CLIENT ALERT

GOVERNMENT NOTIFIES DATA PRIVACY RULES UNDER THE INFORMATION TECHNOLOGY ACT, 2000

In Brief

On April 11, 2011, the Government of India notified the Information Technology (Reasonable Security Practices and Procedures and Sensitive Personal Date or Information) Rules, 2011 (the "**Rules**') under the Information Technology Act, 2000 (the "**IT Act**"). The Rules regulate the manner in which bodies corporate collect, handle, distribute, disclose and transfer personal data of individuals.

BACKGROUND

Under the IT Act, "bodies corporate" are liable if they are negligent in implementing and maintaining "reasonable security practices and procedures" to protect "sensitive personal data or information".

DEFINITIONS

The term "***bodies corporate***" includes "a firm, sole proprietorship or other association of individuals engaged in commercial or professional activities".

The Rules have defined the term "***personal information***" to mean any information that relates to a natural person and which is capable of identifying that person. Corporations or other legal persons are thus excluded.

The term "***sensitive personal data or information***" has been defined to mean personal information that contains information such as passwords; financial information; physical, physiological and mental health condition; sexual orientation; medical history and records and biometric information.

"***Reasonable security practices or procedures***" are those security practices and procedures which are contractually specified or are specified in any law. In the absence of such contract or law, "reasonable security practices or procedures" include a comprehensive documented information security programme and information security policies. The information security policies should contain managerial, technical, operational and physical security control measures that are commensurate with the information assets being protected.

COLLECTION, DISCLOSURE AND TRANSFER

Under the Rules, sensitive personal data or information may only be collected for a lawful purpose that is related to the function or activity of the entity collecting it and even then only after obtaining consent. Such data once collected can only be used for the stated purpose, should be held securely and only for as long as necessary to achieve the purpose. Sensitive personal data or information cannot be disclosed to a third party without prior permission unless there is a contract to the contrary or if required in order to comply with a legal obligation. Any third party recipient cannot disclose it further. At all times, sensitive personal data or information must only be transferred to another body corporate that ensures the same level of data protection as provided under the Rules.

PRIVACY POLICY

Corporate entities are obliged to set out a privacy policy describing the manner in which they handle personal information. The policy should list the types of sensitive personal data or information collected by the body corporate; the purpose for collection and usage; the restrictions on its disclosure and the security practices and procedures adopted.

IMPACT ON BUSINESS

With the enactment of the Rules, corporate entities are forced to re-examine the manner in which they deal with sensitive information or data. They will now have to put in place policies and agreements in relation to the handling of information and comply with the practices and procedures prescribed by the Rules. Failure to do so will bring with it the risk of compensatory damages.