The Data Protection Act 1998 (DPA) [1] became law on 24 October 1998. It is based around eight ‘Principles of Data Protection’ (Table 1) and its provisions apply to manually processed data such as health records. For living individuals, it replaces the Access to Health Records Act 1990 [2]. However, the majority of the Access to Medical Reports Act 1988 [3] remains in force. It is not the purpose of this article to examine in detail the far-reaching implications of the DPA for health professionals in general, as these have been dealt with in documents such as those from the medical defence societies and from the Office of the Data Protection Commissioner [4], or for occupational health departments (there have been two popular explanations of this which are readily available [5,6]), but rather to look at two particular implications for occupational physicians. There are several transitional arrangements relating to various categories of data; for manual filing systems (such as the majority of occupational health record systems), the DPA applies fully from 23 October 2001.

As with any legislation whose application may vary widely with individual cases, many of the provisions of the DPA, whose broad principles reach deep into the heart of the keeping of medical records, will need to be clarified by case law. Occupational health records frequently contain different types of material, as well as records relating to the care of an individual (for example, reports to and from management, work attendance data, etc.—all these data are essential to the effective management of an individual case). This is all ‘sensitive personal data’ held in a ‘relevant filing system’ and, hence, all subject to the provisions of the DPA. This means that individuals to whom the records relate will have to give explicit consent to their processing. It is unclear from the DPA whether this consent will have to be written; however, the draft Code of Practice [4] states that compliance with the ethical guidelines of the Faculty of Occupational Medicine [7] will suffice in most cases. Individuals will also have the right of access to the material, unless certain limited exemptions within the DPA apply. This raises the interesting question of whether an organization’s management might have the right of veto over the release of management reports addressed to an occupational health professional, relating to an individual. To constitute a ‘health record’ for the purposes of the DPA, a record must have been made by or on behalf of a health professional. It would therefore be difficult to consider a letter or report made by an employer who is neither a health professional nor acting on behalf of a health professional to constitute a ‘health record’, even though the letter or report could be filed within an individual’s occupational health file. Thus,

Table 1. The eight data protection principles

1. Personal data shall be processed fairly and lawfully
2. Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes
3. Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed
4. Personal data shall be accurate and, where necessary, kept up to date
5. Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or purposes
6. Personal data shall be processed in accordance with the rights of data subjects in the Act
7. Appropriate technical and organizational measures shall be taken against unauthorized or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data
8. Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data

The first principle is qualified by reference to meeting the conditions in Schedule 2 to the Act (and Schedule 3, in the case of sensitive personal data), but listing these conditions is outside the scope of this article.
in the transitional period prior to October 2001, an employer might seek to modify the information held on file by an occupational health department to deny individuals access to data which the employer considers inappropriate. Following October 2001, individuals will have right of access to these items, subject to the conditions within the DPA. In terms of clarity for individuals and ease for employers, it might be best to adopt a ‘best practice’ approach to this problem.

A particularly difficult problem is the definition of ‘data controller’ under the DPA. It has been assumed in the past that all medical records (including occupational health records) are under the legal custodianship of a health professional who, of course, is under professional ethical obligations relating to confidentiality. The DPA seems to modify this, with issues of compliance with the DPA falling to employers corporately, not to individual managers or practitioners. It is the view of the Data Protection Commissioner that a ‘good practice’ approach will alleviate problems of compliance with the DPA and that the functions of ‘control’ of medical data under the DPA can be delegated to an occupational physician or nurse. However, it should be remembered that, if an occupational health professional is acting as an employee of a particular data controller when compiling an occupational health record, the occupational health professional cannot be a data controller in their own right. The employer remains liable for any breaches of the DPA but, if any offence has been committed with the consent or connivance of, or be due to the neglect of any individual within the body corporate, he or she as well as the body corporate shall be guilty of that offence. Again, the issues that this raises will need to be clarified by case law. An interesting wrinkle within these issues is the position of the self-employed consultant. Whether a self-employed occupational physician acts as ‘data controller’ for particular sets of data can only be decided on a case-by-case basis. This decision will be influenced by the latitude that the occupational physician has in determining how the data are processed. In the majority of cases, where a self-employed consultant is contracted to an organization to provide consultancy services, he or she will be treated as an employee for the purposes of the DPA.

Acknowledgements
I would like to thank Dr Gillian Strawford of the Medical Defence Union Ltd and Mr Iain Bourne of the Office of the Data Protection Commissioner for their help in unravelling some of the knottier points mentioned above.

References