DATA PROTECTION AND THE CHURCH OF ENGLAND

JAMES BEHRENS

of Lincoln's Inn and the Middle Temple, Barrister

1. INTRODUCTION

Computers are in use throughout society—collecting, storing, processing and distributing information. Much of that information is about people—'personal data'—and is subject to the Data Protection Act 1984.[1]

The Act is derived from the Council of Europe Convention for the Protection of Individuals with Regard to the Automatic Processing of Personal Data (1981). That convention set out to maintain a 'just balance between the different rights and interests of individuals' and in particular between the freedom to process information on the one hand and rights of privacy on the other.

The Act gives rights to individuals about whom information is recorded on computer. They may find out information about themselves, challenge it if appropriate, and claim compensation in certain circumstances. The Act places obligations on those who record and use personal data (data users). They must be open about that use by registering under the Act all the purposes for which they use personal data, and they must follow sound and proper practices set out in the Act concerning the data (the Data Protection Principles).

The Act has important consequences for the Church of England. At the parish level, computers may be used for membership and electoral rolls, the organisation of finance, and the administration of covenants. A minister may keep records of those members of the congregation with personal experience in particular areas (e.g. members who in the past have had marital problems, alcoholism, drug addiction, sexual abuse, or occult involvement), in order to assist his pastoral ministry where similar problems arise in his ministry. At the diocesan level, computer records may be kept for the purpose of placing ordination candidates with parishes, to deal with diocesan finance, in connection with ecclesiastical discipline, e.g. under the Incumbents (Vacation of Benefits) Measure 1977, and by various diocesan organisations. At the national level, computers are used by the Church Commissioners, Church House, the Central Board of Finance, General Synod, and by the numerous advisory committees, commissions and boards forming part of the central structures of the Church of England.[2] All these need to consider the application of the Data Protection Act 1984.

2. REGISTRATION

(a) The need to register

The Act is concerned with 'personal data', meaning information which relates to a living individual who can be identified from that information (or from that and other information in the possession of the data user).[3] Information can be as little as a name and address. In most cases it will be clear whether or not information relates to an individual: thus a database held by a theological college containing

[1] I am most grateful for the assistance of the Office of the Data Protection Registrar, particularly Miss Sharon Rowland, in preparing this paper.

[2] See the list in the Church of England Yearbook 1995 pages 24–42.

[3] Section 1 (3).

details of all its ordination candidates is an obvious case where the data user (the theological college) needs to be registered. However, in some cases where the database contains personal data, this is almost incidental to the primary purpose for keeping the database, and the data user may not realise that the Data Protection Act 1984 applies. Thus, for example, in some dioceses a computer system is in operation to deal with faculty applications. The main purpose of such systems is no doubt to improve the efficient running of the faculty jurisdiction within the diocese, not simply to obtain the names and addresses of the churchwardens and the incumbents for each application. However the records are likely to contain this information, and possibly the names and addresses of other interested parties. Thus the applications contain personal data, and the registrar of the diocese should be registered.

(b) The exemptions from registration

There are important exemptions from the requirement to register.

(1) Word processing[4]

Using a computer merely for word processing does not require registration. But these days, with computers containing large hard disks, correspondence is frequently kept on a computer after the letter has been printed, as a record of what has been sent. In these circumstances, the computer is not being used *merely* for word processing, and the Act does apply.[5] The vicar who uses his computer merely for the preparation of his sermons need not register. Once he starts keeping correspondence on his computer, and especially if he types up an address list for future reference, he needs to be registered.

(2) Private and recreational use[6]

Personal data held by an individual and concerned only with the management of his or her personal, family or household affairs, or held by him or her only for recreational purposes is also exempt. The exemption only applies where the personal data is held by an individual. It cannot apply to personal data held by an organisation, e.g. a church. Nor will it apply where an individual keeps records on behalf of a church. Then the church, rather than the individual, will be the data user, and the individual will be merely controlling the data and use of the data as servant or agent of the organisation. The individual need not register but the organisation may need to do so. If the church organist keeps a record on his computer of the names and addresses of the choir, this is unlikely to fall within the exemption; *a fortiori* if the organist is paid by the church for running the choir. In these circumstances the P.C.C. should be registered.

(3) Information that the law requires to be made public[7]

Personal data is exempt if it comprises information which is required by statute to be made available to the public. The parochial electoral roll is a case in point, as this is required to be published.[8] However the electoral roll comprises only the list of names and addresses. If telephone numbers are recorded on the computer, the exemption does not apply.

[4] Section 1 (8).

[5] It is partly for this reason that barristers are recommended to register under the Data Protection Act 1984: see James Behrens and Owen Davies: Holding Data, Counsel, October 1993, page 24.

[6] Section 33.

[7] Section 34 (1).

[8] 'by being exhibited continuously for not less than fourteen days before the annual parochial church meeting on or near the principal door of the parish church': see the Synodical Government Measure 1969, Schedule 3 [the Church Representation Rules] Rule 2(3) (1995 edition).

(4) Payroll, pensions and accounts purposes[9]

Personal data is exempt if it is held only for payroll and accounts purposes, i.e. calculating amounts payable as remuneration for service in any employment or office, calculating amounts payable as pensions for service in any employment or office, paying remuneration or pensions, paying amounts deducted from remuneration or pensions (e.g. National Insurance Contributions), keeping accounts relating to the church, and keeping records of purchases, sales or other transactions in order to ensure that any necessary payments are made by or to the data user for those transactions. Thus, if the church were registered for VAT, and ran a coffee bar as part of its missionary activity, the VAT accounting would fall within the exemption. Using a programme such as *Quicken*® for the church accounts and to pay the salary of a lay worker is exempt.

Covenants should be mentioned here. Using the computer to assist reclaiming income tax on covenants is within the exemption. But using the computer to provide the church with the names and addresses of those who have covenanted in the past, so that these persons can be invited to renew their covenants, is not within the exemption. In these circumstances the computer is being used for fund raising, and the P.C.C. should register this as one of the purposes for which personal data is held.

Even though personal data is exempt under this head, it may only be disclosed in very limited circumstances, broadly for the purpose of audit and giving information about the Church's financial affairs, e.g. for diocesan statistics, and for tax and similar purposes.

(5) Mailing lists[10]

Personal data held only for the purpose of distributing, or recording the distribution of, articles or information to individuals is exempt from registration provided four conditions are satisfied. First, the personal data must consist of only the names and addresses of the individuals or other details needed to contact them, e.g. perhaps fax numbers. If more information is recorded, e.g. as to the occupation, status, interests or preferences of the individual, the exemption does not apply. Second, the personal data must only be used for this specific purpose; if it is used for other purposes, the exemption is lost. The third condition is that all the individuals must be asked whether they consent to this information being held on computer as a mailing list. The fourth condition is that the personal data may only be disclosed if the person concerned gives his consent to such disclosure.

Thus a mailing list kept solely for the purpose of distributing the parish newsletter, or the minutes of the P.C.C. meetings, fall within the exemption, provided no other information is kept about the persons beyond their names, addresses, and perhaps fax numbers, and provided the mailing list is used solely for this purpose. If ordinary telephone numbers (as opposed to fax numbers) are also kept, the list would inevitably be used as a general contact list, once held on a computer, and this would breach the terms of the mailing list exemption.

(c) How to register

Registration currently costs £75 for three years. Application should be made to the Data Protection Registrar, Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF, telephone 01625 535711. It is a criminal offence not to be registered if one should be, and the maximum fine in the Magistrates Court is currently £5,000. If

[9] Section 32.
[10] Section 33 (2) (b).

the prosecution were brought in the Crown Court the fine is potentially unlimited. There are two different forms available for registration: the full (DPR1) registration form, and a specially shortened registration form (DPR4) which provides a shorter and simpler means of registration than the DPR1 form and covers the four main purposes for which most small businesses need to register (personnel/employee administration; marketing and selling; purchase/supplier administration; customer/client administration). The form DPR4 is intended for use by small businesses, and is not designed for use by a Church or church body.

Using the full registration form DPR1, the applicant must select from a list of thirty-nine classes of data subjects (the types of individuals about whom personal data is to be held), a list of seventy-three classes of personal data (i.e. what type of personal data is to be held), and a list of seventy classes of sources and disclosure (i.e. the sources from which you expect to obtain the personal data, and the persons to whom you expect to disclose the information). The applicant must select also the purposes for which the personal data is to be held. There are seventy classes of standard purposes from which to select. The Data Protection Registrar advises that the purposes most likely to be registered by local churches are P005 (Fund raising), P010 (Membership administration), P019 (Charity and Voluntary Organisation Objectives), and P040 (Other Consultancy and Advisory Services).[11] The applicant is expected to select the appropriate entries for each category.[12]

The notes provided by the Data Protection Registrar[13] advise that before you can complete your registration application form you will need to

> carefully read the notes which accompany the form so that you fully understand exactly what information is required; and
>
> carry out an audit of all your planned and present computing activities so that you are fully aware of all the categories of data, sources of information and uses and disclosures of data which your register entry will need to cover
>
> Once you've done all this, you'll need to set aside *an hour or so* [emphasis added] to actually complete the forms and check that the information you've given covers everything that you do.

This is not exactly encouraging. Registration is undoubtedly the worst part of the whole regime. That said, the Data Protection Office is courteous, efficient and very helpful when dealing with enquiries.[14]

---

[11] See Sharon Rowland: A local church of England parish and registration, December 1994, published by the Data Protection Office. See also by the same author, Churches in Scotland and Data Protection Registration, and Churches in Ireland and Data Protection Registration.

[12] It is fair to point out that the applicant may use a free text description for any purpose, data subject, data class, source or disclosure which is not adequately covered by the standard codes, or if he feels it tobe a more appropriate description.

[13] On a sheet entitled 'How to Register' contained in the Small Business Pack published by the Data Protection Office.

[14] In the recent international survey mentioned on page 000 registration is perceived by the majority of sampled organisations in the United Kingdom, Denmark and France as costly, time consuming and burdensome, often due to complicated forms. Registration seems to be less of a concern for sampled organisations in Ireland, Netherlands and Luxembourg. See Privacy Laws and Business Newsletter No 29 (April 1995), published by Stewart H Dresner, page 25.

The Registrar's Legal Adviser is currently looking at ways to implement a less confusing and more simplified system of registration. The Registrar explains this intention in her latest Annual Report to Parliament, the Eleventh Report of the Data Protection Registrar, June 1995, HMSO, ISBN 0102664951. Any revision of the registration system will obviously be constrained by the requirements of the Act. Section 4 (3) of the Act sets out the information which must be contained in a data user's register entry. Any new system would, I imagine, include the use of various codes as there is a clear need for uniformity in the way in which data users describe their practices on the register entry. The register is, after all, a public document and must be as clear and uniform as possible.

(d) Who should be registered?

The person to be registered is the data user. The data user is the legal person who controls the contents and use of a particular collection of personal data.

Taking first the parish level, the P.C.C. and the incumbent each have an independent legal status. The P.C.C. is responsible for the administration of the parish, so that broadly speaking any administrative data held on computer at parish level would need to be registered in the name of the P.C.C. It is possible that the incumbent of the parish might hold pastoral data relating to parishioners and might therefore need to be registered separately as a data user. Personal data held by an individual, as a member of the Church, on behalf of either the P.C.C. or the vicar, would be required to be registered by the P.C.C. or the vicar respectively. The treasurer is accountable to the P.C.C., so if he holds information about covenants which he uses for fund raising, it is the P.C.C. which should be registered.[15]

The conclusion to be drawn is that unless a Church falls within the very limited exemptions, the P.C.C. or the incumbent (or perhaps both) should register under the Act. Although a Church which is just starting to use computers may perhaps fall within an exemption now, the chances are that within a few months it will no longer (for example, as correspondence is kept on the computer, or as new uses are found for the computer). The safe course is to register now; the fee, though unwelcome, is not exorbitant; registration avoids the possibility of criminal prosecution; registration should also alert the Church to good computer practice (the Principles). Registration is however exceedingly bureaucratic and an appalling example of form filling.

At the diocesan level, several bodies should be registered. Section 5 of the Act restricts a *person* from holding data unless registered. A person in law includes incorporated bodies, but not committees, as these do not have legal personality separate from the persons comprised in them. The following bodies should be registered, if they hold personal data, as they all enjoy legal personality: the bishop, his registrar, the diocesan board of finance,[16] the diocesan parsonages board,[17] and the archdeacons. The diocesan synod does not enjoy legal personality, and therefore cannot be separately registered in its own name.[18] In practice the diocesan office should register under the name of the diocesan board of finance, which covers all data held for the diocesan synod.[19] The various diocesan organisations such as the pastoral committee, the diocesan board of education, the diocesan advisory committee, the diocesan board of patronage, the board of social responsibility *et al.* do not need separate registration as they lack legal personality.

At the national level, the Church Commissioners[20] are registered under the Act.[21] The General Synod and the Convocations of Canterbury and York lack legal personality, and so are not registered. Data held by Church House is registered under the name of the Central Board of Finance of the Church of England, which is both a company and a registered charity. The Church of England Pensions Board is registered. The Archbishop of Canterbury's staff at Lambeth Palace are

[15] This has the advantage that no new registration is needed if a new person becomes the treasurer.

[16] See Diocesan Boards of Finance Measure 1925 Section 1: 'Every Diocesan Board of Finance shall be registered as a Company under the Companies Acts'.

[17] See Repair of Benefice Buildings Measure 1972, Section 1(5): 'A Parsonages Board shall be a body corporate, with perpetual succession'.

[18] The Synodical Government Measure 1969 does not attribute legal personality either to the General Synod or to a Diocesan Synod.

[19] All contracts of employment within the diocesan office would of course be made with the diocesan board of finance.

[20] A body corporate: see the Church Commissioners Measure 1947, Section 1 'a body corporate having perpetual succession and a common seal'.

[21] Registration number B 0401158.

registered as 'Lambeth Palace'.[22] The workings of the Crown Appointment Commission are covered by the registration of the Church Commissioners.[23]

3. THE DATA PROTECTION PRINCIPLES

(a) Overview

There are eight Data Protection Principles.[24] Compliance with the Data Protection Principles is central to the purpose of the Act. The Principles are very general, and are mainly concerned with good practices which computer users would generally aspire to. Computer users will need to review their procedures to ensure that they do comply with the principles. The Act requires the Registrar to promote the observance of the Principles. If registered users contravene them, the Registrar can take action against them. In the first place, the Registrar can serve an enforcement notice requiring the user to take particular steps to comply with the Principles in the future. Failure to comply with an enforcement notice is a criminal offence. The Registrar can also serve a de-registration notice if the Registrar considers that compliance cannot be adequately secured by the service of an enforcement notice. The effect of a de-registration notice is that the data user can no longer legally undertake the activities which were previously covered by the data user's entry. Thus the user would no longer be able to hold personal data on computer.

The first six principles establish general standards of data quality. In summary, they specify that data must be:

- obtained fairly and lawfully; and processed fairly and lawfully;
- held only for the specific and lawful purposes contained in the register entry;
- not used or disclosed in a manner incompatible with those purposes;
- relevant, adequate and not excessive for those purposes;
- accurate and where necessary kept up to date;
- not kept longer than necessary.

The seventh principle provides an individual with the right to be informed upon request of all the information held about them on computer by a particular data user. This is known as making a subject access request.

Finally, the eighth Data Protection Principle deals with security. This covers the protection to be given to the computer hardware and software, and protection of the personal data, such as having a formal disclosure policy.

Much advice has been given by the Registrar's office about the application of the principles to differing types of businesses and varying business practices.

For a large organisation compliance with data protection legislation will require some form of management structure and control. Often this is best achieved by the appointment of a data protection officer who should provide guidance at all levels of responsibility within an organisation on specific procedures which should be followed. It should be the responsibility of the owner of the data to inform the data protection officer about any proposals to keep personal information on a computer; and to ensure awareness of the data protection principles defined in the legislation.[25] Church House has such an officer,[26] and diocesan organisations should do so too.

---

[22] Registration number F 129512 X. This is no doubt convenient, as there are several bodies which contribute financially to the running of Lambeth Palace. But Lambeth Palace plainly lacks legal personality, and so should not need to register at all.

[23] The Crown Appointments Commission's secretary, Mr. Hector McClean, is paid by the Church Commissioners.

[24] Sections 3, 10–20, and particularly Schedule 1 to the Act.

[25] See the code of practice for information security management BS 7799, section 10.1.3.

[26] Douglas Fryer, the Data Protection Co-ordinator for the Central Board of Finance at Church House.

(b) The eight principles in detail[27]

The eight principles are as follows:

(1) The information to be contained in personal data shall be obtained, and personal data shall be processed, fairly and lawfully.

When you collect information from individuals, you must be honest and open about why you want it. The Registrar has received many complaints about information unfairly obtained in situations where it is to be used for direct marketing purposes. It might not be thought that this applies to the Church of England, but one can envisage problems where a theological college distributes a list of its ordination candidates to a local theological book supplier, or where a Church distributes a list of members of its congregation to a charity which then uses that list for fund raising.[28]

Within the parish setting, most information concerning members of a congregation will be given by the data subjects themselves. But churches and priests should be careful before including sensitive information on computer if the source of the information is from a third party. Was the information given in confidence, for example? If so, it is almost certainly not compatible with this principle for the information to be recorded on computer. A priest should not record on his own computer, *a fortiori* not on anyone else's, matters which are told him in the context of private confession, as the data subject would not expect this.[29]

(2) Personal data shall be held only for one or more specified and lawful purposes.

This is the corollary of the complex registration procedure. If a Church does not include fund raising as one of the purposes of registration, it would be illegal for the Church to use its computer for fund raising, e.g. by circulating members of the congregation who have previously made gifts to the Church.

(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.

Consider the following situation. One of the tenors in the Church choir has fallen sick. The organist rings the vicar of another church asking him if he knows of any tenors in his congregation who could stand in for the concert next Saturday. The vicar looks on his computer address list for the word 'tenor', and gives the organist a list of five persons who might fit the bill. This is probably *de minimis*, and unlikely to incur the wrath of the Data Protection Registrar if a complaint were to be made, but it can hardly be said that the disclosure is compatible with the Church purposes which have been registered. The proper procedure is for the vicar to telephone the individuals concerned to ask their permission for their

[27] Schedule 1 to the Act.

[28] Use can be made of forms containing opt-out boxes. These include a notification of any non-obvious purpose for which an individual's personal data will be held, and allow the data subject a chance to opt-out of such an additional use of their personal data whilst retaining the original relationship with the data user. Take for example a Church with close links with a local Christian Charity. The Church chooses to pass parishioners' details to the charity so that the Charity can then approach these persons for help. The Church could include notification of this policy on the form used to collect the details of new parishioners. A tick box could be provided by which a parishioner could indicate that he did not want his details to be passed on to the charity. He could then provide the Church with his details, safe in the knowledge that they would not be disclosed.

[29] Schedule 1, part II, paragraph 1 (1) provides that 'in determining whether information was obtained fairly regard shall be had to the method by which it was obtained, including in particular whether any person from whom it was obtained was deceived or misled as to the purpose or purposes for which it is to be held, used or disclosed'. Read with the unrepealed proviso to canon 113 of the Canons Ecclesiastical 1603, it cannot be right that matters confessed are thereafter recorded on computer, for the confessor would not expect any record to be kept of what he had said.

names to be given to the organist before he does so. For information can always be disclosed if the data subject consents.

Consider the common situation of a person inquiring from the vicar if he knows the address and telephone number of a member of his parish. If the address is held on computer, the proper course for the vicar is not to give this information to anyone who asks for it, but to ask the member whether he minds his address being given to the inquirer.

Consider also the following situation: a person leaves church A and joins church B. The vicar of church B telephones the vicar of church A, and asks what vicar A can tell him about the person. The vicar of church A tells the vicar of church B what is on his computer. Although the information on vicar A's computer may be innocuous, it is unlikely that when the information was disclosed to vicar A, consent was given for it to be disclosed to vicar B.

(4) Personal data held for any purpose or purposes shall be adequate, relevant and not excessive in relation to that purposes of those purposes.

If a bishop keeps computer files on the clergy in his diocese, and these records include matters relating to clergy discipline, it may be *excessive* or *irrelevant* if this sensitive information is old. To draw an analogy from the publicity concerning the recent appointment of the Bishop of Durham, it might not be appropriate to record on computer a conviction twenty years old of some sexual impropriety of a curate unless this were considered still relevant either to future discipline or to possible promotion within the Church of England.

Another example is the case of vicars who keep computer records of couples coming to be married. Cases have arisen where the vicar has entered a code onto the record indicating whether or not the couples have been cohabiting.[30] This is surely excessive.

An example of information which would probably be acceptable in a church situation is recording the age of parishioners, as this information may be helpful when organising particular events for particular age groups. What the fourth principle requires is that each church considers such questions, and holds only the data which it actually needs.

(5) Personal data shall be accurate and, where necessary, kept up to date.

Provided that the information is obtained fairly and recorded accurately, you may assume that you are complying with this principle unless the data is challenged by the individual to whom it relates. The remedy for breaches of the fifth principle is simply the correction of the errors. However, if anyone suffers damage as a result of inaccurate data they can sue for compensation through the courts.

(6) Personal data held for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes.

The principle implies that only in exceptional circumstances should data be kept indefinitely. Once a member of a congregation has moved to another church, any personal data about him or her should normally be deleted from the computer belonging to the first church. It is probably unobjectionable to keep a record of a person's new address, as there may be persons wishing to contact them; but even in these circumstances, the vicar should first contact the person to ask whether they mind their address being given to the inquirer.[31] Even then, it would probably not be appropriate to hold such contact details indefinitely.

---

[30] My source for this information is Douglas Fryer. see footnote .

[31] There are circumstances where a new address could be sensitive information.

(7) An individual shall be entitled[32]

(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.

The data user can charge a fee of up to £10 for each register entry for supplying this information. The request must be responded to within forty days. If not, the data subject is entitled to complain to the Registrar or to apply for a court order for access.

Personal data may sometimes be withheld; for example, personal data held for crime prevention or detection, or taxation purposes need not be disclosed where disclosure may be likely to prejudice the purpose in question. Personal data may also be withheld where a claim to legal professional privilege could be claimed in legal proceedings. An exception is also made for certain health data if it is recorded by a health professional.[33] The health professional may withhold from the data subject any personal data which would be likely to cause serious harm to the physical or mental health of the data subject. Thus if a doctor and a vicar are together providing medical and pastoral care to a member of the congregation who has mental illness, and the doctor has disclosed to the vicar details of the mental illness suffered by his patient, the vicar would not have to disclose this information under the subject access provisions without consulting first the doctor and asking whether disclosure was appropriate.

Another exception concerns judicial appointments. Personal data held by a government department is exempt from the subject access provisions if the data consist of information which has been received from a third party and is held as information relevant to the making of judicial appointments. Consistory court judges (i.e. chancellors or, in the case of Canterbury, the commissary general) are appointed by the bishop of the diocese where they will preside, not by the Lord Chancellor,[34] so files kept by the bishop for this purpose would not be exempt.[35]

Theological colleges should study the special rules relating to disclosure of examination marks.[36]

Sources of information do not have to be disclosed. Thus a priest would be entitled to know the substance of complaints made about him to his archdeacon or bishop, though he would not be entitled to be told the identity of the persons who have complained about him, unless these persons consent to this information being given to him.[37]

---

[32] see Section 21.

[33] Under the Data Protection (Subject Access Modification) (Health) Order 1987, S.I. 1987 No 1903.

[34] though both the Dean of Arches and the Lord Chancellor are to be consulted: Ecclesiastical Jurisdiction Measure, Sections 2 (1) and 2 (1A).

[35] Norman Doe in an unpublished paper entitled Churches in the United Kingdom and the Law of Data Protection presented to the Europäisches Datenschutzrecht und die Kirchen convention in Berlin 1994 says that there are strong arguments to suggest that the episcopal office might be classified as a government department for the purpose of Section 31 (1) of the Act, and hence a candidate for ecclesiastical judicial appointment may have no right of access to such files. *Sed quaere.*

[36] Section 35.

[37] see Sections 21 (4) (b) and 21 (5), and paragraph 2.25 of the Guidelines. If the complaints cannot be told without identifying the complainant, the archdeacon or bishop does not have to disclose the information unless he is satisfied that the complainants have consented. This is not however an open invitation for members of the public to write letters for which they are unaccountable. If the information was to be used in legal proceedings, the identity of the complainants would save in exceptional cases have to be disclosed for the evidence to be admissible. The archdeacon or bishop should in most cases therefore encourage the complainants to give their consent for their names to be disclosed.

(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.

Because the Act applies equally to all computer users whatever their size or the nature of the data they hold, it does not specify what 'appropriate security' might be. The new British Standard, the code of practice for information security management,[38] while not being a full specification, gives excellent general guidelines for analysis and remedy. At least the following issues should be considered.

(a) Authorised access to computer records by staff

In many churches or diocesan offices all personal information may be held on a single computer to which all staff have access. This may be perfectly acceptable, but there will be many cases where only some staff should have access to all records, and only some of these should be permitted to amend or delete them. Particular attention should be given to:

- Passwords. These should be changed fairly frequently.
- Established procedures. These should be written and should set out who is authorised to access which records and for what purpose.

(b) Access to records by individuals other than staff

Clear procedures should be established specifying to which particular individuals and organisations data may be disclosed. In a church setting, many individuals will consent to their address and telephone number being given to other members of the fellowship. But it cannot be assumed that all people will agree to this: females particularly may be unwilling for their address and telephone numbers to be given to persons they do not know well, even if these persons attend the same church.

(c) Prevention of the accidental loss or theft of personal data

Procedures, passwords and the correct location of terminals may deal with everyday security. Attention must also be given however to unforeseen contingencies such as the theft of computer equipment, fire or even power failure. Obviously no system is fool-proof but consideration should be given to

- Keeping back-up copies of files in secure areas away from the computer equipment upon which they are normally used. Make a practice of doing backups of the main files on a regular basis—weekly, or even daily if the files are altered daily. For £200 to £300 a computer can be fitted with a tape drive which makes backing up the whole of a hard disk a simple operation.
- The physical security of the computer equipment. Computers left unguarded in an office area in a church may be an easy target for a walk in thief. To minimise this risk I recommend one of the many security kits on the market costing £20 to £25. These attach the computer to a piece of furniture with a steel cable and a lock.

(d) Sensitive data

The Act sets out four categories of personal data which are considered to be especially sensitive.[39] These are:

[38] BS 7799. In force from 15 February 1995. Copies obtainable from the British Standards Institution. Telephone 0181-996 7000.

[39] Section 2 (3). The categories are set out merely in case the Secretary of State should wish make an order modifying the effect of the Principles in relation to data containing such information. No such order has been made to date.

- the racial origin of the data subjects;
- their political opinions, religious or other beliefs;
- their physical or mental health, or sexual life;
- their criminal convictions.

If a minister holds such personal data or even if he has been given information 'in confidence' then additional security measures may be appropriate. In particular, it is probably not appropriate for such information to be held on a computer to which all members of staff have access; for even passwords are by no means foolproof.[40]

(e) Viruses

Computer viruses can wreck havoc on a computer.[41] No system is foolproof, but a very good start is to use one of the commercially available anti-virus programmes which can run in the background the whole time the computer is on, and which sound a warning if a disk containing a virus is used. Large organisations have procedures under which all disks used in the organisations' computers have first to be tested by a special computer, and only used in other computers when they have been 'sheep dipped' in this way. This is probably unnecessary in a small church setting, but should be considered by theological colleges, diocesan offices and particularly large churches.[42]

[40] There are plenty of companies and programmes on the market offering to 'unlock' password protected files. If a person seeking information about a particular person made a copy of the password protected file onto his own floppy disk, he could use one of these programmes on his own computer, or he could pay a third party to unlock the password, whereupon all the sensitive information would be laid bare. I do not anticipate that the companies with this expertise make detailed enquiries whether the person seeking access to the file is entitled to such access before offering their services. And if the whole computer is stolen, it is comparatively easy for a person with technical knowledge to bypass a password which protects the whole computer.

[41] A virus, in computer terms, is a programme which usually has two distinct purposes:

- To stop the user from working efficiently. This may happen by the virus displaying annoying messages at random on the screen, playing random notes through the computer loud speaker, or (and this is much more serious) by destroying or corrupting files on a whole disk drive or an entire network.
- To spread itself so that it may carry on infecting files on other computers.

If a floppy disk containing a virus is placed in a computer, and the user tries to access the floppy disk, for example, in order to copy a file onto the hard disk of the computer, the virus will load itself into the computer's Random Access Memory (RAM), and then infect the hard disk of the computer. From then on, each time the computer starts up the virus will be loaded into memory and will probably infect each new disk which is placed in the drive. And in the meantime it will start corrupting the files on the computer or do whatever else it was designed to do.

[42] I find it extraordinary that the Data Protection Guidelines omits any mention of viruses in its discussion of security. The UK Regulatory document Security and the 1984 Act—Guidance for Computer Users, published in 1987 by the Department of Trade and Industry and the National Computing Centre (printed in the Encyclopaedia of Information Technology Law Section H1.601) also makes no mention of viruses. Yet viruses were already a problem in 1987.
In the Price Waterhouse / Priority Data Systems Computer Virus and Security Survey, February 1995 the incidence of viruses over the last year was found to be as follows:

Company Type	Virus Incidence
Top 200	61%
Financial	72%
Smaller	35%

When Price Waterhouse conducted its previous survey in 1991, the incidence rate reported by the top 200 companies was 28%. In other words, the incidence of viruses is increasing. The most frequently reported viruses according to the survey are Form, Ripper, Cascade, Tequila and Stoned. There are over 5,500 known viruses, including one called AntiClerical (S&S Internationa—the manufacturer of a well known anti-virus programme—describe it as 'quite infectious')! I have twice received virus infected disks from solicitors in the course of my professional practice. The code of practice for information security management BS 7799, deals with viruses in section 6.3.1.

4. INDIVIDUAL RIGHTS

The rights of individuals about whom personal data is held on computer have already been mentioned briefly. But it is useful to look at these rights together under one head. The rights are as follows:

(a) Subject access

An individual is entitled to access to information held about himself on computer, and where appropriate to have it corrected or deleted. This is known as the 'subject access right', and it means that the person is entitled, on making a written request to the data user, to be supplied with a copy of any personal data held by the data user. The data user may charge a fee of up to £10 for each register entry for supplying this information, but in some cases it is supplied free.

Usually the request must be responded to within forty days. If not, the person is entitled to complain to the Registrar or to apply for a court order for access. If personal data is found to be inaccurate, the person may complain to the Registrar or apply to the Court for correction or deletion of the data.

(b) Access to the register

The Data Protection Register is open to public inspection at the Registrar's office in Wilmslow. Copies of individual register entries are available free of charge. A register entry only shows what a registered user is registered to do: it does not reveal whether or not that data user holds personal information about any particular individual.

(c) Complaints to the Registrar

If a person considers that there has been a breach of one of the Data Protection Principles (or of any other provision of the Act), he is entitled to complain to the Data Protection Registrar. If the Registrar considers the complaint is justified and cannot be resolved informally then he may decide to prosecute or to serve an enforcement notice or notice of refusal of registration on the data user in question.

(d) Compensation

A person is entitled to seek compensation through the Court if damage (not just distress) has been caused by the loss, or unauthorised destruction or disclosure of personal data. If damage is proved, then the Court may also order compensation for any associated distress. A person may also seek compensation through the Court for damage caused by inaccurate data.

5. REFORM

(a) The European Union General Data Protection Directive

On 24 July 1995 the European Union General Data Protection Directive was agreed by the Council of Ministers; it had taken five years for the Directive to pass through the European legislative process.[43] It is anticipated that the Directive will be formally adopted in the Spring of 1996. Within three years of formal adoption there must be national legislation implementing the Directive; in the United Kingdom this will probably take the form of primary legislation (a new United Kingdom Data Protection Act) but could instead be implemented by regulations under the European Communities Act 1972.

[43] See Insights: European Union Data Protection Directive, July 1995, published by the Data Protection Office.

The Directive sets out to 'protect the fundamental rights and freedom of natural persons, and in particular their right to privacy, with respect to the processing of personal data'. The United Kingdom Data Protection Act 1984 introduced measures of protection for individuals which have enabled the United Kingdom to ratify the Council of Europe Convention on Data Protection. But unlike the Convention and the Directive, the Act does not refer to privacy.

There are similarities between the provisions of the Directive and those of the Act. Common features include the following:

- registration (called 'notification' in the Directive) will remain, though with the option of a simplified form of registration and further exemptions from registration;
- the general principles of good practice, familiar in the United Kingdom as the eight Data Protection Principles, are incorporated in the Directive; and
- an independent supervisory authority will enforce national data protection legislation, as the Data Protection Registrar currently does.

Elements incorporated in the Directive and new to the United Kingdom include the following:

- the inclusion of some manual records within the scope of data protection legislation;
- rules about the legitimacy of processing;
- special rules for the processing of particularly sensitive personal data: i.e. racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, and data about health or sex life, criminal offences or convictions;
- to protect freedom of expression, exemptions for personal data processed for journalistic purposes or artistic or literary expression;
- a duty on all 'controllers' (data users) to comply with data protection rules whether or not registered under the new system; and
- provisions designed to ensure that generally personal data being transferred to non-European Union countries will be adequately protected.

Whereas many church and diocesan organisations may escape the provisions of the Data Protection Act 1984 because all records containing personal data are kept in ordinary files rather than on computer, when the new directive becomes law in the United Kingdom, users of these records will also need to register under the Act, and comply with the Data Protection principles of good practice.[44]

(b) Manual records

The reason for including manual records within the directive is set out in the preamble to the directive[45]:

> Whereas the protection of individuals must apply as much to automatic processing of data as to manual processing; whereas the scope of this protection must not in effect depend on the techniques used, otherwise this would create a serious risk of circumvention; whereas, nonetheless, as regards manual processing, this Directive covers only filing systems, not unstructured files; where-

[44] Two perceptive and useful commentaries on the Common Position are (1) the article by Vivianne Jabbour and Heather Rowe: The Proposed Data protection Directive and the Data Protection Act 1984 in [1995] Computer and Telecommunications Law Review 38 published by Sweet & Maxwell, and (2) Privacy Laws and Business Newsletter No 29 (April 1995), published by Stewart H Dresner.

[45] The text of the Common Position of the Council of Ministers as agreed on 20 February 1995 is the latest published version of the Directive. The final text of the Directive as agreed on 24 July 1995 is yet to be published. The Data Protection Office states 'The final text of the Directive is close, but not identical, to the text of the Common Position'.

> as in particular the content of a filing system must be structured according to specific criteria relating to individuals allowing easy access to the personal data; whereas, in line with the definition in Article 2 (c) the different criteria for determining the constituents of a structured set of personal data, and the different criteria governing access to such a set, can be laid down by each Member State, whereas files or sets of files as well as their cover pages, which are not structured according to specific criteria, shall under no circumstances fall within the scope of this Directive.

In summary, the inclusion of manual data is a response to the fear that if both methods of processing data are not provided for within the Directive, the protection offered by the Directive would not be complete, and there would be a serious risk of circumvention of its provisions, as organisations may resort to keeping manual files in order to evade the privacy rules. However no evidence has been adduced to show that such a fear is well-founded.

There can be no good reason why disclosure of a member of a congregation's address should be prohibited if that address is kept on computer, but not prohibited if the address is merely kept on a typed list, or in an address book. In other words, many of the Data Protection Principles represent good practice, whether the records are manual or kept on computer.

It is clear that the directive is not intended to apply to *all* manual records. Article 3, which establishes the scope of the Directive, states that it shall apply to the 'processing of data wholly or partly by automatic means, and to the processing otherwise than by automatic means of personal data which form part of a file or are intended to form part of a file'. So the first limitation is that manual records are only included if they form part of a file or are intended to form part of a file. The disorganised priest who keeps no files thereby escapes.

Article 2 (c) goes on to define a 'personal data filing system' as a *structured* set of personal data. Unstructured files, therefore, are not within the scope of these provisions. How much structure is needed is not specified. Consider a filing cabinet containing a simple A to Z divider with correspondence entered in the appropriate divider according to the recipient's surname. This surely is 'structured according to specific criteria relating to individuals allowing easy access to the personal data'.

The recital makes it clear that the Directive only applies where the criteria on the basis of which a filing system is structured relates to an individual—the name, the address, an individual's number, etc. A set of files structured by the date order would fall outside the scope of the Directive.

Industry has complained that the cost of providing subject access to a whole mass of manual documents may be prohibitive. In practice, however, few people exercise their rights of subject access, and this worry may be unjustified.

(c) The processing of special categories of data

Article 8 provides that Member States shall prohibit the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life. However the Article also sets out certain situations where such data may be processed. This includes where the data subject has given his 'explicit consent' to the processing, where it is necessary to protect the 'vital interests' of the data subject and where it is necessary for the 'establishment, exercise or defence' of legal claims. In addition, and of particular relevance to churches, such data may be processed where

> processing is carried out in the course of its legitimate activities with appropri-

> ate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the consent of the data subjects.

Processing is defined in Article 2 very widely.

> processing of personal data ('processing') shall mean any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organisation, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

Processing thus includes merely recording this information in a file or record about the person, whether the record is a manual record or part of a computer database. Under the Article, a minister would only be entitled to record this sensitive information about members of 'the body'. Where a minister only holds information about members of his own congregation, there is no difficulty in considering these persons as the appropriate 'body'. Ministers sometimes keep records of baptisms, weddings and funerals of persons who are not part of their congregation, and here the concept of 'body' needs to be extended to include parishioners or even all members of the Church of England if necessary.[46]

Under the directive information must not be disclosed to a third party without the consent of the member. The restrictions on disclosure accord with what ministers would normally do anyway.[47] So Article 8 is unlikely to make much difference in practice.

6. CONCLUSIONS

The Data Protection Act 1984 governs data protection in the United Kingdom and was the first legislation in the United Kingdom to address the use of computers. The law of data protection is a legislative attempt to balance the concept of free access to, and use of, information by data users on the one hand, with the competing rights of data subjects to have some say and maintain some control over the use of their personal information. Apart from the law of confidence, the common law has not recognised any general principles of rights over information, particularly where the information in question is generally known (see e.g. *Attorney-General* v *Guardian Newspapers Ltd. (No 2)* [1990] 1 A.C. 109, the *Spycatcher* debacle).[48] And apart from the Data Protection Act 1984 there is very little statutory law in this area.[49]

Data Protection makes no distinction between personal information which is secret and other personal information. The Data Protection Act 1984 applies to all personal data. Personal data is information which (a) relates to a living individual,

[46] Alternatively, it could be argued that such persons are 'persons who have regular contact with [the Church] in connection with its purposes'.

[47] see the unrepealed proviso to canon 113 of the Canons Ecclesiastical 1603.

[48] see R. Austin, 'Freedom of Information: the constitutional impact', in J. Jowell and D. Oliver (eds.), The Changing Constitution (2nd Ed., Oxford, 1989) 409.

[49] Examples are the Access to Personal Files Act 1987, the Access to Medical Reports Act 1988 and the Access to Health Records Act 1990. Secondary legislation under the Access to Personal Files Act 1987 regulates the use of and access to information contained in manual documentary files in certain areas, such as social services and housing. The 1988 and 1990 Acts deal with the problem of patients seeking access to medical information on them held on file, and gives the right to patients to refuse permission for their medical files to be disclosed to employers or insurance companies.

who can be identified from that information or from that and other information in the possession of the data user, and (b) is held in a form by which it can be automatically processed, usually, on computer. Furthermore, there must be an intention on the part of the data user to process the information by reference to the individual.[50]

Many churches have already registered under the Data Protection Act 1984. Perhaps many more churches should register. But the Data Protection Act 1984 is not just about registration; it is also about good computer practice, practice which should be adopted by all computer users, churches and others, and whether or not they process personal data. I suspect that little attention is given to these matters, except perhaps by those organisations which are big enough to justify employing computer professionals to advise them. Elementary security procedures may be all that is required to prevent unauthorised access to confidential data, to prevent loss through theft, and to enable data to be recovered if the unthinkable happens. This aspect of the Data Protection Act 1984 needs to be drawn to the attention of churches again and again.

In 1993 and 1994 the European Union conducted a Privacy Practice study to examine data users' internal practices and procedures for ensuring compliance with the national data protection legislation in Denmark, France, Germany, Ireland, Luxembourg, the Netherlands and the United Kingdom. Some of the sampled organisations could not see particular benefits from compliance with the data protection legislation. They gave the following reasons:

- There are already data protection procedures and data security measures in place.
- Other legislation ensures confidentiality and protection for consumers.
- Compliance is too costly.

However, many organisations mentioned a number of benefits to them from compliance with the law:

- Ensuring data quality
- Improving data security
- Good public image and public relations
- Good business practices and quality of services
- Protection for data subjects and customer care
- Ensuring transparency and raising confidence of data subjects
- Increasing and maintaining staff responsibility
- Changing civil servants' mentality and making public sector activities more transparent.[51]

The last of these benefits is of no particular relevance to the Church of England. But all the rest are. The Church of England, at the national, the diocesan and the parish levels, should be encouraged to comply with all aspects of the Data Protection Act 1984, and thereby to reap these benefits.

For the future, I doubt that when the new European Directive is implemented in the United Kingdom it will make much difference in practice to the Church of England. Manual records will be subject to the same regime as records held on a computer, and therefore the right of subject access is potentially much wider. I do not consider this will become a burden in practice. Probably the main effect will be that Churches will be encouraged to improve on their security and office procedures, so that an appropriate level of protection is given to personal data, in whatever form it is recorded. And this, I suggest, is a good thing.

[50] see section 1 (5) (c) of the Data Protection Act 1984.

[51] Privacy Laws and Business Newsletter No 29 (April 1995), published by Stewart H Dresner, page 25.

BIBLIOGRAPHY

Austin, Rodney: 'Freedom of Information: the constitutional impact', in J. Jowell and D. Oliver (eds.), The Changing Constitution (2nd Ed., Oxford, 1989) 409

Behrens, James and Davies, Owen: Holding Data, Counsel, October 1993, page 24

Doe, Norman: Churches in the United Kingdom and the Law of Data Protection, paper presented to the Europäisches Datenschutzrecht und die Kirchen convention in Berlin 1994

Encyclopaedia of Information Technology Law (Sweet & Maxwell)

Insights: European Union Data Protection Directive, July 1995, published by the Data Protection Office

Jabbour, Vivianne and Rowe, Heather: The Proposed Data protection Directive and the Data Protection Act 1984 in [1995] Computer and Telecommunications Law Review 38 (Sweet & Maxwell)

Price Waterhouse/Priority Data Systems Computer Virus and Security Survey, February 1995

Privacy Laws and Business Newsletter No 29 (April 1995), published by Stewart H Dresner

Rowland, Sharon: A local Church of England parish and registration, December 1994, published by the Data Protection Office

Rowland, Sharon: Churches in Ireland and Data Protection Registration, December 1994, published by the Data Protection Office

Rowland, Sharon: Churches in Scotland and Data Protection Registration, December 1994, published by the Data Protection Office

Security and the 1984 Act—Guidance for Computer Users, published in 1987 by the Department of Trade and Industry and the National Computing Centre

Small Business Pack, published by the Data Protection Office

The code of practice for information security management, BS 7799, British Standards Institution 1995

The Eleventh Report of the Data Protection Registrar, June 1995, HMSO.

The Guidelines, 3rd series, November 1994, published by the Data Protection Office