



India poised to tighten data protection law



22 Apr 2004 11:48

India is likely to have a tighter data protection and privacy regime in place later this year, after bowing to pressure from...

India is likely to have a tighter data protection and privacy regime in place later this year, after bowing to pressure from Western users of outsourcing services.



The National Association of Software and Service Companies (NASSCOM) in Delhi is confident that new measures will be passed as law in the coming session of India's parliament, said Kiran Karnik, president of NASSCOM which is working closely with the government on the new rules.

India's elections for a new federal government started on Tuesday, and the new parliament, required to take up the new legislation for data protection, will be installed by 6 August.

"It is becoming extremely important for India to have in place a distinctive legal regime promoting data protection," said Pavan Duggal, a Delhi-based cyber law consultant. "This is necessary to create appropriate confidence among investors and foreign companies to the effect that the data they send to India for back-office operations is indeed safe, and there are appropriate statutory mechanisms in place should a breach of data take place."

Opponents of offshore outsourcing to India have often cited the absence of a data protection and privacy law in India as a strong reason for stopping the movement of call centre and BPO work to the country.

Labour MEPs affiliated with trade union Amicus said they would ask the European Commission to protect British consumers whose personal data is being transferred to India, warning that offshore outsourcing is "an accident waiting to happen".

Rather than have a separate law to deal with data security and privacy issues, the government is considering an amendment to its Information Technology Act of 2000. NASSCOM is in the process of inserting new clauses in the IT Act 2000, and these are being reviewed by the government.

The act in its existing form only covers unauthorised access and data theft from computers and networks, with a maximum penalty of about \$220,000, and does not have specific provisions relating to privacy of data. The new clauses are likely to enable the act to conform to the so-called adequacy norms of the European Union's Data Protection Directive and the Safe Harbor privacy principles of the US, according to NASSCOM.

The adequacy norms allow the EU to declare that third-party countries have levels of data protection that conform to European standards and thus allow data on EU citizens to be transmitted outside of the union.

Government officials were not available for comment, but according to informed sources, after the new rules are in force, India will negotiate with

the EU to get it to recognise India as a country that offers an adequate level of protection for personal data.

Until a tighter data protection legal regime is in place, foreign customers are relying upon contractual obligations to impose obligations for protecting and preserving data, according to Duggal.

"However, foreign customers are, increasingly, realising that such contractual obligations are not necessarily the best effective remedy available," said Duggal.

"This is so because in the event of a breach of the security of data, getting effective remedy under the contractual obligations is itself problematic, time consuming and self defeating. Having appropriate statutory protection with stipulated statutory penalties, damages and other remedies would act as a good deterrent against the breach of data privacy."

Duggal added that the government should consider penalties up to between \$5.5m to \$11m for breaches of data.

Even though the government has delayed the implementation of a legal framework for prosecution of data and privacy breaches, Indian BPO companies have implemented processes such as the BS7799 standard for information security management.

"Clients expect outsourcing companies they do business with in India to provide at the process level the same capability to ensure privacy, confidentiality, and security of data that their local outsourcers have," said Prakash Gurbaxani, chief executive officer of TransWorks Information Services, a Mumbai-based BPO and call centre company.

Standards such as BS7799, and the ISO17799 standard for information security, restrict the quantity of data that can be made available to employees of BPO and call centres.

"One of the things that you do, for example, is that you make sure that the agent workstation has no other software than is required for the job, has no internet access that could be potentially used to e-mail say a credit card number to someone else," said Gurbaxani. "You also ensure that the office is paperless so that no data can be copied out."

Despite these checks, there has been some fraud in the Indian BPO industry. One case reported was of an employee in a call centre in Noida, who last year misused the credit card and other details of a US citizen to buy electronics equipment from Sony.

"He was caught, arrested and subsequently convicted for online cheating in the subcontinent's first cyber crime conviction," said Duggal, who was the counsel for Sony.

Stray cases of fraud should not however be blown out of proportion to make it appear that fraud is widespread in India's BPO industry, according to industry sources. The risks of BPO operations, such as fraud prevention, are risks that all financial services companies have to deal with irrespective of what countries they operate in, Karnik said.

CW+ Features



E-Handbook
[Online domain maturity](#)



E-Handbook
[CEB IT Budget Benchmark 2015 to 2016](#)



E-Handbook
[A Computer Weekly Buyer's Guide to Next-Generation Service Management](#)

John Ribeiro writes for IDG News Service

[Read more on IT outsourcing](#)

GMB union gets good response from MPs over British Airways IT outsourcing concerns

GMB takes concerns over British Airways IT outsourcing to MPs

Ofcom outsources IT management to Indian services supplier NIIT

Top 10 IT outsourcing stories of 2015

Load More

0 comments

Oldest

Share your comment

Send me notifications when other members comment.

Register or Login

E-Mail

email@techtargt.com

Username / Password

Username

Password

Comment

By submitting you agree to receive email from TechTarget and its partners. If you reside outside of the United States, you consent to having your personal data transferred to and processed in the United States. Privacy

-ADS BY GOOGLE

SearchCIO

Four ways to build a successful CIO-CEO relationship

Digital business is having a profound effect on the CIO-CEO relationship. Here's how CIOs can seize the moment.

Digital business disrupts CIO-CEO relationship

Technology is a top-three business priority for 25% of CEOs, according to Gartner, paving the way for CIOs to play a more ...

[About Us](#) [Contact Us](#) [Privacy Policy](#) [Our Use of Cookies](#) [Videos](#) [Photo Stories](#)

[Guides](#) [Advertisers](#) [Business Partners](#) [Media Kit](#) [Corporate Site](#) [Experts](#)

[Reprints](#) [Archive](#) [Site Map](#) [Events](#) [E-Products](#)

All Rights Reserved,
Copyright 2000 - 2016, TechTarget