

Privacy and the new Data Protection Act

Prof. Simon Rogerson

**Originally published as ETHicol in the IMIS Journal Volume 9
No 6 (December 1999)**

It is a prerequisite that people within a civilised society should be law abiding. Indeed from the earliest times laws have been created to sustain and develop society so that its citizens can live peaceably, and to provide some form of address against those who go astray. It is tempting and often the case that the role of law is interpreted as simply being a control mechanism rather than providing guidance as to what is considered as being acceptable behaviour. This leads to an attitude of legal compliance rather than seeing the law as a minimum acceptable standard. Those involved in undertaking or controlling computer-related activity regularly adopt a legal compliance attitude. This however may not be enough because, in all judgements relating to the development and application of information and communication technology, concern for the health, safety and welfare of the public must be primary. Privacy of the individual is a good illustration of this point.

The 1984 Data Protection Act in the UK did not really address the issue of privacy of the individual because, for example, it did not cover all data processing and storage, it had many exemptions explicitly specified and it was driven by political concern over the economic repercussions of companies leaving the UK to establish their operations elsewhere in Europe if an act, which was compliant with the European Directive, was not in place. Primarily the Act required organisations to register their computerised data processing activities of personal data. Legal compliance did very little to sustain, let alone improve, an individual's right to privacy.

The new Data Protection Act received Royal Assent on the 16 July 1998. The Act and the secondary legislation required to support it, will be brought into force on the 1 March 2000. The new Act has a clear focus on individual privacy. The Information Commissioner's initial interpretation of the new Act illustrates this. The new Act expressly provides that personal data are not to be treated as processed fairly unless, as far as practicable, the following criteria are met:

- the individual has given his or her consent to the processing
- the processing is necessary for the performance of a contract with the individual
- the processing is required under a legal obligation

- the processing is necessary to protect the vital interests of the individual or to carry out public functions
- the processing is necessary in order to pursue the legitimate interests of the data controller or certain third parties (unless prejudicial to the interests of the individual).

Stricter conditions apply to the processing of sensitive data. This category includes information relating to racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life and criminal convictions.

There is a new eighth principle restricting the transfer of personal data outside the EU. Personal data may only be transferred to third countries if those countries ensure an adequate level of protection for the rights and freedoms of data subjects. When determining adequacy data controllers should consider, for example, the nature of the data, the country of origin and final destination, and the law or any relevant codes of conduct in force.

The definition of data in the new Act has been extended so that it now catches information which is recorded as part of a relevant filing system where the records are structured, either by reference to individuals or by reference to criteria relating to individuals, so that specific information relating to a particular individual is readily accessible. This definition will catch some types of manual data as well as automated forms of processing.

Clearly, the new Act has much to offer regarding the safeguarding of personal privacy but does it go far enough? Consider the case of health data. In its recently published opinion on the ethical issues of healthcare in the information society, the European Group on Ethics in Science and New Technologies (EGE) explained that personal health data necessarily touch upon the identity and private life of the individual and are thus extremely sensitive and that confidentiality of personal health data must be guaranteed at all times. This implies that the informed consent of the individual is required for the collection and release of such data.

The new data protection legislation upholds much of this requirement but there are shortcomings. Probably the most notable relates to EGE's comment that the respect for the confidentiality of health data continues after the death of the person. Once a person dies he or she is no longer a data subject and therefore the Act no longer applies which means the personal health data can be distributed, processed and published without restriction under the Act. This seems unacceptable as personal health data of dead people may well have repercussions for those still living. Responsible organisations and individuals handling such data are likely to respect this implication and consequently will still maintain data confidentiality. However, the unscrupulous might see an opportunity to benefit from this situation by making once restricted data available in return for a fee. Many would argue this might be legal but it is not ethical.

The new Act offers a great opportunity for computer practitioners at all levels to improve their level of professionalism regarding the public. The Act is a clear indication that respect of an individual's privacy is paramount. Why not use the opportunity to review the processing of personal data and implement what is right for the individual rather than simply achieving legal compliance? Put yourself in the place of the data subject and ask yourself if you are happy with the amount of data that is collected, stored, manipulated and transmitted about you in the systems that you are running regardless of the fact that they are legally compliant. If the answer is no then do something about it!

Information about the Data Protection Act 1998 can be found by visiting the Information Commissioner's website (<http://www.dataprotection.gov.uk/>).

Please send your views on ethical and social responsibility issues and cases of ethical dilemmas to:

Professor Simon Rogerson
Director
Centre for Computing and Social Responsibility
Faculty of Computing Sciences and Engineering
De Montfort University
The Gateway
Leicester
LE1 9BH
Tel:(+44) 116 257 7475
Fax:(+44) 116 207 8159
Email:<srog@dmu.ac.uk>
Home Page: (<http://www.ccsr.cse.dmu.ac.uk>)