Data Protection

THE CHURCH OF ENGLAND
RECORD CENTRE

Summary

This factsheet intends to explain what implications the Data Protection Act 1998 (DPA) has for you and how good records management can help with compliance. You will discover:

- Which principles are laid out in the DPA
- When and how to notify the Information Commissioner's Office of the personal data you hold
- How to deal with a Subject Access Request (SAR)

Please note that the information detailed in this note is for general purposes only. It does not constitute legal advice and may not suit your own particular purposes. For legal advice on which you can rely you should contact your own legal adviser(s).

Definitions

Data protection involves some specific terminology which it's important to be familiar with. In particular:

- A **data controller** is an organisation or individual that determines the purposes for which and the manner in which any personal data is processed.
- A **data subject** is an individual about whom personal data is held. For example, if a bishop holds a personal file (blue file) for a priest, that priest will be the data subject with regards to the personal data held on his or her file.
- **Personal data** is, broadly, of any information about a living individual which is capable of identifying that individual. Identification can be by the information alone or in conjunction with any other information in the data controller's possession or likely to come into such possession. It can apply to data held in manual or electronic form. However, the DPA only regulates data held in manual form if it is held in a "relevant filing system" (see below).
- **Sensitive personal data** is personal data relating to an individual's racial or ethnic origin, political opinions, religious beliefs, trade union membership, physical or mental health condition, sexual life, alleged or actual criminal activity and/or criminal record.
- A **relevant filing system** is a system of holding manual (i.e. paper) records from which specific information about a specific individual can be readily accessed. An example of such a system would be a set of employment records consisting of a filing cabinet containing files of named individuals in surname order.
- **Processing** is anything done with or to personal data.

These and other terms are discussed in more detail on the website of the Information Commissioner's Office (www.ico.gov.uk), which is a very useful source of information about data protection and other legislation such as the Freedom of Information Act 2000. It should be noted that the bodies which comprise the Church of England are not subject to Freedom of Information legislation.

Data Protection principles

Good records management is an effective way of ensuring compliance with the DPA. The DPA gives individuals the right to know what personal data is held about them and provides a framework to ensure that personal data is handled properly. With

effect from April 2010, the Information Commissioner's Office (ICO) has been able to issue fines to those who knowingly or recklessly breach the DPA. Compliance is therefore an issue to be taken seriously.

Overview of the eight principles

Schedule 1 of the DPA outlines eight data protection principles, which are paraphrased below. In summary, all personal data must be:

1. Fairly and lawfully processed in accordance with Schedules 2 and 3 of the DPA (see below).

2. Processed for limited purposes notified to the ICO and to the data subject (you cannot use data for another purpose without letting the data subject know).

3. Adequate, relevant and not more than is necessary to complete the task for which it was collected. However, keeping records for historical and research purposes is a legitimate reason for holding data.

4. Accurate and up-to-date (data subjects can request corrections).

5. Not kept for longer than is necessary to complete the task for which it was collected.

6. Processed in line with the data subject's rights (particularly the right of subject access, as described later on in this factsheet).

7. Kept secure, with appropriate technical and organisational measures to protect against unauthorised or illegal processing, or accidental loss.

8. Not transferred to a country or territory outside the European Economic Area, without an adequate level of protection for the rights of data subjects.

Conditions for fulfilling the first principle – processing data fairly and lawfully

Schedule 2 of the DPA sets out a number of conditions that can fulfil the first data protection principle (that data is fairly and lawfully processed). Only one of these conditions needs to be met for any processing operation to proceed lawfully. One condition is obtaining consent from data subjects for the processing of their data – this is perhaps the most clear-cut way of ensuring that processing is fair and lawful. However, alternative conditions include:

- processing to ensure legal compliance
- processing to fulfil a contract with the data subject
- processing in pursuit of the legitimate interests of the data controller

Further advice should be sought if you are unsure about whether the processing you intend will comply with the Schedule 2 conditions.

Schedule 3 sets out additional conditions for processing sensitive personal data (defined as described in the "definitions" section above). In addition to satisfying one of the conditions under Schedule 2, the data controller must also satisfy one of the conditions under Schedule 3. The Schedule 3 conditions are narrower than the Schedule 2 conditions but include:

- Data subjects giving their explicit consent.

- Data processing carried out in the course of the legitimate activities by a body which exists for political, philosophical, religious or trade union purposes, and which is not established or conducted for profit.
- Data processing necessary for equal opportunities monitoring.

As a result of the pastoral nature of much of the Church of England's work, you may often need to process "sensitive personal data" (which, as noted in the "definitions" section above, includes data on religious beliefs). Where such data is processed routinely, further advice should be sought.

How records management supports compliance with the eight principles

Effective records management supports compliance with the eight data protection principals in several ways, including:

- The regular maintenance of electronic and paper filing systems ensures that data is kept up to date.
- Retention schedules ensure that data is kept for no longer than is necessary (the DPA should be borne in mind when drawing up retention schedules). Other factsheets in this series provide retention schedules for parishes, dioceses, bishops and cathedrals.
- A clear filing structure ensures that records are able to be retrieved in accordance with the data subject's rights for access (see below).
- Good records management involves keeping records secure through appropriate physical and technical measures (your filing structure should make reference to which files are confidential and any access restrictions in place).

A key point both for compliance with the DPA and for good records management is that you must know the purpose for which you are holding any information. This will determine how long you keep the information and how you manage it. Other factsheets give advice on looking after your paper and electronic records from the point of their creation to their eventual archiving or destruction. A full list of available factsheets is given at the end of this factsheet.

Notification under the DPA

Under the DPA, data controllers that process personal data in an automated form are required to notify the Information Commissioner's Office (ICO), unless they are exempt. Failure to do so is a criminal offence. A data controller's entry in the ICO's Register of Data Controllers must be renewed annually, for a small fee (a larger fee is payable for certain organisations with 250 or more members of staff).

Exemptions are generally possible for:

- Data controllers who only process personal data for the following purposes: staff administration (including payroll); advertising, marketing and public relations (for their own business activity); accounts and records.[1]
- Some not-for-profit organisations.

The following Church of England bodies will usually be required to notify:

[1] See "Notification exemptions: A self-assessment guide" on the Information Commissioner's website (www.ico.gov.uk).

- Diocesan Boards of Finance and Boards of Education
- Bishops and Archbishops
- Deans and Chapters of cathedrals

For parishes, each incumbent and each Parochial Church Council (PCC) is considered to be a data controller, because each is a separate legal entity that processes personal data. Each needs to decide whether they need to notify. PCCs will generally be classed as not-for-profit organisations exempt from notification. Incumbents (or priests-in-charge) will, however, need to notify if records of pastoral care discussions are held on computer, assuming such records concern beliefs, relationships and opinions, as opposed to simply factual information such as dates of birth or baptism.

The process of notification involves completing the notification form available on the ICO website (www.ico.gov.uk) and then emailing the form to the ICO with the required fee (direct debits are also possible). The resulting register entry will show that data is processed for a number of purposes (most of which are standard ones prescribed by the ICO) and list the relevant data subjects (who the data is about) and data classes (the types of data processed) under each purpose. A data processing purpose used in many church contexts is “Pastoral Care” (this purpose should always be included in the notifications of bishops and incumbents).

Subject Access Requests

The DPA also provides data subjects with important rights, including the right for individuals to find out what personal data is held about them on computer and in paper records in a “relevant filing system” (see “definitions” section above). Such a request for information is known as a Subject Access Request (SAR) and must be made in writing (though this can mean by email or fax, as well as by letter). You are also entitled to charge a fee of up to £10.

You must respond to a valid SAR and have 40 calendar days in which to do so. It is worth bearing in mind that if you choose to charge a fee, the 40 days only start when the fee is received.

Individuals generally use SARs to see a copy of the personal data held about them. However, case law suggests that rights under the DPA are limited to:

- a right to be informed whether personal data is being processed by or on behalf of that data controller
- if data is being processed, a right to be given a description of that data, the purposes of the processing and the recipients of any disclosure

The purpose of subject access is not to assist in the discovery of documents that might assist a person in litigation or complaints against third parties. Thus, strictly speaking, there is no obligation to provide copies of documents containing personal data, just the information which constitutes the personal data in the document. However, it is usually more straightforward to supply a copy of the document either in whole or in redacted form.

It should also be noted that to be “personal data” the data must be biographical in some significant sense (so more than just the mere mention of the individual in a document) and should have the individual as its focus. There is no obligation to provide data which is not “personal data” according to these definitions.

Several exemptions can also apply to disclosure in response to a SAR, including, for example, information that is subject to legal professional privilege or pertaining to a regulatory function. It is also important to be careful about releasing information relating to third parties. The DPA allows you to refuse to comply with a SAR if doing so would involve disclosing information about another identifiable individual, except in cases where the other person has consented to the disclosure, or if it is "reasonable in all the circumstances to comply with the request without that individual's consent".[2] Generally speaking, the rights of an individual to know about his or her data need to be balanced against the rights of others. In cases involving, for example, safeguarding, you should be very careful about the rights of third parties.

Finally, it should be remembered that individuals may contact the ICO for help if they feel they are being denied their subject access rights or believe that their personal data has not been handled according to the eight principles. Complaints are usually dealt with informally, but if this is not possible, enforcement action can be taken. It is therefore sensible to approach data protection as an exercise in risk management and to keep the law in mind in your day to day administrative practices. As mentioned earlier in this factsheet, the website of the Information Commissioner's Office (www.ico.gov.uk) is a valuable source of further guidance.

Factsheets available in the records management toolkit

- What is records management
- Organising your records
- Looking after your paper records
- Looking after your electronic records
- Looking after your emails
- Looking after your multimedia records
- Agreements with record offices
- Access to records
- Data protection
- Copying and copyright
- Glossary

Further guidance

For further guidance please contact the Church of England Record Centre:

15 Galleywall Road, South Bermondsey, London, SE16 3PB.

020 7898 1030

archives@churchofengland.org

Last updated January 2013

[2] Section 7(4) of the Data Protection Act 1998. See the Technical Guidance Note "Dealing with subject access requests involving other people's information" on the Information Commissioner's website (www.ico.gov.uk).