

THE UK DPR GIVES ADVICE ON DATA PROTECTION ACT COMPLIANCE FOR DOCUMENT IMAGE PROCESSING

The draft Guidance Note on Document Image Processing (DIP), published in September 1994, was the first draft policy document issued by the new Data Protection Registrar, Elizabeth France (PL&B September 1994 p.19). In November, Privacy Laws & Business organised two workshops as an opportunity for public and private sector data users to comment and participate in the regulatory process. This report is based on the advice given by Assistant Data Protection Registrar, David Smith, at the November workshops.

Why are DIP systems different?

The major differences between traditional computer data and DIP are that:

1. with traditional computer systems, one should input only relevant information, but with DIP, there is no filter of what goes into the system.
2. with traditional computer systems, one holds information in accessible fields, but with DIP, one holds information at the level of a document.
3. with traditional computer systems, one may delete specific data but with DIP, at least the less sophisticated systems, the user cannot delete specific information in the same way.

The guidance is aimed at the basic systems with the basic level of scanning a document into a computer. However, where possible, data protection guidance should be applicable to the new DIP areas of text/voice/image integration.

The Data Protection Act was introduced because Parliament considered that using computers to process information automatically posed a threat to individuals' privacy. At that

time, paper records were not widely seen as a threat. Now, DIP is not only used to save space but also to facilitate retrieval. By applying DIP to manual records, the framework has to be changed and the draft guidance note provides rules to follow to protect the rights of individuals.

Advice 1. In relation to *microfiche and microfilm*, if there is an automatic way to retrieve the information, then the Act will apply. But if the user has to search manually, record by record, then it will not apply. The ability to automatically obtain information about individuals will determine if the Act applies. An index on computer will come under the Data Protection Act, but a microfiche itself will not.

In DIP systems, the user cannot extract information automatically but only retrieve it. The documents are indexed and can be called up one by one and then be transferred to a traditional computer system.

Registration

Advice 2. *The introduction of DIP does not change the registration requirements of the Act* as registration is not based on the system in use. The data user does not have to register the fact that he uses DIP. Changes to the registration will be needed if information which data users enter in the DIP is held for an additional purpose or there are new classes, sources, disclosures, etc.

Advice 3. *Records held for historical purposes*, such as records of the company's activities since its foundation, might be held on a DIP system. The Act does not prevent the holding of such historical records indefinitely, as long as it does not cause damage or distress to the data subject.

Advice 4. In relation to *data classes*, care must be taken. The user can register for uncategorised information held on DIP for information volunteered in correspondence, as there is no way of knowing what people are going to write. The additional wording in free text might be "information given in correspondence." However, it is not sufficient

to write "information held on DIP system," as this is not sufficiently descriptive. The Registrar will pay attention if uncategorised information is ticked alone. The company must tick the other fields which relate to the activities of the company.

The Principles

First Principle: Information should be obtained and processed fairly and lawfully

Advice 5. DIP does not change the fundamentals of this principle. There is no need to notify the individual that information is to be held on DIP, as opposed to any other system. *The need is to tell him what you do with the information.*

Fourth Principle: Personal data shall be adequate, relevant and not excessive

If, for example, a local authority receives a letter from a data subject stating that he is moving and giving his new address, that is the information that the local authority will need. If the individual volunteers more information, in theory, there is no need to record that information. In a traditional computer system, you would key in only the relevant information from the letter as you can select the material for inputting. In DIP systems, this is difficult.

Advice 6. In the above case, the Registrar recognises that, *you cannot have control over information which has been volunteered to you in a letter and, therefore, it may be recorded in a DIP system.*

Advice 7. *When information is given in an application form, the data user has control of what he asks and, before putting it in a DIP system, must check that:*

1. the information he is asking for is relevant and not excessive, and
2. the forms are designed to ask for only the necessary information.

The data user must also take care to ensure that he:

1. accurately records the data subject's statement, and

2. can add the date the information was given and a note saying that the information was accurate at the time it was given.

If the information provided is irrelevant or excessive, the data user must re-think whether he needs that information and needs to input the whole document onto the DIP system.

Advice 8. In relation to *back files and existing documents*, the recommendation given is that if the information is excessive, then do not put the document into DIP, unless the excessive information can be left out. The Registrar recognises that for back files there is a problem as it would be very difficult to start checking old documents.

Fifth Principle: data must be accurate

Advice 9. *If the document is inaccurate but has to be retained for some reason, the user needs an indication of that fact. Whatever comes up on the screen must be complete and accurate information, including any note or comment added to the record. For example: "the information on the image was accurate but it has been superseded by new information."*

Advice 10. *If a document relates to third party information or information filled in on behalf of the company by third parties, it must state who recorded it and the date it was recorded. The date on the document determines which is the most up-to-date record.*

Advice 11. *In the case of a medical diagnosis, the Act will not require the removal*

Data Protection Manager Looking for New Role

A UK data protection manager with information systems strategy experience is looking for new opportunities. He is currently the data protection manager for an organization employing 22,000 people with £450 million in annual turnover. He would prefer a West Midlands location.

For further information, please contact the Privacy Laws & Business office.

of the information from the record if it could be important for future medical reasons.

Sixth Principle: personal data should not be kept for any longer than is necessary

For example, an organisation may only need the date of birth of people until a certain age; after that, the information is not necessary. Here, the Registrar takes the same view as for the fourth principle.

Advice 12. *If information is volunteered, then there is no way of controlling it. Thus, the document can be kept for as long as it is necessary because some information on it is relevant. However, if you ask for information, such as date of birth and this information is not necessary after a certain date, then you have to design the form or the system in a way to get rid of such information at the appropriate time.*

Advice 13. *For back files, the recommendation is to add a reminder date which will alert the user when it is time to review the information.*

Advice 14. *Information that has to be kept for long periods of time for legal reasons. The Registrar is reluctant to accept that because of a unforeseeable future reason, you might need to keep information forever. If an organisation can provide a good reason such as mortgage, finance, or money laundering regulation, then this should be acceptable. Legal requirements are not questioned by the Registrar.*

Seventh Principle: Data subject access

Advice 15. *Data subjects have a right to a copy of all information about them which is held on a DIP system, including opinions for references. On opinions, the Data Protection Act does not empower an individual to challenge accuracy and you may withhold the identity of the person who gave the opinion. Where another data subject may be identified by the disclosure of information, the identity of that individual may be withheld.*

Eighth Principle: Security

Advice 16. *Security requirements are the same for DIP as for any conventional system.*

DOCUMENT IMAGE PROCESSING USERS' WORRIES ABOUT THE GUIDANCE NOTE

Many of the 1,000 members of Cimtech (the Centre for Information Management and Technology, a document management trade and user organisation), use DIP. Their worries about the DIP draft guidance note relate to three areas:

1. The impact in general on system design, functional requirements and system specification. Potential users may need to upgrade the design of their DIP system and this may increase costs. Where users already have DIP systems, they may need to change the design which may equally incur higher costs. For example, where documents may be currently indexed on a case basis, they may, in future, need to be indexed on a document basis.
2. The problem of back file conversion and how to deal with old information stored on microfilm and/or paper.
3. The problem of legal admissibility and possible conflict between the Data Protection Act and the work being undertaken in this area by the British Standards Institution (which has produced BSI standard 7768), the Legal Images Initiative and a collaborative effort by the Document Management Suppliers Group (DMSG) and the UK Association of Image and Information Management (UKAIIM, a division of CIMTECH). All of these groups are distinct. The concern which CIMTECH has is that the standards, codes of practice and guidelines produced by these groups may conflict with the guidance note produced by the Data Protection Registrar. This conflict applies, in particular, to the issue of certification. BSI 7768 requires that DIP operators will have to certify that they have input the original documents and that they have not tampered with them. However, the Data Protection Registrar requires that certain data is deleted before inputting it into a DIP system, for example, if it is inaccurate.

Physical control, different levels of access control to the document, and audit trails should be in place, among other things. In relation to access control of a computer bureau, it is subjected to the same security requirements as the data user who contracted them. The Registrar might investigate an agreement between the bureau and the contractor.

Enforcement

In the draft guidance note, there is an outline of the breaches which may occur.

Advice 17. If there is a breach of one principle, the Registrar will look into it, if there is a complaint, and will advise accordingly, for example, to delete an inaccurate record. Only in extreme cases of breaches of principles, might an enforcement notice be issued and a change on the system might be required.

The Registrar's criteria for taking enforcement action will include looking into the specific case and assessing:

1. whether there was damage or distress

2. the sensitivity of the data
3. the number of individuals affected
4. how long the data is being held and what efforts the company has made to comply with the Act.

Advice 18. With the guidance in place, whoever installs a new system will have to comply. A less rigorous view might be taken towards old systems and back files. However, the Registrar would like to see one set of rules applied to old and new systems. Perhaps data users with old systems will have more time to adjust, as has been discussed for the provisions related to manual records in the EU data protection draft directive.

A fuller version of this paper, with examples of anonymised participants' experience of data protection problems related to DIP, and the participants' recommendations to the Data Protection Registrar, is available from the *Privacy Laws & Business* office.

Privacy Laws & Business Newsletter Subscription Form

The *Privacy Laws & Business Newsletter* subscription: four issues, legislation and information service. Subscription £250 (UK), £265 (elsewhere). Sample copy £25 (UK), £40 (elsewhere).

Name.....

Address.....

Telephone..... Fax.....

You may pay by:

1. **Cheque** enclosed made payable to: Privacy Laws & Business

2. **Credit card:** American Express, Visa, Mastercard or Access. (Please indicate your card).

Credit card number..... Expiry Date.....

Card billing name and address if different from above:.....

3. **Please invoice me**.....

Signature..... Date.....

GUARANTEE

If you are dissatisfied with the newsletter, the unexpired portion of your subscription will be repaid.

**Privacy Laws & Business, Roxeth House, Shaftesbury Avenue, Harrow,
Middlesex, HA2 0PZ, United Kingdom**