A Practical Guide to the Data Protection Act

by John Woulds

December 2004

The Constitution Unit

Contents

A Practical Guide to the Data Protection Act **5**
What is this Guide? 5
To whom is the Guide directed? 5

1. Introduction **7**
1.1. What is data protection? 7
1.2. What is the scope? 7
1.3. Who are the players? 10

2. Some basic necessities **13**
2.1. Conditions for processing 13
2.2. Notification 15

3. Handling personal data **17**
3.1. Data collection 17
3.2. Disclosure of and access to information 19
3.3. Disclosure to data subjects [3] subject access 20
3.4. Enforced subject access 22
3.5. Data about other individuals 22
3.6. Other requests from individuals 23
3.7. Effect of FoIA 23
3.8. Quality of data 24
3.9. Security 25
3.10. Records management 25

4. What if it goes wrong? **27**

5. Transitional provisions **29**

6. Further information and advice **31**
6.1. Scope of the Guide 31
6.2. Sources of further information and advice 31

A Practical Guide to the Data Protection Act

What is this Guide?

The Data Protection Act 1998 is a difficult piece of legislation, but data protection is simple in concept and does not need to be complicated or difficult in practice.

What you need is a guide, which takes you to the main compliance issues and alerts you to the possible pitfalls but without wasting your time on aspects that are unlikely to be relevant to your role as an official in a public authority.

That is the purpose of this Guide. It addresses those matters that are likely to be most important to you in your daily working life.

The focus is on those aspects of the Act which influence directly how you deal with individuals; some aspects of the Act are not touched on at all (see section 6.1). But if you follow the advice in this Guide, you will understand the main areas of risk when you are handling information about individuals and will have taken steps to deal with them.

This guide was first published in October 2001. There have been two developments since then that make

1. Introduction

Manual data are covered by the Act if they form ¯part of a relevant filing system°. Broadly speaking, this means that they must be structured in such a way as to facilitate the processing of specific information about an individual.

Example 1 [3] Relevant filing system

A personnel department structures its files in such a way that the annual staff appraisal forms are kept in a separate filing system. The forms are indexed by the name of the staff member and the year of the appraisal. The data form ¯part of a relevant filing system° as the structure is such that specific information (ie the annual appraisal for a particular year) for each staff member is readily accessible. The data would form part of a relevant filing system with any structure which achieves the same effect.

If the precise boundary of the manual data definition is important to you, then you will need to take advice, paying due regard to the guidance issued by the Information Commissioner. Our advice, though, is to treat all information as data, in which case, the boundaries are unimportant.

The definition of data also includes data which form part of an accessible record (concerning health, education, housing or social services) and which would not otherwise be covered by the definition. This category is included so as to preserve certain rights of individuals in respect of such data, which were provided in other legislation pre-dating the Act[2].

Effect of FoIA

From 1 January 2005, by virtue of the FoIA *all* manual records held by public authorities come within the definition of ¯data° whether or not they form part of a ¯relevant filing system°.[3] In one respect, this simplifies matters since it means that the way in which personal information is recorded by a public authority is no longer relevant in determining whether that information is ¯personal data° (see below). But it does not mean that all personal information in manual records is now treated in the same way. Only certain provisions of the DPA apply to manual records which do not form part of a ¯relevant filing system° (ie the manual records brought within the scope of the DPA by the FoIA). The position is very complicated. Broadly, the provisions that apply are those which relate to access to personal data either by the individual whose data are held or by a third party; and the right for the individual concerned to have his/her data corrected. The remaining provisions of the DPA do not apply.

Any difficulty over the boundaries between the different elements of the definition of data can be avoided by treating all manual data as data for the purpose of the Act. This is the only sensible practical advice.

Personal data

In order for data to be personal data, the data must relate to a living individual who can be identified from the data or from the data and any other information which is in, or is likely to come into, the possession of the data controller (see section 1.3 for the definition of data controller). (The term ¯relate to° is significant. See the section on the effect of the Durant judgment, on the following page.)

In normal day-to-day transactions with the public, the question of whether data are personal data or not is usually resolved easily. Systems whose function is to support decisions about individuals or achieve

[2] The most significant are the Access to Health Records Act 1990, the Access to Medical Reports Act 1988, the Access to Personal Files Act 1987 and the Housing Act 1988.

[3] FoI Act 2000, s. 68.

the rest of the data protection edifice is built. Almost everything else prescribed in the Act is related in one way or another to compliance with the principles.

2. Some basic necessities

In this Chapter, we mention two technical requirements in the Act which must be taken care of in order for processing of personal data to be lawful. They are: establishing conditions for processing and handling notification.

2.1. Conditions for processing

The Data Protection Principles set a general standard for processing personal data. Principle 1 imposes a general requirement to process fairly and lawfully, but also imposes specific conditions. It makes it an explicit requirement that processing is not allowed unless one or more of the following conditions is satisfied (Schedule 2 of the Act):

Box 2 ³ Summary of conditions for processing any personal data

Personal data may be processed:

± with the consent of the data subject
± to establish or perform a contract with the data subject
± to comply with a legal obligation
± to protect the vital interests of the data subject
± for the exercise of certain functions of a public interest nature
± for the legitimate inteic inte g

2.2. Notification

The Act places an obligation on data controllers (with some exemptions) to notify the Information Commissioner of certain details of any processing of personal data. This is the process known by the term notification.

Most of the details notified by data controllers are recorded by the Commissioner in a public register. Reference to the register allows anyone to understand in general terms the processing carried on by any registered data controller.

Officials other than data protection officers do not need to concern themselves with the notification

Practical Tips 1

- ± Always give a full explanation on forms (on paper or on-line) of why information is needed, who is going to use it, what other sources of information may be used and what choice the data subject has.
- ± Do the same on the telephone the first time information is sought from the data subject, but avoid unnecessary repetition when you make further contact concerning on-going transactions.

3.2. Disclosure of and access to information

Disclosure of information is processing, whether the disclosure is to a member of staff, to a third party outside the data controller's organisation or to the data subject himself or herself. Special provisions apply when the disclosure is to the data subject, and these are dealt with in sections 3.3, 3.4 and 3.5.

Disclosure to other departments or to third parties is constrained in the same way as any other processing. No disclosure of personal data may be made unless there is a fair and lawful basis for it. In the case of processing by a public authority, some disclosures may be providedu su † M l' ! o

Practical Tips 3

- ± Set a timetable for dealing with a subject access request and keep a log of each stage.
- ± Make direct contact with the data subject to establish what information he or she wants and to get any information you need to process the request.
- ± If the request is associated with a complaint, deal with it as part of the normal complaints procedure.
- ± Use any discretion you have on charging in the light of the on-going relationship with the data subject.

3.4. Enforced subject access

Enforced subject access is the practice of some bodies, including public authorities, of requiring an individual to make a subject access request to the police or to another public authority and to make the information provided available to them. This is usually done for the purpose of seeing details or making inferences about the individual's criminal history.

This practice has long been regarded by the Information Commissioner, the police and others, as an abuse of the individual's statutory rights. It will become unlawful once other arrangements for disclosure of criminal records are put in place under the Police Act 1997.

Public authorities which currently make use of enforced subject access should take immediate steps to stop doing so. It is unacceptable for a public authority to continue with a practice which it is known will soon become unlawful.

3.5. Data about other individuals

Sometimes, giving access to personal data to the data subject can not be done without revealing personal data about other individuals. Third party data should not normally be made available without the consent of the individuals concerned, although the Act does not make this an absolute requirement.

If you have the consent of those other individuals, then the information should be revealed. If you have not, then you should seek their consent if it is practicable to ls, l M

yourwi " urhaverdrcony " ! er]h _ theO ierhe _ ir c mhs tance y Ł D he information i " u c,- if- thf2information- concerne,- e, al D eidy1 = m A o n- d- thf2tatf2s M ie- thf3 mi _ s e- f Ł A the e- f tmi " ‘

Example 12 ³ Severing third party information

An email message, edited before release to the data subject, Mr Smith:

To: ³ ³ ³ ³ ³
From: ³ ³ ³ ³ ³
Subject: Mr Smith

Mr Smith keeps calling about his daughter, Sarah Smith. He is very aggressive on the telephone and does not listen to reason. He has been abusive to several members of staff, and both ³ ³ ³ ³ ³ and ³ ³ ³ ³ ³ have complained about him. ³ ³ ³ ³ ³ says that he told her ³ ³ ³ ³ ³ ³ ³ ³ ³ ³ ³ ³ ³ ³ ³. Information from ³ ³ ³ ³ ³ of ³ ³ ³ ³ ³ ³ ³ ³ ³ ³ ³ ³ ³ ³ ³ is that he behaves in a similar way to their staff. I suggest that future contact with Mr Smith should be handled only by James Green, and Mr Smith should be told that politely if his calls coI T M X Mth

4. What if it goes wrong?

No matter how good the internal compliance mechanisms, things will sometimes go wrong. Data subjects will be quick to spot compliance problems and to complain about poor quality data or lax security or failure to give subject access.

Complaints should be dealt with quickly through internal complaints mechanisms. The objective should be to maintain the relationship with the data subject, to resolve the particular issues in question, and to improve standards of compliance overall.

Inevitably, some complaints will go to the Information Commissioner, who will make an assessment of whether the processing concerned is in compliance with the Act or not. The Commissioner does have formal powers of enforcement, but he uses these rarely.

If the complaint concerns a single occurrence of non-compliance which is put r ce

5. Transitional provisions

Prior to 1 March 2000, when the Data Protection Act 1998 was brought into effect, processing of personal data was regulated under the Data Protection Act 1984. The 1998 Act allowed for a transitional period during which, effectively, the more limited provisions of the 1984 Act remained in force for processing which was already under way before 24 October 1998.

That transitional period came to an end on 23 October 2001, so that, in most respects, the 1998 Act applies in full to all processing of personal data, whether in automated or manual form. There remains limited transitional relie ľ s l ◗ ertainl anual b lb d lb d ɔ ɹ p b nab of t ! id ² n.Th]M elie ľ s n i theprovisionsof ; in £ ip e1, os ; rin £ ip es Ɣ, Ơ, ъ an ɱ Ă an ɱ osb lb _ À a ! c ğ s ъ n], eras À re an ɱ destructioq ŏ

T ʌ M ɹ ɱ " h Ƶ im a ϱ s Î я ,

! ɥ

6. Further information and advice

6.1. Scope of the Guide

There are a number of provisions in the legislation which we do not deal with in this Guide, on the basis that they are not likely to be relevant in the day-to-day work of the typical public official. The most important of these are:

± Transfers of personal data outside the European Economic Area
± Data controllers outside the UK
± Exemptions (other than from subje subj

ISBN: 1 903903 38 6