The UK Information Commissioner, responsible for ensuring compliance with UK data protection laws, has just released Part 2 of the Employment Practices Data Protection Code (Code), dealing with the handling of employee records.¹ This follows the Commissioner’s release in July of Part 3 of the Code, which addressed employee monitoring.²

Part 2 of the Code is likely to be relevant to most UK businesses, which necessarily must process some information about their employees from time to time. Part 2 deals with such topics as the handling of employee sickness, pension and insurance data, allowing employee access to data, and employee data in the merger and acquisition context.

The Code does not have the force of law, but rather provides the Commissioner’s own views on how organizations can comply with the UK Data Protection Act 1998. Thus, businesses that comply with the Code are likely to limit their exposure under the Act, as well as potential liability for breaches of confidence.

UK employers should be interested in the following compliance “benchmarks” set by the Commissioner when considering their own handling of employee data.

**General**

- **Notify employees** - ensure that both new and existing employees are made aware of any personal data that is processed about them and under what circumstances it will be disclosed to third-parties.

- **Allow access** - ensure that employees are made aware of their subject access rights and the procedures for gaining access to their data.

- **Legitimate purpose** - ensure that a legitimate purpose exists for the processing of employee data, and that any information collected actually is responsive and proportionate to that need.

**Security**

Appropriate security should be in place to protect employee data against unauthorized access, loss, or destruction, including, where appropriate, a system of secure cabinets, access controls and passwords to

---

¹ The Employment Practices Data Protection Code can be found at the Commissioner’s website at www.informationcommissioner.gov.uk.

² See Covington & Burling Special Bulletin, Data Protection in the Workplace (July 2002).
ensure that only authorized staff can view employee data. Audit trail capabilities should be used to track all access and amendments made to employee data. Steps should be taken to ensure the reliability of any staff handling personal data, including confidentiality clauses where appropriate, and controls should govern any off-site processing of employee data.

**Sickness and Accident Records**

Sickness and accident records should be maintained separately from other employee records, including absence records (i.e., records that do not specifically refer to the reasons for an employee’s absence). Whenever possible, employers should rely on absence records, rather than more detailed sickness and accident records. Employers should only disclose such records where there is a legal obligation to do so, where necessary in connection with legal proceedings, or where an employee has given the employer their explicit consent.

**Pension and Insurance Schemes**

Information collected for work-related pension and insurance schemes should not be used for other general employment purposes. This includes information obtained from internal trustees or administrators of pension schemes, and administrators of any health or insurance scheme. Employees should be informed of any data that will be collected in connection with a health or insurance scheme and how it will be used.

**Equal Opportunities Data**

Information used in connection with equal opportunities monitoring should be anonymised whenever possible. Because such monitoring will almost certainly involve sensitive data, an employer will need to satisfy one of the conditions under the Act for processing such data.

**Marketing**

Employees should be notified if their data will be used to market or advertise goods or services to them, and have an opportunity to opt-out of such marketing. Employee data should not be provided to third-parties for marketing purposes unless employees affirmatively have consented to such a disclosure.

**Subject Access**

Systems should be in place for responding to employee access requests within the statutory 40 days, and checks should be performed to verify the identity of any individual making such a request.

**References**

A clear policy should establish who can provide references on behalf of an organization. Confidential references about an employee should not be provided by an employer unless this is the employee’s wish. When an employee requests a copy of any third-party references held by the employer, the
employer should determine what information must reasonably be withheld to protect the identities of third-parties identified in the reference.

Mergers and Acquisitions

Employee data handed over to a third-party in the context of a pending merger or acquisition should be anonymised whenever possible, and only after assurances are secured that the data will be used solely in connection with the contemplated business venture and destroyed or returned after use. Whenever practicable, employees should be informed about such disclosures.

Outsourcing

A written contract should be implemented where an employer outsources the processing of employee data to a third-party. The contract should require at a minimum that the third-party may process the data only on the employer’s instructions and must implement adequate security measures to protect the data.

Retention

Standard retention times for employee information should be established, and reflect the underlying need for retaining the data.

For more information, please contact:

Dan Cooper
dcooper@cov.com

Chris Walter
cwalter@cov.com