The Data Protection Act 1998

This circular provides information to NIAO Staff on the Data Protection Act 1998, and guidance on its application.

Background

1. The Data Protection Act 1998 (the Act), which came into force on 1 March 2000, replaced the earlier Act (1984) which first established certain rights in relation to personal information held on living individuals.

2. The Act applies to personal data that is subject to processing. Personal data is that which relates to a living individual who can be identified from the data, *or* from the data and other information that is in, or is likely to come into, the possession of a Data Controller. It also includes expressions of opinion and indications of intention on the part of the Data Controller (or anyone else) in respect of the individual. Processing includes obtaining personal information, the retention and use of it, access and disclosure and final disposal.

3. Data may exist in either a form suitable for processing automatically (e.g. by computer) or manually (e.g. on paper, fiche). Manual data must be stored in a relevant filing system. This is any system that is structured in such a way that specific information relating to a particular individual is readily accessible.

4. A wide variety of technologies can be used to hold personal data, and are therefore covered by the Act. These include:

    - computers, PCs and laptops, electronic organisers (e.g. hand held computers);
    - telephone recorded messages and fax machines;
    - Internet documents, e-mail, word processed documents;
    - document image processing systems, videos, and CCTV;
    - paper filing systems and card indexes;
    - microfiche and microfilm.

Legal requirements

5. The Act requires a Data Controller to notify the Information Commissioner of certain details about its processing of personal data. These details include the purposes for which processing is carried out, the individuals about

whom personal data is held (data subjects), the types of personal data processed (data classes) and to whom data may be disclosed (recipients). The Commissioner uses these details to make an entry describing the processing in a public register. NIAO, as a Data Controller, has notified the Commissioner of its use of personal information for both administrative and audit purposes.

6. Data Controllers must comply with the eight "Data Protection Principles" contained within Schedule 1 of the Act, which are that data must be:

   (1) fairly and lawfully processed;
   (2) processed for limited purposes;
   (3) adequate, relevant and not excessive;
   (4) accurate;
   (5) not kept for longer than is necessary;
   (6) processed in line with a data subject's rights;
   (7) secure; and
   (8) not transferred to countries without adequate protection.

7. The NIAO Data Protection Officer will advise on how these principles are to be applied.

Rights of data subjects

8. Data subjects have certain rights under the Act, including the right to access personal data, subject to certain exemptions. The NIAO Data Protection Officer is responsible for co-ordinating and responding to subject access requests. Any subject access request received by a member of staff must be referred immediately to the Data Protection Officer.

Compliance within the NIAO

9. Personal data must only be used for NIAO purposes.

10. Compliance with data protection legislation is managed through the NIAO Data Protection Officer, but system owners and other staff also have important roles.

11. The NIAO Data Protection Officer is responsible for:

    - ensuring that NIAO is properly registered under the Act;
    - providing advice on interpreting the Act;
    - providing guidance to staff on their individual responsibilities and the procedures that they should follow.

12. System owners are responsible for implementing procedures designed to ensure that NIAO complies with the Data Protection Principles. Where personal information is used for audit purposes, the audit manager responsible for the work in question will assume the responsibilities of System Owner.

13. Any member of staff who controls the use of personal information covered by the Act must notify the NIAO Data Protection Officer. They should describe the information in question and give details of their proposed use of it in the relevant 'Personal Data Usage Notification Form'.

14. A procedure step relating to Data Protection processing has been introduced to the Team21 Planning folders. This step should be completed for each financial audit.

Other

15. Any queries on this circular should be addressed to the NIAO Data Protection Officer.