Legal and Regulatory Update

Data security and offshoring

Belinda Haden

Received (in revised form): 12 September 2005

Belinda Haden

joined CM Insight in 2003. In addition to her hands-on consultancy role, she has focused on the company's programme for quality and on research into key developments in the contact centre markets. Her background in research and analysis has enabled her to author several white papers, including the UK Contact Centre Industry study for the DTI (offshore section) and several client-driven papers on contact centre industry issues and developments. Operational projects have included call centre audits, offshore transition and risk management.

Keywords: data security, offshore, data protection, India

Abstract

This paper addresses how organisations can ensure that personal data are protected when outsourcing call centres offshore.

Introduction

Recent stories in the tabloid press suggesting that customers' personal data have been offered for sale by workers in Indian call centres have called into question security of data when Western companies outsource business functions offshore. *The Sun* newspaper revealed in June 2005 that an Indian ex-call centre employee had sold its reporter financial data about 1,000 UK bank customers for £3 per record.

The story appears to imply that the UK Data Protection Act of 1998 covers data security requirements within the UK, but that outsourcing work to offshore destinations automatically moves data security outside the jurisdiction of UK and European data laws. Any average reader could be forgiven for assuming that, if their data are in the hands of a company that has placed work offshore, their data are not protected by law. This is far from the truth, as this paper will show.

Data Protection Act 1998

The 1998 Data Protection Act makes a number of requirements, many of which pertain to the privacy of data and the rights of individuals to expect their data to be handled and stored securely. Specifically, data controllers must comply with the Act's eight principles of good information handling practice. The principles require personal data to be:

- processed fairly and lawfully
- processed only for limited purposes
- adequate, relevant and not excessive
- accurate
- not kept longer than necessary
- processed in accordance with individuals' rights
- kept secure
- not transferred to countries outside the European Economic Area (EEA) without adequate protection.

It is the seventh and eighth principles, then, that are relevant to the recent alleged security breaches. It is worth noting, also, that the Act does not expressly forbid transfer out of the EEA, simply transfer without adequate protection.

Data security and transfer

Belinda Haden
CM Insight
The Old Warehouse
Church Street
Weybridge
Surrey KT13 8DG, UK
Tel: +44 (0)1932 268100
E-mail: belinda.haden@cm-insight.com

Sending data overseas

If your company is sending personal data to other countries within the EEA (the 25 member states of the European Union, plus Iceland, Liechtenstein and Norway), then the UK Data Protection rules allow you to transfer data without further provision. But, since some of the new Central and Eastern European member states may not yet have enacted data protection legislation, you would be well advised to be cautious and treat them as if they were outside the EEA, as follows.

Check which law applies

If you are sending personal data to countries outside the EEA, you should check whether the European Commission has recognised that country's data protection law as being of equivalent status to the 1995 European Data Protection Directive. The countries that currently have this recognition are Argentina, Canada, Guernsey, the Isle of Man, Switzerland and the USA (under the Safe Harbor Agreement).

If a US company is involved, you need to check that it has signed up to the Safe Harbor Agreement. You should also remember that US financial services companies are not covered by the agreement. The European Commission is also currently investigating whether Australia and New Zealand have adequate data protection laws.

What about India?

India, along with the Philippines and South Africa, is not currently on the 'approved' list of data protection countries. New Indian data protection laws were actually on the verge of being passed in 2004 after being agreed by the then-ruling BJP Party and the Indian IT industry. But the incoming Congress Party dropped the legislation after ousting the BJP in the April 2004 election.

Adequate protection

India is now, once again, in the early stages of producing data protection legislation, but there is currently no formal data protection regulation in place to protect the interests of UK consumers served by Indian call centres. The use of electronic and paper data in India is governed by the Information Technology Act 2000, the Indian Copyright Act 1957 and the Trademarks Act 1999. The lack of formal and specific data protection regulation, however, should not be a hurdle to good practice, as 'model contracts' effectively export by contract the UK Data Protection Act. This is currently considered by the Information Commissioner as 'adequate protection'.

India as a scapegoat

Much of the recent media speculation about data security has centred on India. On further investigation, however, it appears that much of the data for sale were not actually held in India, suggesting that although the brokering of the information was undertaken in India, the source of the data must have been the UK. For example, Royal Bank of Scotland and Nationwide, two companies whose data were offered for sale, do not even hold any data offshore. It seems likely, therefore, that India was simply the location of the data brokering, and not necessarily the venue for the actual data theft.

Tight management and vigilance

Safer in the UK?

To claim that data protection breaches occurred because India has less formal data protection regulation is naïve in the extreme. Indeed, strong data protection rules have not prevented data spillage or abuse in the UK, any more than a law against ‘breaking and entering’ has eliminated burglary. Security breaches occur when a more lackadaisical approach is taken to management — this is as likely to happen in the UK as it is in any other destination — or when you have an errant employee.

Companies often make the mistake of thinking that once a process is offshored, minimal management is needed, but this is not the case. Because of the distance, increased management and vigilance are required. This means ensuring that company procedures are adhered to in every location, irrespective of geography.

In fact, most offshore companies do take their security procedures seriously and realise that where there are high numbers of workers — whether onshore or offshore — there is a risk of a leak. Most offshore companies have strict security measures in place — they are aware of misgivings that UK companies may have over security and do their utmost to ensure that all the correct procedures are followed.

Adequate protection

In order to minimise risks of sending data offshore, there are several things a company can do.

If the country to which you are sending the data is not on the ‘approved’ list, then the issue of data security must be clearly dealt with in the contract you agree with your business partner. Adequate protection, as defined in the eighth principle of good information handling, suggests ensuring through the contract that the outsourced service provider will comply with the UK data protection standards. Where the service provider is acting as a ‘data processor’, the Information Commissioner has expressed the view that a presumption of adequacy can be made in most, if not all, instances of transfers of personal data outside the EEA.

Contractually obliging the overseas supplier to comply with the Act is only a first step. Companies must be diligent in policing and checking the security arrangements put in place by those suppliers. The Act makes it clear that responsibility for making sure these are adequate lies firmly with the company from which the data originate.

Covering data protection via the contract

Good practice safeguards

Furthermore, UK companies should ensure that their offshore partners are diligent in checking whether the people they recruit have criminal records. This is more difficult to achieve in India, for example, than in the UK, where such information is centrally available and can easily be checked. At present in India there is no unique identification system (such as the UK National Insurance number system). The Indian call centre and IT industry body (NASSCOM) is moving towards the adoption of a national employee screening programme — a move which should be encouraged and supported by UK companies using offshore call centres.

Companies can also insist that the data are monitored to pick up

Monitoring data activity

suspicious activities. Anti-fraud checks should involve regular monitoring of data systems, to ensure that the traffic is 'normal'. This may include monitoring the use of peer-to-peer messaging, internet logs and print requests, and applying administration controls to certain applications. Some companies even adopt analytic software to identify comparative behaviours — this may help you to identify when a certain person is using a certain application at a very unusual part of the day.

More mundanely, many Indian outsourced service providers (OSPs) appear to have tighter security frameworks than UK call centres. It is not uncommon in Indian call centres for agents to be forbidden from taking their mobile phones, and even pens or paper, to their workstations — as this will make it more difficult for them to copy and remove customer data. UK companies do not typically employ this level of safeguard.

In summary, then, UK companies should act with responsibility and common sense. Before selecting a partner offshore, due diligence should confirm the integrity of the chosen partner. Then the UK data protection principles should be exported to the destination country via a model contract. Thirdly, the UK company should actively manage and monitor the offshore partner's supervision of their data security.