UK Registrar seeks comments on EU data security provisions

The Office of the UK Data Protection Registrar issued a consultation paper in early December regarding information security provisions in the EU Data Protection Directive. The Registrar asks for comments by 31st December 1997 (but may allow a little extra time) in order to assist her in developing proposals for implementation.

The consultation deals with the security provisions of Articles 17 and 19 of the Directive, which require that:

1. controllers implement appropriate technical and organisational security measures to protect personal data, and that
2. controllers notify a general description of the security measures they have adopted to the supervisory authority.

The short, 6-page consultation paper contains:

- a brief analysis of the requirements of Art. 17,
- a suggestion to develop a particular approach to compliance for small and medium-sized enterprises (SMEs), and
- initial thoughts on what the notification process under Art. 19 should be like.

Comments and suggestions are sought on all these issues. Technical security measures need to be backed by management systems.

Controllers to adopt and enforce a security policy

The consultation paper suggests that information security cannot be regarded just as security of information systems. Apart from technical measures, organisations need to ensure that the security policy is adopted and enforced.

The Registrar's office notes that there are some minor differences between Article 17.1 and the requirements in the 1984 Act. For example, the requirement to protect against unauthorised alteration of personal data does not appear in the Directive's text as such. On the other hand, the general requirement of Article 17.1 for protection against all other unlawful forms of processing is likely to include unauthorised alteration.

The Directive's wording on the implementation of security measures states that in choosing appropriate security, account must be taken of the state of the art and the cost of implementation of the measures, as well as the risks involved in processing and the nature of data. The Registrar's interpretation is that this does not require controllers to have the latest security technology in use, but they need to keep security measures under review and take account of new developments in technology. However, the cost of implementation can be taken into account.

General description of security

A new requirement in Article 19 is the obligation to notify a general description of the security measures taken in order to comply with Article 17. The level of security measures needed will vary from one case to another. There are, however, measures that can be taken to assist compliance. The British Standard BS7799 on Information Security Management and the possibility of obtaining certification of compliance in the future, if the scheme is introduced, is a helpful tool for large companies. The Registrar is particularly interested in determining the level of support for a suggestion to require formal certification under BS7799 in specified cases of high risk processing. Informal self-assessment is also an option, particularly for SME's. Organisations could also use risk assessment and the evaluation of counter-measures.

Controllers to notify security measures

A new requirement in Article 19 is the obligation to notify to the supervisory authority a general description of the security measures taken in order to comply with Article 17. As general notification is being simplified, the Registrar is not willing to introduce a complex system of notifying security measures. A basic security description would be developed. A more detailed notification could be required from controllers of sensitive data.

Information Security - A Consultation Paper **is available from, and comments to, Dr J N Woulds, Director of Operations, Office of The Data Protection Registrar, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF. Tel: +44 1625 545 700 Fax: +44 1625 524 510 e-mail: data@wycliffe.demon.co.uk http://www.open.gov.uk/dpr/dprhome.htm**