Man bytes index 
and (maybe) index bites man—
some notes on the Data Protection Act

J. Eric Davies

Introduction

In July 1984, after a fairly lengthy Parliamentary
gestation, the Data Protection Act\(^1\) reached the Statute
Book of the United Kingdom. With that, the foun-
dations were laid for a system for regulation and over-
sight of the use made of computers to handle personal
information in this country. As the issues and contro-
versies which illuminated (and sometimes obscured) the
work on creating data protection legislation recede into
history* we are now left with the Act and the need to
come to terms with its provisions. There is a little time in
which to do so because its operation is staged to allow for
such assimilation and preparation as is necessary, given
the nature of the subject. More on the Act’s timetabling
later. It needs to be made abundantly clear at this
juncture that the Act is concerned only with information
about identifiable living individuals which is processed
by equipment operating automatically in response to
instructions given for that purpose—a computer to you
and me. Moreover, word processing operations alone are
eliminated from the scope of the Act and a suitably
worded clause [Section 1(8)] sees to this. Those who wish
to ponder the technological and philosophical niceties of
this entire area should study the definitions in Sections 1
and 41 for further enlightenment! The Act touches us all
as individuals because we are now inevitably ‘in’ some-
one’s computer. Clearly it also affects those organ-
izations, institutions and even individuals who utilize
computers to process personal data. The indexing
community is not immune from the legislation. Those
who, for example, enlist the aid of computers for their
indexing and who work on material involving the index-
ing of details about individuals need to be aware of the
principles and practice of data protection whether they
work in a large organization or on their own. Equally,
those who use the ‘backs of envelopes’ or other paper-
based record-making schemes for indexing, or do not
ever index material relating to living persons, are outside
the scope of the legislation. One is tempted to advise
them to read no further!

The legislation

The Data Protection Act can be regarded for sim-
plicity as comprising essentially two features. The first is
an enumeration of a set of principles describing and
indeed stipulating good practice in the use of personal
data. The second is a description of the structure of
regulatory institutions and mechanisms designed to
ensure that the principles are followed. In addition,
much of the Act is concerned with defining the techni-
calities of the subject and with detailing exceptions and
variations to the general rules to be followed in the
 treatment of personal data. These notes will, in the main,
confine themselves to the general provisions of the legis-
lation. Readers are therefore strongly recommended to
study the text of the Act in full to establish a total picture
of how they may, or may not be affected by the
legislation.

The legislation—Principles

Since they form such a fundamental part of the legis-
lation it is worth quoting in full the eight principles of
data protection to be found in Schedule 1, Part I of the
Act.

*Those who hanker after a historical perspective to the subject
can do no better than read Ann Crook’s valuable two-part
survey:


THE DATA PROTECTION PRINCIPLES

Personal data held by data users

1. The information to be contained in personal data
shall be obtained, and personal data shall be processed,
fairly and lawfully.
2. Personal data shall be held only for one or more speci-
fied and lawful purposes.
3. Personal data held for any purpose or purposes shall
not be used or disclosed in any manner incompatible with
that purpose or those purposes.
4. Personal data held for any purpose or purposes shall
be adequate, relevant and not excessive in relation to that
purpose or those purposes.
5. Personal data shall be accurate and, where necessary,
kept up to date.
6. Personal data held for any purpose or purposes shall
not be kept for longer than is necessary for that purpose or those purposes.

7. An individual shall be entitled—
   (a) at reasonable intervals and without undue delay or expense—
      (I) to be informed by any data user whether he holds personal data of which that individual is the subject; and
      (II) to access to any such data held by a data user; and
   (b) where appropriate, to have such data corrected or erased.

Personal data held by data users or in respect of which services are provided by persons carrying on computer bureaux

8. Appropriate security measures shall be taken against unauthorised access to, or alteration, disclosure or destruction of, personal data and against accidental loss or destruction of personal data.

Thus it will be observed that the Principles encompass operations with personal data ranging from its acquisition to its disposal after it has fulfilled its purpose. Moreover, an individual who is the subject of any data enjoys a right of access to it, and can pursue its correction or erasure where appropriate. Further explanation of the scope of the Principles appears in Schedule I, Part II: INTERPRETATION.

The legislation—Institutions and mechanisms

The regulatory institutions and mechanisms specified in the Act, and being created in its wake, are designed to identify what personal data processing is taking place and thereafter, through a series of controls, to direct activity particularly when it appears to be 'straying' from the Principles. The Office of a Data Protection Registrar has been created for the operation of the law. The Registrar has many and diverse powers and responsibilities pertaining to the oversight and regulation of data processing involving personal information. One of the prime responsibilities with which the Registrar is charged is that of creating and maintaining a Register of data users and bureaux concerned with personal data.

The activities of data users and bureaux have to be formally recorded in the Register, except for those few examples of data use, or types of data user, covered by exemption provisions (discussed later) in the Act. The Registrar has powers therefore to require data users and bureaux to give him appropriate and adequate information with which to compile the Register. When the legislation is in fuller operation, it will be prohibited (and therefore a punishable offence) for those so required to continue operating without being registered. Much work has recently been undertaken by the Registrar's Office to devise suitable procedures for registration, including the design of appropriate registration forms and codes to abbreviate the detail which will have to be furnished. Pilot trials of the registration process have taken place in which a range of user interests have been involved. Many, many thousands of registration applications are anticipated in the early stages of the operation and it is in both the users' and Registrar's interests if the process can be streamlined and rendered as trouble-free as possible. Naturally, an undertaking of this magnitude is expensive in labour and other resources, and some attempt at cost recovery is inevitable, so a fee is payable for registration. The fee is not envisaged to be such that it will represent an onerous burden, especially for commercial organizations, but it may be an unwelcome budget item for individual operators.

Having collected and compiled the material, the Registrar has a further responsibility to make the information contained in the Register available for public inspection. Through this means the private individual can at least establish who is processing what personal data and possibly determine whether a request for data subject access is worthwhile. The mechanics of making the Register accessible have also received consideration and it is likely that in addition to access directly at the Registrar's Office, deposit of copies at public offices such as libraries will eventually render the material more widely available for consultation.

Another of the Registrar's prime responsibilities is, of course, ensuring that any use of personal data is in accordance with the Principles of data protection. He is provided with an array of powers and devices designed to fulfill this task. In appropriate circumstances he may:-

+ refuse registration,
+ de-register a user or bureau,
+ issue an enforcement notice to direct certain activity,
+ issue a notice prohibiting transfer of information outside this country,
+ institute court proceedings for offences committed under the Act,
+ with a Warrant enter and search premises, examine items and seize evidence,
+ consider complaints about data protection.

Viewing his powers and duties in, perhaps, a more positive light it should also be noted that they include:-

+ promoting observance of the Principles,
+ encouraging the preparation and dissemination of suitable 'codes of practice',
+ disseminating appropriate information about the Principles and the operation of the law.

All this may create a little anxiety in the minds of some who could regard the Registrar as having too much power and discretion to interpret what are fairly general principles. There is reassurance available, however, in the form of the Data Protection Tribunal whose task it will be to adjudicate upon matters of disagreement between the Registrar and data users. Note that the Tribunal does not concern itself directly with data subjects' problems.
The legislation—exemptions

Some words on exemption provisions in the Act may be appropriate. In the main they can be studied in Part IV (Sections 26 to 35) of the Act, and the reader is recommended so to do. As was noted earlier, word processing operations are effectively exempted from the legislation by being ‘defined out’ of the scope of the Act in Section 1(8), so other parts of the text should also be viewed carefully to establish its applicability to any specific operation. Quite a number of formal exemptions are enumerated in Part IV. Many apply to very specialized purposes or data use such as the exemption from data subject access and non-disclosure provisions of information used to fight crime, or tax evasion and fraud. Few exemptions are readily applicable to the regular personal data processing applications which customarily face the indexer, information scientist, or librarian. Perhaps worth mentioning are exemptions in the following categories, though there are others which might affect particular cases:

Exemption from registration, data subject access and the non-disclosure provisions;
+ data held only for payroll and accounting purposes
  —subject to certain limitations on disclosure,
+ domestic, personal, family or related household affairs information, or for recreational purposes,
+ clubs, societies’ members’ data—subject to the consent of members,
+ distribution lists—subject to disclosure limited by consent of data subjects.

Exemption from the data subject access provisions;
+ preparing statistics,
+ carrying out research,
+ data kept only for the purpose of replacing other data
  in the event of the latter being lost, destroyed or impaired.

Exemption from non-disclosure provisions;
+ where urgently necessary to prevent injury or damage
  to health,
+ where disclosure is required by any law or by order of
  a court,
+ where disclosure is to the data subject, or his representative or is by his consent.

The legislation—timetable

So far in these notes the staged nature of the legislation has received only a passing reference. It is, however, important to appreciate the way in which the application of the Act is staged in order that planning for data protection may be properly phased, and in order that a crucial provision which may be operative at a certain point is not overlooked with unwelcome results! Some, and only some of the detail in the staging of the Act is described below:

+ Act passed (12 July 1984)
  Formal passing of the legislation
+ Two months later (12 September 1984)
  From this date it has been possible for an individual data subject to sue for damages suffered as a consequence of the loss, destruction or disclosure, without the authority of the data user, of data relating to him.
+ ‘Commencement date’ (11 November 1985)
  Date officially pronounced by the Secretary of State. Acceptance of applications for registration begins on this date.
+ Six months after ‘commencement date’. From this date operations without being registered prohibited.
  An individual data subject may sue for damages suffered as a consequence of inaccuracy of data from this date.
+ Twenty-four months after ‘commencement date’. All aspects of the legislation become operative including:-
  Registrar’s powers to serve Notices.
  Registrar’s general powers to refuse application for registration.
  Implementation of data subject access rights.

Data protection practicalities

Thus, the entire edifice of data protection comprising the Principles, and associated regulatory bodies and mechanisms is planned for in the Act and is in the course of being erected. Already the Registrar is firmly established in Office and the all important ‘commencement date’ for the Act is imminent (if not passed by the time these notes appear!) To all intents and purposes we are in the ‘active phase’ of the data protection legislation and suitable preparation is necessary for those to whom it applies. How then is the situation best approached? For the person involved in the business (large or small) of indexing, an appraisal of activity must be undertaken. It must be established whether and how a computer is used for processing personal data, and if any exemptions apply. Those who have read this far in these notes will now appreciate that the utilization of even a modest microcomputer for the business of selecting, sorting, arranging and formatting index entries relating in some way to identifiable individuals would come within the ambit of legislation. Use of a machine solely as a word processor would, however, not do so. The definitions provided in Section 1 of the Act to which the reader was referred earlier are particularly relevant in determining the nature of activity covered by the law, especially Section 1(2) defining ‘Data’, 1(3) defining ‘Personal data’, and 1(7) defining ‘Processing’.

Once the nature of operations undertaken has been established and described, then preparation for registration should be made. The Registrar will furnish standard
forms on which an application for registration, accompanied by the appropriate fee, must be submitted. The information required to effect registration will include the full identity and address of the data user, or bureau, together with particulars of the operations to be registered. It should be noted that the Registrar is interested in data use, and the purposes of data use, rather than in learning about specific files. Registration involving several files of information may yet be relatively straightforward and unencumbered if they all apply to a basic purpose such as index construction and formatting for example. Registration is not a 'once and for all' process and will be renewable. The initial period may last up to three years. In addition, application for all process and will be renewable. The initial period may last up to three years. In addition, application for amendments to the registration details can be made at any time to reflect a change in the nature of activity undertaken by a data user.

Particulars about data use sought from users include:
+ source of data (where, or who does it come from?)
+ purpose of data (what is it used for?)
+ types of data subject (what types of person does the data describe?)
+ types of personal data (what kind of data about a person is held?)
+ disclosures of data (who will see the data?)
  ♦ related to source of data
+ overseas transfers (where, if at all, will the data go outside this country?)

Assuming that the registration is accepted by the Registrar, then operations may continue. It should be borne in mind, however, that work may proceed only according to the description of operations specified upon registration and with due regard for the Principles of data protection. Appropriate attention should, for example, be accorded to the accuracy, relevance and up-to-dateness of any information acquired, treated and used. In certain circumstances it may well be advisable, therefore, for an indexer to reassure himself or herself about the integrity of any draft or text upon which indexing work is performed. Furthermore, physical and system security should be established as being adequate for information handled and the work performed.

Arrangements to provide for requests, however infrequent and irregular, from data subjects for access to information also need to be considered and built into any operation. There should be a reliable and economic means by which a request can be fulfilled within the requisite legal period (40 days) even before an index is completed, let alone published.

People engaged in a large organization are faced with similar data protection requirements, but obviously the scale of operations is bigger, and the problems are likely to be more plentiful! Inevitably, more applications of systems and files will be evident, and a proper census of activity is a pre-requisite of good data protection management and a basic preliminary to registration. (How can you register what you don’t know you’ve got?) Suitable systems, operations and procedures; and managerial policies and measures need to be devised and implemented to ensure effective data protection in-house. Again, data subject access arrangements must not be overlooked and suitable routines need to be established. Data Protection awareness, both in terms of legal and operational factors, also takes on a new dimension as staff in a large organization have to be educated and trained to adopt appropriate attitudes and methods of working regarding personal data.

A large organization may indeed have sufficient operations on personal data to justify the nomination of a ‘data protection officer’ to coordinate and oversee relevant matters and to take responsibility for day-to-day affairs. Except in the largest organizations the role may not necessarily justify a full-time appointment. But it can usefully form part of a senior manager’s brief, and is worth consideration as a means of ‘getting to grips’ with data protection within an organization.

Information and advice

There is now no shortage of material to read and conferences to attend through which to seek (and perhaps find, if you are lucky!) reassurance about data protection. Those needing advice on specific operations or situations may be able to enlist the aid of their professional associations. (The Library Association, The Institute of Information Scientists, and Aslib—The Association for Information Management, are a few of the many who are active to some degree in this area.) The Office of the Registrar of Data Protection is, of course an obvious source of expert information and advice, but inevitably the resources available there are limited and likely to remain so as priority begins to be given to the process of registration and supervision of data use. The Registrar’s Office has helpfully published some informative and authoritative material and everyone is recommended to read the Guidelines Series, designed to explain the Act and its operation, which are available on application.* In addition, the library and information fraternity may (it is hoped!) find something of use in a book by this author which appeared recently.

Conclusion

To sum up, the key to living successfully with the Data Protection Act is awareness. Awareness of the law’s requirements and operation; awareness of the need to nurture and safeguard the integrity and security of information about people; and awareness of the ways in which your operations work and need to be protected.

*The Registrar can be contacted at: Office of the Data Protection Registrar, Springfield House, Water Lane, Wilmslow, Cheshire, SK9 5ZX. Telephone enquiries: Wilmslow (0625) 535777
These notes have given an outline of the factors involved and as such, it is hoped, have provided a firm basis on which those in the indexing business may build.

References

J. Eric Davies, MA, FLA, MBIM, MInfSc, MIRT, is Senior Assistant Librarian, Loughborough University of Technology; also, Library Association Councillor and Member of the Library Association Working Party on Data Protection.

Where is the wisdom we have lost in knowledge? Where is the knowledge we have lost in information?

—from The rock by T. S. Eliot

Copyright for indexers
Tamara Eisenschitz

Copyright protection applies to written, musical and artistic works and protects the form of the creative work as opposed to the ideas or information within it. For this article, only literary works need be considered. The applicable UK law is the Copyright Act of 1956. The owner of copyright is normally the creator of a work; it can then be assigned or licensed to any other person or organization, such as the publisher of the work.

UK Copyright Law

Copyright protection is a negative protection. It forbids anyone to reproduce the work as it stands, or to make a translation or adaptation without permission of the copyright owner. Reproduction, etc., of a substantial part of a work is also forbidden, but there is no definition of ‘substantial’; it depends on context.

The work has to be an original one, but the level of originality required is minimal. Compilations and lists are included as they do require mental effort in their creation. Two cases decided by the courts concerned football fixtures for the Pools and broadcasting schedules for the Radio Times and TV Times. Therefore one can conclude that an index would count as a copyright work.

The one question that remains is, does an index attract an independent copyright, or is it a derivative work? There is no case law on indexes to refer to, but in general the existence of an independent copyright implies enough intellectual input to create a separate work. Thus a simple computer-generated KWIC or KWOC index would probably not count as separate, but human-created indexes would be separate. Translations normally have their own copyrights, as do many musical arrangements such as a transposition from full orchestra to keyboard. In practice an indexer should determine the copyright position by contract before starting work.

Copyright law forbids certain actions by unauthorized people, with a few exceptions for library copying and fair-dealing copying. If infringement is suspected it must be dealt with by a civil action in the High Court. If successful, available penalties include delivery up of all stock to the owner, or payment of the value of all copies made, or special damages for flagrant illegal behaviour, or an injunction not to copy any more material.

International protection

The protection of the UK Copyright Act exists in the UK only, but membership of two international conventions, the Berne and Universal Copyright Conventions, spreads this protection to nearly all the world. Essentially, each country protects the works of foreign convention members to the same extent as it protects the works of its nationals.

Neither in the UK nor under the Berne convention are any formalities required. Copyright protection exists automatically from the moment a work is created. The familiar © together with the name of the copyright owner and date of first publication are required for coverage under the Universal Convention whose adherents accept this as sufficient from foreigners, irrespective of what formalities they may require from their own nationals. The USA in particular is a member of the