any customer considering outsourcing to India that involves either the collection of personal information in India, the sending to India of personal information collected elsewhere, or the accessing by Indian service providers of personal information residing outside of India. At present, the consequences of non-compliance with the Rules are unclear, beyond the potential liability imposed by Sections 43A, 72 and 72A of the IT Act described above. While Sections 72 and 72A are not new and the Rules do not directly expand their application, the issuance of the Rules may be an indication of an intent by the GOI to enforce these sections more aggressively. Any customer potentially impacted by the Rules should monitor the public announcements that will inevitably be forthcoming from the GOI relative to the application and interpretation of the Rules.

Below we discuss concerns raised by the Rules, in their current form, for customers utilizing outsource service providers in India who "touch" personal information collected by the customer inside or outside of India.

Compliance With Laws of the Collection Jurisdiction May Not Protect Customers. The Rules appear to apply to all personal information whether or not relating to a citizen of India and whether collected in India or elsewhere. In other words, the Rules appear to have extraterritorial application with the only required nexus to India being the use of an Indian computer system to process, store, handle or merely access the information. The Rules provide no express or even implied "safe harbor" for compliance with the data collection and other privacy requirements of the country where the personal information was originally collected. Since this interpretation would have the practical effect of preempting foreign privacy laws, it is not likely that such an interpretation of the Rules will prevail. At present, however, there is no clear guidance on this.

Assurances of Compliance With Rules From Service Providers. Customers outside of India providing data containing personal information to a service provider located in India (including permitting the Indian service provider to access personal information residing on the customer's systems outside of India) or engaging a service provider located in India to collect personal information in India, whether from sources within or outside of India (such as might be the case in call center operations) should require a confirmation from the service provider that it is compliant with the Rules or, if not, that it has a plan in place to become compliant. Customers will want to take these precautions to protect against the charge that the service provider was acting in the capacity as the agent of the customer when it violated the Rules. All new arrangements with service providers in India should contain express requirements that the service provider comply with the Rules to the extent that they apply to the services being rendered.

---

[21] Rules, Sec. 7.

[22] Rules, Sec. 5(8).

Customer Obligations Under the Rules. Customers may receive inquiries from their Indian service providers regarding the customer's data collection, privacy and security practices to determine if they are compliant with the Rules. For instance, where "sensitive personal data or information" is transferred to India or accessed from India, whether it is collected from providers inside of India or from providers located outside of India, the Rules require that certain consents be obtained in connection with the original collection of the information, as well as for the transfer (including access) of the information to the Indian service provider. Where compliance with the Rules is impractical, expensive or disruptive to the customer's operations, customers should avoid precipitous actions until clarification regarding the interpretation and enforcement of the Rules is forthcoming.

Indemnities. Indemnity provisions in existing outsourcing contracts should be analyzed to determine if the customer is adequately protected from potential liability arising from non-compliance with the Rules by the service provider. All future outsourcing contracts should include provisions providing specifically for such indemnity. Reciprocal indemnities may be requested by the service provider.

Certifications of Reasonable Security Practices and Procedures. The Rules prohibit the transfer of personal information to any service provider that does not comply with the Rules security requirements. It should be assumed that "transfer" includes accessing the information. Customers should specifically require outsource service providers in India processing, handling or accessing personal information to obtain IS/ISO/IEC 27001 compliance certifications or alternative certification of compliance with GOI approved industry best practices, in each case on an annual basis. The question remains whether such a certification would satisfy a U.S. customer's requirements relative to the service provider's system of internal controls over financial reporting (SOC 1 type 2 reports (formerly SAS 70 reports)) and issues relating to security, availability, processing integrity, confidentiality and privacy (SOC 2 type 2 reports) or whether such reports will be required in addition to the annual certification required by the Rules. Customers may receive inquiries from Indian service providers regarding the customer's security practices and procedures to test them against the Rules' requirements, since any transfer of personal information from India would be governed by the Rules.

Website Content. Customers will need to compare their published privacy policies with the requirements of the Rules.

Notice Requirements. Customers will need to consider methods available to it to provide the information required by the Rules to providers of personal information.

Consent Requirements. If a customer is collecting "sensitive personal data or information," it should consider the feasibility and methods available to obtain the prior written consent of the provider approving the purpose and usage and any anticipated transfers or disclosures of the information. The Data Security Council of India has stated that it is likely that, notwithstanding the Rules requirement for "paper" consents, electronic consents will likely be acceptable.

Error Corrections; Grievance Resolution Process. Customers should consider if their processes and procedures for correction of inaccuracies and deficiencies in personal information and for addressing grievances by information providers meet the Rules requirements and, if not, whether they can/should be modified to do so.

Service Provider as Collector of Personal Information. If the service provider is collecting personal information in India on behalf of the customer (e.g., customer service call center operations), it is likely

that new procedures will be required to be implemented by the service provider to ensure compliance with the Rules.

Accessing Information Only. Pending clarification of the Rules, customers should assume that, if a service provider in India is accessing the personal information, it will be treated the same as a "transfer" of the information under the Rules.

Risk of Suit in India. Customers collecting or otherwise handling "sensitive personal data or information" relating to Indian citizens outside of India that are at any point "touched" by a computer system located in India could be subject to suit in India for any violation of Section 43A of the IT Act. As a practical matter, customers with operations in India would likely be more at risk from such a threat than those without such operations.

Allocation of Cost of Compliance. Outsource service providers in India collecting or otherwise handling personal information will likely incur increased costs related to compliance with the Rules. These costs will, if not immediately passed through to the customer, inevitably be passed through over time, thereby increasing the costs of outsourcing to India. These costs, added to the costs incurred by the customer to comply with the Rules, could affect the equation relative to assessing the cost advantages of outsourcing to India over other alternatives.

■ ■ ■

If you have any questions about this Legal Alert, please feel free to contact any of the attorneys listed below or the Sutherland attorney with whom you regularly work.

Scott M. Hobby	404.853.8051	scott.hobby@sutherland.com
Charles F. Hollis III	404.853.8100	chuck.hollis@sutherland.com
Derek C. Johnston	404.853.8099	derek.johnston@sutherland.com
John B. Miller, Jr.	404.853.8095	jay.miller@sutherland.com
Peter C. Quittmeyer	404.853.8186	peter.quittmeyer@sutherland.com
Timothy R. Dodson	404.853.8109	tim.dodson@sutherland.com