

INDIA IMPLEMENTS BRAND-NEW DATA PROTECTION LAWS

India has recently amended its Information Technology Act of 2000 (the “ITA”), adding much-anticipated provisions on data protection, cybercrimes, ISP liability, and electronic signature authentication. The Indian Ministry of Communications and Information Technology is now in the process of drafting further rules per the recommendations of NASSCOM (the IT industry advising body) and the Data Security Council of India’s (DSCI). As soon as the Ministry completes its review process, the amendments will be binding and impact all countries doing business with or in India.

A general increase in cybercrimes and the terrorist attack in Mumbai on November 26, 2008 likely expedited the passing of the ITAA. The rapid growth of India’s outsourcing and IT sectors (where data processing is a key component) has also likely contributed toward the ITAA’s passage. The ITAA represents an investment in India’s data security infrastructure. Most importantly, the amendment sends a strong message to the rest of world that India is still a secure place to do business.

Key Provisions of the Information Technology Amendment Act

The Information Technology Amendment Act (ITAA), as the act is called, will **require all foreign corporations with offshore Indian service partners to maintain “reasonable security practices and procedures” when handling “sensitive personal data”** on their computer systems (Section 43A). The statutory definitions of “reasonable security practices” and “sensitive personal data,” etc. are currently being finalized.

However, as NASSCOM’s and DSCI’s recommendations now stand, **“reasonable security practices”** will likely require organizations to document their security controls standards and processes. In the event of a security breach, the organization will need

to demonstrate conformity with the procedures and that the procedures commensurate with the assets being protected.

The ITAA’s definition of **“personal data”** will likely be information which directly or indirectly identifies a person, whether by reference to an identification number or the person’s physical, economic, cultural, physiological, or mental details. This definition is consistent with the EU Privacy Directives. Indeed, the ITAA introduces the concept of “personal data” into Indian law. While the original Act punished unauthorized data extraction and/or damage to data, it did not include this provision.

Finally, the ITAA’s definition of **“sensitive personal data”** on the other hand may exclude references to racial or ethnic origins and political or religious beliefs. This stands in marked contrast to the EU’s Directives.

For companies doing business in or with India, it will therefore be imperative to be familiar with Section 43A of the ITAA and its particular definitions for key terminology. It clearly has important implications for the Indian outsourcing industry and its partners in other countries.

Moreover, the ITAA also expands liability for data use from individuals to include corporations. A company’s failure to ensure that data in their possession is secure creates a private right of action in the individual whose sensitive personal information is compromised.

The ITAA represents a major step towards setting up strong data protection laws for Indian businesses and foreign partners alike. However, many details remain to be ironed out by the Ministries and their advising body, the DSCI, before we can ascertain the impact of this law on outsourcing transactions.

On another topic, the ITAA also expands the scope of cybercrimes by including cyberterrorism, increases some of the penalties for cybercrimes, and includes enhanced data retention, access, and cooperation requirements for intermediaries such as ISPs and network and telecom partners.

Tips for Businesses

In light of the modifications created by the ITAA, as a company conducting business in or with India, it is advisable that you revisit your contracts with India to ensure that they have adequately addressed data protection issues. You should also revise any long-term contracts where the data security provisions are outdated or inadequate in light of the ITAA modifications.

The following are some tips to consider when evaluating your existing outsourcing contracts with Indian partners:

- Evaluate your Indian partner's information security practices and procedures, and ensure that the partner resolves any gaps or deficiencies.
- Ensure that your outsourcing agreement expressly requires your Indian service partner to comply with the ITAA and any other data protection laws applicable.

- As long as the Indian Government has not yet specified the appropriate security procedures, your outsource agreement should also require your company to comply with industry-recognized security standards (ex: the Payment Card Industry Security Standard).
- Your outsourcing agreement should address the definition of a "security breach".
- Your agreement should include thorough audit rights, so you may verify that your partner is fulfilling its obligations.
- Your agreement should additionally provide for document remedies in case of non-compliance, including indemnities, terminations rights, etc.
- The agreement should also lay out the partners' liability for direct and indirect damages for security breaches.

Ultimately, until India formally adopts the ITAA via publication in the Official Gazette, with "sensitive personal data" defined and "reasonable security practices and procedures" specified, companies considering outsourcing their operations to an Indian partner are advised to carefully examine contracts before undergoing moving operations involving critical data with an Indian offshore partner.

By Annabelle RICHARD, Avocat à la Cour and Attorney at Law (New York Bar), and Arya SHEKAR, legal assistant.

Ichay & Mullenex Avocats is a French law firm focusing on all legal issues related to the new technologies in France and abroad. They are considered experts in intellectual property and Internet law, e-commerce, online gaming, data protection. Ichay & Mullenex Avocats also assists its clients on all issues related to financing, mergers & acquisitions, restructuring, etc. and advises them on their litigation and arbitration procedures.

5, rue de Monceau 75008 Paris - France
Tel : +33 1 42 89 19 80
Fax : + 33 1 42 89 14 99
www.ichay-mullenex.fr