Blog: Do your homework and ensure data protection compliance with a home working policy

Date : June 25, 2014

The rise in home working and bring-your-own-device (BYOD) working arrangements brings with it compliance risks. Every organisation must have in place adequate measures to ensure that personal information being accessed by home workers is kept secure. A case against a Scottish Local Authority, which was reported on the ICO's website, illustrates the risks.

An employee of Aberdeen City Council worked from home on a non-work personal computer and accessed work documents containing personal data (as defined under the UK data protection rules). When accessing the files in question the computer auto-saved the personal data to the computer's "My Documents" file. The computer had a file transfer programme installed on it, which the employee was unaware of, and which *automatically* uploaded the entire contents of the "My Documents" file onto a website, including information of a highly sensitive nature. This occurred in late 2011 and the information remained available online until early 2012 when another member of staff from the council came upon the material after carrying out an online search linked to their own name and job title.

Very quickly on learning of the incident the council also removed the source documents from the website. Following this, under the UK's data protection rules, the incident was also speedily reported to the UK's Information Commissioner's Office (ICO). Following an investigation, in mid-2013 the ICO imposed a financial penalty of £100,000 on the council after it had concluded that a serious data breach had occurred. In addition, the ICO imposed an undertaking on the council requiring the council to implement the following:

- technical controls to prevent personnel using non-work equipment from downloading personal data and sensitive personal data;
- the use of encryption on all portable and mobile devices used to store and transmit council-held personal data; and
- appropriate security measures to protect the unauthorised and unlawful processing, accidental loss, destruction and/or damage of personal data.

The ICO also highlighted the following failings of the council:

- no relevant home working policy in place for staff;
- not sufficient enough measures in place to restrict the downloading of sensitive information from its network; and
- no checks in place to see whether existing data protection guidance was being followed.

The message from this case is clear - check that a home working setup is up to the job in data protection compliance terms. For businesses the key issue is security. If their employees are putting the company's data in the cloud the company needs to know that and needs to manage the process. For most companies the only practical way of dealing with the risk is to train employees on the risk and make sure they understand that company data is only used on company applications - for example, for BYOD in the Citrix environment not on the offline hard disc environment of the laptop itself.

Jonathan Armstrong & André Bywater are lawyers with Cordery in London where their focus is on compliance issues.

Jonathan Armstrong Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1784

jonathan.armstrong@corderycompliance.com

André Bywater Cordery, Lexis House, 30 Farringdon Street, London, EC4A 4HH

Office: +44 (0)207 075 1785

andre.bywater@corderycompliance.com