**Data Protection in the Workplace**

In the same week which saw 150 Hewlett-Packard employees suspended pending investigation into abuse of the company’s e-mail system, the Information Commissioner has released the third part of its Employment Practices Data Protection Code. This section of the Code is concerned with ‘Monitoring at work: an employer’s guide’¹, and is subject to a short period of consultation that will end on 8 August 2002. The Code follows on the heels of a working document on surveillance in the workplace published by the Article 29 Working Party, a body of European privacy regulators formed under the EU’s Data Protection Directive.²

The Code is in four parts, and addresses (in addition to monitoring), recruitment and selection, employment records and medical information. Although the Code will not be legally binding under the Data Protection Act 1998, the Information Commissioner has made it clear that a failure to comply with the benchmarks contained in the Code “is likely to mean that an employer will not comply with the Act”. Accordingly, businesses should seek to abide by the Code at all times.

If there is one core principle underpinning the Commissioner’s views on monitoring, it is ‘proportionality’; an employer’s monitoring of employees must be proportionate to the lawful objectives the monitoring is intended to achieve. In order to ensure that proportionality is achieved, the draft Code strongly recommends that employers conduct ‘impact assessments’ to determine whether, in a specific circumstance, monitoring is justified in terms of the potential benefits it will bring as compared to any adverse impact it may have on the privacy expectations of the relevant worker(s).

The Code addresses various forms of monitoring which may take place in the employment context, including vehicle monitoring, covert surveillance and video/audio monitoring. In this bulletin, however, we concentrate on those sections which will be of general concern to all employers -- “Monitoring - General Considerations” and “Monitoring of Communications”. These relate to monitoring of employee emails and Internet usage, in particular.

**Monitoring - General Considerations**

The Code sets out 11 benchmarks designed to assist businesses achieve compliance with the UK Data Protection Act 1998. Many of the benchmarks are useful illustrations of how a

---

¹Available from the Information Commissioner’s website at: http://www.dataprotection.gov.uk/dpr/dpdoc.nsf
²Available from the European Union’s website at: http://europa.eu.int/comm./privacy.
business can achieve compliance, while others may be seen as possibly imposing impractical burdens on employers. Set out below are the benchmarks which an employer should aim to meet:

1. Identify who within the organisation can authorise monitoring of employees that might have an adverse impact and ensure employees are aware of their employer’s responsibilities under the Act;
2. Prior to monitoring, identify the specific business benefits that monitoring is intended to bring. Assess the impact of monitoring on employees. Conduct an impact assessment to determine whether the impact on employees is justified by the likely benefits.
3. In making this assessment, consult trade unions and other workers’ representatives, or the employees themselves.
4. If monitoring is to be used to enforce the organisation’s rules and standards, make sure that the rules and standards are clearly set out in a policy which also refers to associated monitoring. Ensure employees are aware of the policy.
5. Tell employees what monitoring is taking place and why, and periodically remind them of this.
6. If sensitive data (i.e. data concerning health, religion, ethnic origin) is collected, ensure that one of the specific conditions for the collection of sensitive data is met.
7. Keep to a minimum those who have access to personal information obtained through monitoring.
8. Avoid using personal data collected through monitoring for purposes other than those for which monitoring was introduced, unless it is clearly in the employee’s interests to do so.
9. If the information obtained through monitoring might have an adverse impact on employees, present them with the information and allow them to make representations.
10. Ensure employees have the right of access, if exercised, to any information collected about them by monitoring.
11. Do not monitor employees simply because a customer has sought to impose this as a condition of business.

Employers may reasonably be concerned with the recommendation to consult with workers’ representatives in relation to the impact assessment. Since monitoring will often be intended to detect improper conduct on the part of employees, it is arguable that such an obligation will defeat the purpose which monitoring is aimed to achieve. Presenting employees with any negative material obtained through monitoring and allowing them to make representations on it will also require a significant investment in management time and, in many cases, would seem to be unnecessary.

**Monitoring of Communications**

Employers are increasingly concerned about the extent to which they can monitor the use by employees, contractors and agency staff of communications in the workplace, for example telephone, e-mail and internet monitoring.
The Code discusses this area in detail and contains useful guidance in relation to the interplay between the Data Protection Act 1998 and the Regulation of Investigatory Powers Act 2000 (RIPA) (and the related Lawful Business Practices Regulations). RIPA broadly prohibits the interception of an electronic communication, by businesses, either on their own or others’ systems. There are some exceptions, the two most notable being interceptions taking place with the consent of the sender and recipient and interceptions connected with the operation of the communications service itself.

The Lawful Business Practice Regulations issued under RIPA set out further exceptions, many of which are helpful to business. These include interceptions that are effected for the purpose of establishing the existence of facts, to check that the business is complying with regulatory, or self regulatory, procedures and to prevent or detect criminal activity. Businesses should be aware that activity that violates RIPA may not, but can, have implications in relation to the Data Protection Act as well.

Recommendations regarding implementation

Applying the general principles of proportionality set out above, the Information Commissioner recommends that employers take the following steps to ensure compliance:

- establishing policies on the use of internet and electronic communications and making employees aware of those policies;
- ensuring that line managers, and others with responsibility for processing personal data, are aware of their obligations under the Act;
- conducting an audit to identify what personal data is generated by the organisation and how it is processed;
- undertaking an impact assessment to ensure monitoring is justified; and
- informing employees and other third parties who may be affected that monitoring is taking place and for what purpose(s) it is taking place.

Additionally, both employers and employees should be aware that they are potentially liable for damage suffered to an individual as a result of management breaches of the UK’s data protection legislation. For this reason, employers should consider establishing clear procedures for line managers on data protection and providing training in this area.

Overview

The general message conveyed by the draft Code is as the nature of the communication becomes more personal, the higher the threshold to lawfully monitor it. For pure business communications, for instance, employer monitoring represents a relatively low level of intrusion on the individual’s privacy and correspondingly requires lesser justification. Where, however, business communications include personal information about the employee, monitoring the communication will require stronger justification. Finally, for communications purely personal in nature with no business-related content, employers must be able to offer a particularly powerful and persuasive justification to monitor the communication, otherwise it will be unlawful. Where businesses remain in any doubt about the lawful basis for their monitoring activities, they should consult with legal counsel.
This is a special Briefing which is issued jointly by Covington & Burling’s European Data Privacy and Labour and Employment groups.

For more information, please contact:

**Dan Cooper**
dcooper@cov.com

**Chris Walter**
cwalter@cov.com

COVINGTON & BURLING
Registered Foreign Lawyers and Solicitors - London
265 Strand
London WC2R 1BH

Tel: 020 7067 2000
Fax: 020 7067 2222
cov.com

This Briefing is for information purposes only.