complinet

Data protection and home working: hidden risks for employers

Oct 23 2008 Bridget Treacy

Bridget Treacy

Working from home used to be something of a novelty, but is now a regular part of many workers' lives. Many employees' arrangements include a regular amount of time worked from home. Other employees take work home in the evenings, and have done so for many years. It is only recently, however, that employers have begun to think about the data protection risks that are associated with home working.

Headline-grabbing incidents

In fact, the dynamic of home working brings with it a variety of data protection risks. These have attracted greater attention following some of the more notorious data breach incidents that the media has reported in recent months. Some of these headline-grabbing breach incidents have involved home working: UK incidents that involved laptops stolen from cars or homes (UK Ministry of Defence and Nationwide Building Society) and files left on trains for journalists to find.

Who is responsible for the data?

It is, of course, the employer who bears the risk of these data protection incidents. In data protection terms, the employer is the "data controller", responsible for the personal data of its staff, customers and vendors. As data controller, the employer is required to comply with the eight data protection principles contained in the Data Protection Act 1998. These principles include an obligation to ensure that data is safeguarded from unauthorised access by the implementation of appropriate technical and organisational security measures. When employees work at the employer's premises, the employer is able to impose practices and procedures on staff, to ensure that personal data is processed in accordance with the data protection principles. Once an employee works remotely, it is harder to implement and monitor compliance with good data protection practices. How does the employer ensure that records remain confidential? And that records remain within the control of the employer? How can the employer ensure that information used at a worker's home is securely held?

Important issues for an employer

There are five main risks for an employer to focus on.

1. Data security

   It is clear that the employer retains responsibility for the security of personal data that an employee processes at home. Much of this data will also be commercially sensitive or confidential data. An employee owes an implied duty of confidence to an employer, although employers may wish to consider requiring employees (and workers) to sign separate confidentiality agreements which contain clear statements as to how data should be processed and safeguarded when used in a home-working context. In addition, ensuring the security of IT systems is a high priority. It is easier to enforce company IT security and data protection policies if an employee is required to use company equipment or to access the company network via a secure virtual private network.

2. Data in transit

   IT security is probably the most obvious risk area. Less obvious, perhaps, is the need to secure portable storage devices on which vast quantities of data may be held, and paper records. It is accepted best practice that laptops that contain personal data will be encrypted and that other devices, such as the ubiquitous BlackBerry, data cards and thumb drives, will be encrypted, password protected, or capable of being disabled in the event of loss. Moving data between office and home creates a security challenge.

3. Data retention and destruction

   Data must be held securely until the expiry of the relevant retention period and then securely disposed of. Employees need to be aware of retention periods and companies need to ensure that in the event that retention periods are suspended, such as when a litigation hold or preservation order is imposed, those working from home are also able to comply. In the case of destruction of data, it is paper files which are most at risk. How many employees really do shred paper waste at home? Carelessly discarding personal data in domestic refuse creates a significant opportunity for identity thieves.

4. Data breach

   In the event that there is a data breach that involves remote workers, it is critical that these workers know exactly how to respond: who to contact, when and how should be widely known. The sizeable fine that the Financial Services Authority imposed on Nationwide in 2007 was largely due to the fact that the building society possessed inadequate procedures so that staff did not know what to do in the event of a security breach.

5. Privacy issues

Employers also need to be aware that attempts to monitor staff at home must be very carefully planned so as not to infringe the Human Rights Convention which specifically safeguards a person's home, family life, correspondence and privacy more generally. In addition, employers must have strong policies that govern these issues which are easily accessible to home workers. Regular training on these policies must also be offered.

Given the prevalence of home working, particularly on an informal basis, companies must think very carefully about the relevance and impact of these practices on data protection obligations. We have seen several recent examples of data breach incidents where the careless use or transport of data outside the workplace have resulted in data being lost or compromised. This is an issue which is likely to attract increased attention and one which companies must address actively.

This article does not provide a complete statement of the law. It is intended merely to highlight issues which may be of general interest and does not constitute legal advice.
Author Biography:

Bridget Treacy is a Partner in the Privacy and Information Management team at Hunton & Williams.
