Data Protection Act 1998

Legal Guidance

COMMISSIONER'S FOREWORD

The Data Protection Act 1998 (the "Act"), together with a number of Statutory Instruments (a list of which appears in the annex to this publication) came into force on 1 March 2000, repealing the Data Protection Act 1984.

The Freedom of Information Act 2000 (the "FoIA") received Royal Assent on 30 November 2000. Some of its provisions came into force on or after 30 January 2001, including the change of name of my Office. As at the date of publication of this guidance the substantive provisions of the FoIA have not been implemented. Indeed the Government has yet to make an announcement on the phasing of implementation, which must be effected in full by 30 November 2005. When fully in force, the FoIA will amend the Act in certain respects. This publication reflects only those amendments already in force.

This legal guidance replaces "The Data Protection Act 1998 - An Introduction" which I published in October 1998, prior to the coming into force of the Act. That introductory guidance set out our initial interpretation of the new legislation and served an important role in assisting data controllers acquire an early understanding of it, in advance of implementation.

This publication has been prepared as a reference document for data controllers and their advisers. Where relevant, reference is made to some of the most important Statutory Instruments. This should assist in interpretation, as the secondary legislation introduces significant additional requirements.

It is my intention to continue to develop this guidance, increasing its detail and authority as my Office gains practical experience of applying the Act. It is important that data controllers should be aware that my advice may develop in certain areas in the light, for example, of decisions taken on particular cases or other relevant case law. As such changes become necessary we shall amend the web version. Those familiar with the introductory guidance will notice some areas where the thinking of my Office has already evolved, such as the definitions of personal data and data controller, and the practical application of the conditions for processing in Schedules 2 and 3 of the Act.

As I am required to do, I have sought to interpret the Act in the light of the provisions of the Human Rights Act 1998, which came into force on 2 October 2000. This will need to be kept under review. The full effect of the Human Rights Act on our legal system, and on society as a whole, has yet to be felt. It is, however, clear that the role of information in our society makes it increasingly important to develop respect among data controllers for the private lives of individuals and to ensure good information handling practice. The Human Rights Act, and in particular Articles 8 and 10 of the European Convention on Human Rights provide the legal framework within which interpretation of the Act, and the Data Protection Principles which underpin it, can be developed.

The Act allows two periods of transition so that most of the requirements that it introduced for the first time did not apply to all personal data immediately. However, the first of those periods of transition comes to an end on 24 October 2001 and only a very limited category of personal data will continue to be subject to more limited transitional relief for a further six-year period. This publication retains, for the sake of legal accuracy and completeness, the original detailed guidance relating to transitional exemption provisions that appeared in the introductory guidance. From a practical point of view however, I acknowledge that the

classes of personal data to which these provisions relate, and will continue to relate beyond 24 October 2001, are now relatively small.

I trust that this guidance goes some way towards answering data controllers' most frequently asked questions and that it will be a valuable starting point in helping them to achieve compliance with the Act.

Chapter 1: Introduction

The Data Protection Act 1998 ("the Act") gives effect in the UK law to EC Directive 95/46/EC (the "Directive"). The Act replaces the Data Protection Act 1984 (the "1984 Act") and was brought into force on 1 March 2000. There are, however, two transitional periods, the first of which expires on 24 October 2001 and the second of which expires on 24 October 2007, which provide that the processing of certain personal data does not become fully subject to the Act until these dates. Important subordinate legislation also came into force on or after 1 March 2000 and a full schedule of the relevant Statutory Instruments can be found at the end of this publication. For ease of reference, throughout the text, the full title and number of each Statutory Instrument ("S.I.") is provided.

This publication provides a broad guide to the Act as a whole. Where possible, an indication of the view of the Commissioner as to how certain provisions of the Act should be interpreted has been included and in some cases this may only involve reiterating guidance established under the previous legislation.

The Act uses some familiar and some unfamiliar words and phrases. It is particularly important to review the meaning of the familiar words and phrases as, under the Act, their definitions differ from those used in the 1984 Act. Chapter 2 deals with the definitions used in the Act.

There are eight Data Protection Principles (the "Principles") in the Act. Except to the extent that any data controller is able to claim an exemption from any one or all of them (whether on a transitional or outright basis), all of the Principles apply to all data controllers who must comply with them. The Principles are dealt with in detail in Chapter 3.

The Act gives legal rights to individuals (data subjects) in respect of personal data processed about them by others. These are detailed in Chapter 4.

There are a number of exemptions from various provisions of the Act. Chapter 5 details these. Transitional exemptions and provisions, which may apply in respect of certain processing, where the data controller may not need to comply with all the provisions of the Act immediately, are dealt with in Chapter 6.

The Data Protection Registrar referred to in the 1984 Act became the Data Protection Commissioner by virtue of the Act. With the coming into force of certain provisions of the Freedom of Information Act 2000, the Data Protection Commissioner became the Information Commissioner and is referred to as the "Commissioner" throughout this publication.

The Commissioner's powers and duties are set out in Chapter 7. This Chapter details the Commissioner's duty to carry out assessments which replaces the duty to consider complaints under the 1984 Act.

Chapter 8 deals with the system of notification which replaced the registration scheme and, finally, Chapter 9 details the offences contained in the Act.

The Freedom of Information Act 2000 ("FoIA") makes various amendments to the Act and these amendments are reflected in the text to the extent that they are in force. This publication will be amended to reflect further amendments as they are brought in. Further

information regarding the FoIA can be found on the Commissioner's web site or is available upon request.

This publication does not deal with The Telecommunications (Data Protection and Privacy) Regulations 1999 (S.I. 2093) which the Commissioner is also responsible for enforcing. Separate legal guidance and compliance advice are already available on this legislation on our website.

How to Contact the Commissioner's Office

Information Commissioner
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

To Notify call:	01625 545740
Information Line:	01625 545745
Switchboard:	01625 545700
Fax:	01625 524510
Website:	www.dataprotection.gov.uk
E-mail:	data@dataprotection.gov.uk

Chapter 2: Definitions

2.1 Data (including manual data/relevant filing system)

Definition

Data means information which:-

(a) is being processed by means of equipment operating automatically in response to instructions given for that purpose;

(b) is recorded with the intention that it should be processed by means of such equipment;

(c) is recorded as part (or with the intention that it should form part) of a relevant filing system (i.e. any set of information relating to individuals to the extent that, although not processed as in (a) above, the set is structured either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible); or

(d) does not fall within paragraph (a), (b) or (c) but forms part of an "accessible record". An "accessible record" is defined in section 68 of the Act and can be summarised here as a health record, educational record (local education authority schools and special schools only), local authority housing record or local authority social services record.

It should be noted that data forming part of an accessible record may fall within paragraphs (a), (b), (c) or (d) of the definition of data.

"Processing" is defined separately – see paragraph 2.3 below.

From the above definition it is clear that the Act is concerned not only with automatically processed or processable information but also data falling within the definition of "relevant filing system" as defined in paragraph (c) above and which are referred to throughout this publication as "manual data". Such data may be subject to transitional relief until 2001 or 2007, for details of which see Chapter 6 on Transitional Provisions. Data controllers (see paragraph 2.5 below for definition) will now have to consider whether information that is recorded manually comes within the Act. The inclusion of manual data is an important development.

2.1.1 Which manual data are covered by the Act?

All data controllers are under a duty to comply with the Data Protection Principles in relation to all personal data with respect to which they are the data controller (subject to the various exemptions). Some manual data are now also included within this definition. Non-automated information may be found in a variety of different media e.g. paper files, rollerdex, non-automated microfiches. Data controllers should examine all their non-automated information systems (referred to in this chapter as "manual information") in order to determine how far the Act applies to personal data processed in those systems. To be subject to the Act, the manual information must fall

within the definition of "data" in the Act. As indicated at paragraph 2.1(c) above, data includes information which is recorded as part of a "relevant filing system" or with the intention that it should form part of a "relevant filing system". The term "relevant filing system" means:-

"any set of information relating to individuals to the extent that, although the information is not processed by means of equipment operating automatically in response to instructions given for that purpose, the set is structured, either by reference to individuals or by reference to criteria relating to individuals, in such a way that specific information relating to a particular individual is readily accessible".

It is not wholly clear how this definition translates in practical terms in all conceivable situations. The Commissioner can only give general guidance; the final decision in cases of dispute is a question for the Courts. Whether or not manual information falls within this definition will be a matter of fact in each case. It is not possible for the Commissioner to state categorically whether or not certain types of information or files are caught by the Act although it is recognised that there are certain areas of business where the question of whether manual information falls within the definition will be of particular significance, e.g. personnel files. In deciding whether manual information falls within the definition, data controllers should consider the following:-

- There must be a **set** of information about individuals. The word "set" suggests a grouping together of things by reference to a distinct identifier i.e. a set of information with a common theme or element. Examples might include a set of information on customers or employees. Sets of information about individuals need not necessarily be grouped together in a file or files. They may be grouped together in some other way, for example, by prefix codes, or by attaching an identifying sticker within a file or files. Similarly, the information does not necessarily have to be grouped together in the same drawer of the filing cabinet or the same filing cabinet; nor does it necessarily have to be maintained centrally by an organisation. The set of information might be dispersed over different locations within the organisation, for example, different departments, branch offices, or via home workers.

- The set of information must be structured in such a way that **specific** information about a particular individual is **readily accessible.** What does or does not amount to such specific information will be a matter of fact in each individual case. The Act does not define what is meant by "readily accessible". In deciding whether or not it is readily accessible, a suggested approach is to assume that a set or sets of manual information which are referenced to individuals (or criteria relating to individuals), are caught by the Act if they are, as matter of fact, generally accessible at any time to one or more people within the data controller's organisation in connection with the day to day operation of that organisation.

In practice, data controllers may find that their manual files consist partly of information which forms, or is intended to form, part of a "relevant filing system", and partly of information which does not. **It is essential for data controllers to keep in mind that it is the information and the ease with which it may be located which they should assess rather than whether it is in itself a file or filing**

system. In other words a file is not synonymous with "relevant filing system" Manual information which forms part of clearly highly structured files, for example, card indexes or records, is likely to fall within the definition.

The Commissioner recognises that data controllers may find that there are grey areas in determining whether or not certain manual information is subject to the requirements of the Act. It is suggested that in those cases where data controllers are unsure whether or not manual information comes within the definition of data/"relevant filing system" they should evaluate how accessible the data are by making reasoned judgements. Data controllers should consider whether or not and, if so, the extent to which, a decision not to treat the information as being covered by the Act will prejudice the individual concerned. Where the risk of prejudice is reasonably likely then data controllers would be expected to err on the side of caution and take steps to ensure compliance. Whether the Commissioner decides to enforce any particular case does not affect the rights of individuals to seek redress from the Courts under the Act on the basis of a different or wider interpretation of "relevant filing system".

Where manual information falls within the definition, data controllers may not have to comply with the requirements of the Act in full immediately as transitional relief may apply (see Chapter 6). Where the data controller does not qualify for transitional relief manual data should have been processed in compliance with the Act from 1 March 2000.

2.2 Personal Data

Definition

Personal data are defined in the Act, at section 1(1), as follows:-

"data which relate to a living individual who can be identified:-

- from those data; or

- from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller

and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual".

According to the definition in the Act, therefore, where an individual is capable of being identified from data (as defined in the Act) which relate to that individual, such data are personal data. The definition in the Act is not without difficulty and the Commissioner recognises that, potentially, the definition has a very broad scope. This, in turn, will have a considerable impact on data controllers in terms of compliance with the Data Protection Principles, in particular, the First Data Protection Principle.

It is important not to look at the definition of personal data in isolation as it is the Commissioner's view that for the scope of the definition to be understood properly, it should be considered in the context of the definitions of "data", "data controller" and "data subject" in the Act.

The following questions and answers break down the definition and analyse its component parts. It is important to note that these elements are cumulative:-

2.2.1 What determines whether data relate to an individual?

Potentially, this aspect of the definition could be construed very widely. In the Commissioner's view, whether or not data relate to a particular individual will be a question of fact in each particular case. One element to be taken into account would be whether a data controller can form a connection between the data and the individual.

Data do not have to relate solely to one individual and the same set of data may relate to two or more people and still be personal data about each of them. For example, joint tenants of a property or holders of a joint bank account or even individuals who use the same telephone or e-mail address.

Information may relate to an individual in a business capacity and not just to their private life. Information about the business of a sole trader will amount to personal data as information about the business will be about the sole trader. Information about an individual in a partnership will be personal data if it relates to a specific partner. This will be more likely in a small partnership.

Although the Act refers to individuals and not other legal entities such as limited companies, there will be situations where information about a limited company or other legal entity amounts to personal data because it relates to a specific individual, for example, the performance of a department which is under the control of a specific individual. Information relating solely to the legal entity will not be personal data.

2.2.2 Does the Act only relate to living individuals?

Yes. The Act is only concerned with living individuals and so if the subject of the information is dead, then the information cannot be personal data.

2.2.3 The individual must be capable of being identified. How does the Commissioner approach this issue?

The individual must be capable of being identified from data in the possession of the data controller, or from those data and other information in the possession of, or likely to come into the possession of, the data controller.

The Commissioner recognises that an individual may be "identified" without necessarily knowing the name and address of that particular individual.

The Commissioner's view is that it is sufficient if the data are capable of being processed by the data controller to enable the data controller to distinguish the data subject from any other individual. This would be the case if a data subject could be treated differently from other individuals.

For example:

The capture of an image of an individual by a CCTV camera may be done in such a way that distinguishable features of that individual are processed and identified from the captured images. However, in order to be able to identify that individual it will be necessary to match the image to a photograph, a physical description, or a physical person. If this can be done the CCTV footage will be personal data.

In the context of the Internet, many e-mail addresses are personal data where the e-mail address clearly identifies a particular individual. The Commissioner is Elizabeth France. The e-mail address elizabethfrance@dataprotection.gov.uk is thus personal data about the Commissioner**.**

In the majority of cases the ability to "identify" an individual will be achieved by knowing the name and address of an individual or by the data controller being in possession of some other information. The definition also allows for an individual to be identified from data together with information **"likely to come into the possession"** of the data controller.

It will be for a data controller to satisfy himself whether it is likely that such information will come into his possession to render data personal data. This will depend largely on the nature of the processing undertaken by a data controller.

This issue is clearly relevant in the context of personal data which a data controller wishes to anonymise, as to which, see 2.2.5 below

For example:

If the information about a particular web user is built up over a period of time, perhaps through the use of tracking technology, with the intention that it may later be linked to a name and address, that information is personal data. Information may be compiled about a particular web user, but there might not be any intention of linking it to a name and address or e-mail address. There might merely be an intention to target that particular user with advertising, or to offer discounts when they re-visit a particular web site, on the basis of the profile built up, without any ability to locate that user in the physical world. The Commissioner takes the view that such information is, nevertheless, personal data. In the context of the on-line world the information that identifies an individual is that which uniquely locates him in that world, by distinguishing him from others.

Another way in which information may come into the possession of a data controller is in relation to an image captured on CCTV. This might produce an image which is not of a distinguishable individual, but the actual identity of that individual may become apparent from other information likely to come into the possession of the data controller.

2.2.4 What is meant by the expression "possession" in this context?

The concept of possession is very wide. In the Commissioner's view possession does not necessarily mean that the identifying data are in the physical control of the data controller, or likely to come under his physical control.

For Example:

> A data controller enters into a contract with a data processor for the processing of personal data. The arrangement is that the data processor may receive some of the identifying data from a third party and some from the data controller. The data are processed in accordance with the terms of the contract. The data controller determines the purposes for which and the manner in which the personal data are to be processed by the data processor but may not have sight of all or any of the information which identifies a living individual. The data controller would, however, be deemed to be in possession of those data. The data controller could not argue in such a situation that the identifying data are not in his "possession" and absolve himself of his responsibilities as data controller.

2.2.5 Can personal data be anonymised?

The issue of information in the possession of, or likely to come into the possession of, a data controller has an impact on a data controller who seeks to anonymise the personal data he is processing by stripping those data of all personal identifiers.

In anonymising personal data the data controller will be processing such data and, in respect of such processing, will still need to comply with the provisions of the Act.

The Commissioner recognises that the aim of anonymisation is to provide better data protection. However, true anonymisation may be difficult to achieve in practice. Nevertheless, the Commissioner would encourage that, where possible, information relating to a data subject, which is not necessary for the particular processing being undertaken, should be stripped from the personal data being processed. This may not amount to anonymisation but is in line with the requirements of the Data Protection Principles.

The Commissioner considers anonymisation of personal data difficult to achieve because the data controller may retain the original data set from which the personal identifiers have been stripped to create the "anonymised" data. The fact that the data controller is in possession of this data set which, if linked to the data which have been stripped of all personal identifiers, will enable a living individual to be identified, means that all the data, including the data stripped of personal identifiers, remain personal data in the hands of the data controller and cannot be said to have been anonymised. The fact that the data controller may have no intention of linking these two data sets is immaterial.

A data controller who destroys the original data set retaining only the information which has been stripped of all personal identifiers and who assesses that it is not likely that information will come into his possession to enable him to reconstitute the data, ceases to be a data controller in respect of the retained data.

Whether or not data which have been stripped of all personal identifiers are personal data in the hands of a person to whom they are disclosed, will depend upon that person being in possession of, or likely to come into the possession of, other information which would enable that person to identify a living individual.

It should be noted that the **disclosure** of personal data by a data controller amounts to processing under the Act.

For example:

> The obtaining of clinical information linked to a National Health Service number by a person having access to the National Health Service Central Register will amount to processing of personal data by that person because that person will have access to information enabling him to identify the individuals concerned.

It will be incumbent upon anyone processing data to take such technical and organisational measures as are necessary to ensure that the data cannot be reconstituted to become personal data and to be prepared to justify any decision they make with regard to the processing of the data.

For example:

> In the case of data collected by the Office of National Statistics, where there is a disclosure of samples of anonymised data, it is conceivable that a combination of information in a particular geographic area may be unique to an individual or family who could therefore be identifiable from that information. In recognition of this fact, disclosures of information are done in such a way that any obvious identifiers are removed and the data presented so as to avoid particular individuals being distinguished.

If data have been stripped of all personal identifiers such that the data controller is no longer able to single out an individual and treat that individual differently, the data cease to be personal data. Whether this has been achieved may be open to challenge. Data controllers may therefore be required to justify the grounds for their view that the data are no longer personal data.

When a subject access request is received, a data controller must be able to identify the data relating to the data subject making the request, to enable him to provide information specific to that data subject. In making a subject access request, a data subject might provide the data controller with sufficient information to enable his data to be distinguished from data relating to other individuals, in a situation where the data controller would not otherwise be able to do so from the information in his possession, which he may have stripped of all personal identifiers. In this case the data relating to the individual making the request become personal data but the information provided by the data subject does not render the other data being held personal data unless the data controller believes that it is likely that the information will come into his possession to render the other data personal data.

If there are any doubts as to whether data are personal data the Commissioner's advice would be to treat the data as personal data, having particular regard to whether those

data are sensitive personal data. In respect of such data, if a subject access request is received and the data controller cannot satisfy himself as to the identity of the person making the subject access request, or as to his ability to locate the information to which the subject access request relates because the data have been stripped of identifiers, then the data controller would not be obliged to comply with the subject access request, advising the data subject accordingly.

2.2.6 What about expressions of opinion or intention?

The definition of personal data contained in the Act now expressly includes any indication of the intentions of the data controller or any other person in respect of an individual. This aspect of the definition was not included in the definition of "personal data" in the 1984 Act. The consequence of this may mean, for example, that an employer who processes appraisals of employees would have to disclose not only his opinions of the employees but also any intention to offer or decline promotion on the basis of those opinions subject to any exemption available at any particular time.

2.3 Processing

Definition

Processing, in relation to information or data, means obtaining, recording or holding the information or data (which includes, in relation to personal data, obtaining or recording the information to be contained in the data) or carrying out any operation or set of operations on the information or data, including –

- organisation, adaptation or alteration of the information or data;
- retrieval, consultation or use of the information or data (which, in relation to personal data, includes using the information contained in the data);
- disclosure of the information or data (which, in relation to personal data, includes disclosing the information contained in the data) by transmission, dissemination or otherwise making available, or
- alignment, combination, blocking, erasure or destruction of the information or data.

This definition incorporates, amongst other things, the concepts of "obtaining", "holding" and "disclosing". These aspects of the definition were not included in the definition of processing in the 1984 Act. The definition in the Act is a compendious definition and it is difficult to envisage any action involving data which does not amount to processing within this definition.

2.4 Data Subject

Definition

Data subject means "an individual who is the subject of personal data". A data subject must be a living individual. Organisations, such as companies and other corporate and unincorporated bodies of persons cannot, therefore, be data subjects.

A data subject need not be a United Kingdom national or resident. Provided that the data controller is subject to the Act, rights with regard to personal data are available to every data subject, whatever his nationality or residence.

2.5 Data Controller

Definition

Data controller means:-

"… a person who (either alone or jointly or in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be, processed".

It is important to establish whether or not someone is a data controller because it is data controllers who are required to comply with the Data Protection Principles. Section 4(4) of the Act provides that:-

"… it shall be the duty of a data controller to comply with the Data Protection Principles in relation to all personal data with respect to which he is the data controller".

A data controller must be a "person" i.e. a legal person. This term comprises not only individuals but also organisations such as companies and other corporate and unincorporated bodies of persons.

According to the definition in the Act, a data controller or data controllers, must decide the **purposes** for which personal data are, or will be, processed **and the way** in which personal data are, or will be, processed. The Commissioner's view is that the determination of the purposes for which personal data are to be processed is paramount in deciding whether or not a person is a data controller and that when a person determines the purposes for which personal data are to be processed, a decision as to the manner in which those data are to be processed is often inherent in that decision.

The determination of the purposes for which, and the manner in which, any personal data are, or are to be, processed does not need to be exclusive to one data controller. Such determination may be shared with others. It may be shared jointly or in common. "Jointly" covers the situation where the determination is exercised by acting together equally. "Determination in common" is where data controllers share a pool of personal data, each processing independently of the other.

It is important to appreciate the difference between the definition of a data user under the 1984 Act and that of data controller under the Act as it is quite possible that persons who were not data users under the 1984 Act in respect of particular processing activities will be data controllers under the Act. It is also possible that persons who carried on computer bureaux, as defined in the 1984 Act, and who were not also data

users may find that they fall within the definition of data controller in the Act rather than the definition of "data processor".

An illustration of the difference between the concepts of data user and data controller is in the context of credit reference agency data. The credit reference agency was a data user under the 1984 Act and is a data controller under the Act. The agency customers/subscribers who had access to credit reference agency data by way of a remote terminal, on a read-only basis, were not considered to be data users under the 1984 Act **by virtue of such access**. This was because they had no control of the content of the agency data and therefore fell outside the definition of data user. Such agency customers/subscribers may, however, have been data users in respect of other processing activities which they undertook.

Under the Act, the Commissioner's view is that agency customers/subscribers who access agency data to inform decisions regarding individuals are data controllers. This is because they decide why and how they use personal data. Remember that the concept of "processing" is very wide. The word can be used to encompass all manner of activities/operations that a particular data controller may want to perform on the personal data in question.

In respect of the credit reference agency, amongst other things, it obtains, records, holds, organises, adapts, alters and discloses personal data. The agency customer/subscriber consults, obtains or retrieves personal data disclosed to it by the agency before using such data, for example, to inform a decision on whether to supply a customer. It is the ability to decide these things that makes them data controllers to the extent of the processing undertaken by them.

There may be other examples of people, businesses and organisations who were not subject to the 1984 Act but who are subject to the Act because of the fact that they are now data controllers.

2.6 Data Processor

Definition

"Data processor, in relation to personal data, means any person (other than an employee of the data controller) who processes the data on behalf of the data controller."

The Act introduces specific obligations upon data controllers when the processing of personal data is carried out on their behalf by data processors (see Chapter 3). The data controller retains full responsibility for the actions of the data processor and so the definition of data controller has an impact on this context.

2.7 Recipient

Definition (s.70(1))

Recipient, in relation to personal data, means any person to whom the data are disclosed, including any person (such as an employee or agent of the data controller, a

data processor or an employee or agent of the data processor) to whom they are disclosed in the course of processing the data for the data controller.

The term does not include any person to whom disclosure is or may be made as a result of, or with a view to, a particular inquiry by or on behalf of that person made in the exercise of any power conferred by law. As a consequence, a data subject may not be provided with such information in accordance with section 7(1)(b)(iii).

2.8 Third Party

Definition (s70 (1))

"Third party, in relation to personal data, means any person other than –

- the data subject,
- the data controller, or
- any data processor or other person authorised to process data for the data controller or processor."

The expression third party does not include employees or agents of the data controller or data processor, which persons are for the purpose of this expression to be interpreted as being part of the data controller or processor. As such, this expression is distinguishable from "recipient", which effectively separates employees/agents of the data controller/processor from the data controller/processor itself.

Chapter 3: The Data Protection Principles

Introduction

There are eight Data Protection Principles ("the Principles") in the Act, sometimes referred to as the Principles of "good information handling" which data controllers are required to comply with. Except to the extent that any data controller is able to claim an exemption from any of the Principles (whether on a transitional or outright basis) the Principles apply to all personal data processed by data controllers. Data controllers must comply with them, irrespective of whether they are required to notify and whether or not they have actually notified.

The Principles are set out in Part I of Schedule 1 of the Act. Part II of Schedule 1 comprises the interpretation provisions which expand upon the First, Second, Fourth, Sixth, Seventh and Eighth Principles.

Schedule 2 of the Act provides conditions for the processing of any personal data relevant for the purposes of the First Principle, whilst Schedule 3 provides conditions for the processing of sensitive personal data relevant for the purposes of the First Principle over and above those set out in Schedule 2. Additional Schedule 3 conditions are set out in The Data Protection (Processing of Sensitive Personal Data) Order 2000 (S.I. No. 417)(the "Sensitive Data Order").

Schedule 4 of the Act consists of cases where the Eighth Principle (prohibiting the transfer of personal data outside the European Economic Area) does not apply.

When considering the Principles it is worth remembering the wide scope of the definition of "processing" in the Act and, in particular, the fact that the term includes "obtaining" and "disclosure" of the data.

3.1 First Principle

"Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

- at least one of the conditions in Schedule 2 is met; and
- in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met."

This introduces the requirement that, as a requisite of fair and lawful processing, personal data shall not be processed unless at least one of the conditions in Schedule 2 of the Act ("the conditions for processing") is met and, in the case of the processing of sensitive personal data (see paragraph 3.1.2 below) at least one of the conditions in Schedule 3 of the Act ("the conditions for processing sensitive data") is also met.

Meeting a Schedule 2 and Schedule 3 condition will not, on its own, guarantee that processing is fair and lawful. **The general requirement that data be processed fairly and lawfully must be satisfied in addition to meeting the conditions.**

3.1.1 Conditions for Processing (Schedule 2 of the Act)

At least one of the following conditions must be met in the case of all processing of personal data (except where a relevant exemption applies):-

- The data subject has given his consent to the processing (see paragraph 3.1.5 below).

- The processing is **necessary –**

  (a) for the performance of a contract to which the data subject is a party; or

  (b) for the taking of steps at the request of the data subject with a view to entering into a contract.

- The processing is **necessary** to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

- The processing is **necessary** in order to protect the vital interests of the data subject.

The Commissioner considers that reliance on this condition may only be claimed where the processing is necessary for matters of life and death, for example, the disclosure of a data subject's medical history to a hospital casualty department treating the data subject after a serious road accident.

- The processing is **necessary** –

  (a) for the administration of justice;

  (b) for the exercise of any functions conferred by or under any enactment;

  (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department;

  (d) for the exercise of any other functions of a public nature exercised in the public interest.

- The processing is **necessary** for the purposes of legitimate interests pursued by the data controller or by the third party or parties to whom the data are disclosed, **except** where the processing is unwarranted in any particular case because of prejudice to the rights and freedoms or legitimate interests of the data subject.

The Commissioner takes a wide view of the legitimate interests condition and recommends that two tests be applied to establish whether this condition may be appropriate in any particular case. The first is the establishment of the legitimacy of the interests pursued by the data controller or the third party to whom the data are to be disclosed and the second is whether the processing is unwarranted in any particular

case by reason of prejudice to the rights and freedoms or legitimate interests of the data subject whose interests override those of the data controller. The fact that the processing of the personal data may prejudice a particular data subject does not necessarily render the whole processing operation prejudicial to all the data subjects.

The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied. No order has been made to date.

3.1.2 Sensitive Personal Data

The Act defines categories of sensitive personal data, namely, personal data consisting of information as to:-

(a) the racial or ethnic origin of the data subject;

(b) his political opinions;

(c) his religious beliefs or other beliefs of a similar nature;

(d) whether he is a member of a trade union (within the meaning of the Trade Union and Labour Relations (Consolidation) Act 1992);

(e) his physical or mental health or condition;

(f) his sexual life;

(g) the commission or alleged commission by him of any offence; or

(h) any proceedings for any offence committed or alleged to have been committed by him, the disposal of such proceedings or the sentence of any court in such proceedings.

3.1.3 Conditions for Processing Sensitive Data (Schedule 3 of the Act)

At least one of the following conditions must be satisfied, in addition to at least one of the conditions for processing in Schedule 2 (which apply to the processing of all personal data), before processing of sensitive personal data can comply with the First Principle:-

- The data subject has given his **explicit** consent to the processing of the personal data (see paragraph 3.1.5 below).

- The processing is **necessary** for the purposes of exercising or performing any right or obligation which is conferred or imposed by law on the data controller in connection with employment.

The Secretary of State may specify cases by order where this condition is either excluded altogether or only satisfied upon the compliance with further conditions. No order has been made to date to this effect.

- The processing is **necessary** –

(a) in order to protect the vital interests of the data subject or another person, in a case where –

(i) consent cannot be given by or on behalf of the data subject, or

(ii) the data controller cannot reasonably be expected to obtain the consent of the data subject, or

(b) in order to protect the vital interests of another person, in a case where consent by or on behalf of the data subject has been unreasonably withheld.

- The processing –

(a) is carried out in the course of its legitimate activities by any body or association which exists for political, philosophical, religious or trade union purposes **and** which is not established or conducted for profit;

(b) is carried out with appropriate safeguards for the rights and freedoms of data subjects;

(c) relates only to individuals who are either members of the body or association or who have regular contact with it in connection with its purposes; and

(d) does not involve disclosure of the personal data to a third party without the consent of the data subject.

Each of these provisions needs to be satisfied in order to fall within this condition. However, the Commissioner is of the view that data controllers who rely upon this condition as a basis for processing may make subsequent non-consensual disclosures of sensitive personal data only if there is a basis for doing so under one of the other Schedule 3 conditions.

- The information contained in the personal data has been made public as a result of steps deliberately taken by the data subject.

- The processing –

(a) is **necessary** for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is **necessary** for the purpose of obtaining legal advice, or

(c) is otherwise **necessary** for the purposes of establishing, exercising or defending legal rights.

The Commissioner's view is that (c) above is of limited scope and data controllers should adopt a narrow interpretation and rely upon another Schedule 3 condition if

there is any doubt as to whether it applies. In particular, it should not be used to construct a legal right where none exists.

To illustrate this point, in a common scenario where negotiations are taking place between an individual and an insurance company with a view to entering into a contract of insurance, various disclosures have to be made which may include sensitive personal data about a third party to enable the insurer to assess the risk and calculate the premium. Examples could be a group insurance policy for holiday insurance where medical details of individuals who are not party to the negotiations are disclosed, or car insurance where conviction details of named drivers would have to be revealed by the proposer. No contract exists at this stage and the insurance company may decide not to accept the risk and enter into a contract of insurance.

Reliance by the insurance company, as data controller, upon paragraph (c) of this condition as a basis for processing the sensitive personal data of a third party would not be acceptable to the Commissioner prior to the existence of the contract and the data controller would have to rely upon another condition for processing sensitive data in Schedule 3 or under the Sensitive Data Order unless, on a case by case analysis, the data controller has reasonable grounds for believing that an agency relationship exists between the individual with whom he is dealing and the data subject. (i.e. a relationship exists whereby one party, the "agent," has the authority or capacity to create legal relations between a person acting as "principal" and a third party).

- The processing is **necessary** –

  (a) for the administration of justice;

  (b) for the exercise of any functions conferred by or under any enactment; or

  (c) for the exercise of any functions of the Crown, a Minister of the Crown or a government department.

The Secretary of State may by order specify cases where this condition is either excluded altogether or only satisfied if further specified conditions are met. No order to this effect has been made to date.

- The processing is **necessary** for medical purposes (including the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services) and is undertaken by –

  (a) a health professional (as defined in section 69 of the Act); or

  (b) a person who owes a duty of confidentiality which is equivalent to that which would arise if that person were a health professional.

- The processing –

(a) is of sensitive personal data consisting of information as to racial or ethnic origin;

(b) is **necessary** for the purpose of identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons of different racial or ethnic origins, with a view to enabling such equality to be promoted or maintained; and

(c) is carried out with appropriate safeguards for the rights and freedoms of data subjects. The Secretary of State may specify by order circumstances in which such processing is, or is not, to be taken as carried out with appropriate safeguards for the rights and freedoms of data subjects. No order to this effect has been made to date.

- The personal data are processed in circumstances specified by order made by the Secretary of State. Currently the only such order is the Sensitive Data Order. This includes detailed provisions for:

(1) processing that is in the substantial public interest and is necessary for the prevention or detection of any unlawful act and must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice those purposes; or

(2) processing that is in the substantial public interest and is necessary for the discharge of any function which is designed for protecting members of the public against;

- dishonesty, malpractice, or other seriously improper conduct by, or the unfitness of incompetence of, any person, or
- mismanagement in the administration of, or failure in services provided by, any body or association, and
- must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the discharge of that function; or

(3) the disclosure of personal data that is:-

(i) in the public interest and

(ii) is in connection with:-

- the commission by any person of any unlawful act (whether alleged or established), or
- dishonesty, malpractice, or other seriously improper conduct by, or the unfitness or incompetence of, any person (whether alleged or established), or

- mismanagement in the administration of, or failures in the services provided by, any body or association (whether alleged or established)

(iii) is for the special purposes as defined in section 3 of the Act; and

(iv) is made with a view to the publication of those data by any person and the data controller reasonably believes that such publication would be in the public interest.

(4) processing that is:-

(i) in the substantial public interest;

(ii) is necessary for the discharge of any function which is designed for the provision of confidential counselling, advice, support or any other service; and

(iii) is carried out without the explicit consent of the data subject because the processing:

- is necessary in a case where consent cannot be given by the data subject, or

- is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent, or

- must necessarily be carried out without the explicit consent of the data subject being sought so as not to prejudice the provision of that counselling, support, advice or other service.

(5) processing that:

(i) is necessary for the purpose of:-

- carrying on an insurance business (as defined); or

- making determinations in connection with eligibility for, and benefits payable under, an occupational pension scheme (as defined),

(ii) is of sensitive personal data relating to the physical or mental health or condition of the data subject who is the parent, grandparent, great grandparent or sibling of the insured person or member of the scheme;

(iii) is necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject and the data controller is not aware of the data subject

withholding his consent; and

(iv) does not support measures or decisions with respect to the data subject.

(6) processing of sensitive personal data in relation to any particular data subject that are subject to processing already under way immediately before 1 March 2000 and where the processing is necessary for carrying on insurance business or establishing or administering an occupational pension scheme, where such processing is either;

(i) necessary in a case where the data controller cannot reasonably be expected to obtain the explicit consent of the data subject and the data subject has not informed the data controller that he does not so consent; or

(ii) it must necessarily be carried out even without the data subject's explicit consent so as not to prejudice those purposes.

For an explanation of "processing already under way" and transitional relief, see Chapter 6.

(7) processing of sensitive personal data consisting of information as to religious beliefs (or other beliefs of similar nature) or physical or mental health or condition where:-

(i) the processing is necessary for identifying or keeping under review the existence or absence of equality of opportunity or treatment between persons with a view to enabling such equality to be promoted or maintained; and

(ii) it does not support measures or decisions relating to a data subject otherwise than with the data subject's explicit consent; and

(iii) it does not cause nor is likely to cause substantial damage or distress to the data subject or any other person.

The data subject has the right to prevent such processing by notice in writing to the data controller.

(8) processing of personal data consisting of information as to the data subject's political opinions that is carried out by certain people or political organisations where it does not cause nor is likely to cause substantial damage or substantial distress to the data subject or any other person.

Again, the data subject has the right to prevent such processing by notice to the data controller.

(9) processing that

(i) is in the substantial public interest;

(ii) is necessary for research purposes (as defined in section 33 of the Act);

(iii) does not support measures or decisions with respect to any particular data subject otherwise than with the explicit consent of the data subject;

(iv) does not cause nor is likely to cause, substantial damage or substantial distress to the data subject or any other person.

(10) processing that is necessary for the exercise of any functions conferred on a constable by any rule of law.

It is to be noted that The Sensitive Data Order provides that if the processing of sensitive personal data is necessary for identifying or keeping under review the existence or absence of equality of opportunity, or treatment between persons holding different beliefs or different states of physical or mental health or condition with a view to maintaining or promoting such equality or opportunity, or consists of the processing of information as to the data subject's political views conducted by any person or organisation as defined in The Sensitive Data Order, the data subject has the right to require the data controller to cease such processing within a reasonable period.

- The Commissioner is aware of certain factual circumstances where data controllers processing sensitive personal data experience difficulty in satisfying a Schedule 3 condition. In such circumstances, when considering the exercise of her discretion whether to take enforcement action, the Commissioner would look carefully at the processing, taking into account any damage and distress caused to the data subject as a result of that processing.

  Given that the Secretary of State has the power to make further orders, data controllers who find genuine difficulty in satisfying a Schedule 3 condition may make representations to the Lord Chancellor's Department with a view to such processing forming the basis of a further order.

3.1.4 Lawfulness

The Act does not provide any guidance on the meaning of "lawful". The natural meaning of unlawful has been broadly described by the Courts as "something which is contrary to some law or enactment or is done without lawful justification or excuse". (R v R [1991] 4All ER 481). The term applies equally to the public and private sector and to breaches of both statute and common law, whether criminal or civil. An example of information unlawfully obtained might be information, which is obtained as a result of a breach of confidence or in breach of an enforceable contractual agreement. Since 2 October 2000 it applies to a breach of the Human Rights Act 1998 by a data controller bound by that Act.

This means that a data controller must comply with all relevant rules of law whether derived from statute or common law, relating to the purpose and ways in which the data controller processes personal data.

There are certain areas of law concerning the use of information and the relations of data controllers with individuals, which have particular relevance where breaches of the first and Second Principles are being considered. These are:-

(a) Confidentiality arising from the relationship of the data controller with the data subject.

(b) The ultra vires rule and the rule relating to the excess of delegated powers, under which the data controller may only act within the limits of its legal powers.

(c) Legitimate expectation, that is, the expectation of the individual as to how the data controller will use the information relating to him.

(d) Article 8 of the European Convention on Human Rights (the right to respect for private and family life, home and correspondence).

These areas, particularly (b) to (d) above, are especially important in the case of data controllers in the public sector, who, for example, often have extensive statutory powers enabling them to require information from individuals.

There are circumstances where an obligation of confidence arises between a data controller and an individual about whom information is recorded, for example, in relation to medical or banking information. The effect of an obligation of confidence is that a data controller is restricted from using the information for a purpose other than that for which it was provided or disclosing it without the individual's permission. It would be unlawful for a data controller to do this unless there was some overriding reason in the public interest for this to happen. Where such personal data are processed for a purpose other than that for which the information was provided, the processing is likely to be unlawful processing.

Many public bodies, for example, government and statutory organisations, deal with personal data in order to carry out specific functions. In doing so they must act within the limits of their powers. Such powers may be set out in statute or be defined in a scheme of executive powers. Such bodies should be aware of the extent of their powers, in particular any specific restrictions on the use or disclosure of data. Where personal data are processed outside those powers then the processing may be unlawful.

Where a public body obtains information of a confidential nature in order to carry out its statutory functions then processes that information for other purposes, there is likely to be a breach of the obligation of confidence to that individual, unless there is a good reason or some legal justification for using the information in that way.

Research carried out by the Commissioner indicates that individuals have a high level of trust in the manner in which their information will be held by public bodies and believe that it will not be passed onto anyone else, or used for any but the most limited purposes apart from the purpose for which the information has been given.

An individual's legitimate expectation as to how the information given to a public body will be used will, therefore, also be relevant in considering whether there has been a breach of the First Principle.

3.1.5 Consent

One of the conditions for processing is that the data subject has given his consent to the processing.

The Commissioner's view is that consent is not particularly easy to achieve and that data controllers should consider other conditions in Schedule 2 (and Schedule 3 if processing sensitive personal data) before looking at consent,. No condition carries greater weight than any other. All the conditions provide an equally valid basis for processing. Merely because consent is the first condition to appear in both Schedules 2 and 3,does not mean that data controllers should consider consent first.

Consent is not defined in the Act. The existence or validity of consent will need to be assessed in the light of the facts. To assist in understanding what may or may not amount to consent in any particular case it is helpful to refer back to the Directive. This defines "the data subject's consent" as:-

"…any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed".

The fact that the data subject must "signify" his agreement means that there must be some active communication between the parties. A data subject may "signify" agreement other than in writing. Data controllers cannot infer consent from non-response to a communication, for example from a customer's failure to return or respond to a leaflet.

The adequacy of any consent or purported consent must be evaluated. For example, consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.

Where a data subject does not signify his agreement to personal data relating to him being processed, but is given an opportunity to object to such processing, although this does not amount to consent for the purposes of the Act, it **may** provide the data controller with the basis to rely upon another Schedule 2 condition, for example, the legitimate interests condition, provided that the data subject is given the right to object before the data are obtained.

Consent must be appropriate to the particular circumstances. For example, if the processing is intended to continue after the end of a trading relationship then the consent should cover those circumstances. However, it must be recognised that even when consent has been given it will not necessarily endure forever. While in most cases consent will endure for as long as the processing to which it relates continues, data controllers should recognise that, depending upon the nature of the consent given and the circumstances of the processing, the individual may be able to withdraw consent.

There is a distinction in the Act between the nature of the consent required to satisfy the condition for processing and that which is required in the case of the condition for processing sensitive data. The consent must be "explicit" in the case of sensitive data. The use of the word "explicit" and the fact that the condition requires explicit consent **"to the processing of the personal data"** suggests that the consent of the data subject should be absolutely clear. In appropriate cases it should cover the specific detail of the processing, the particular type of data to be processed (or even the specific information), the purposes of the processing and any special aspects of the processing which may affect the individual, for example, disclosures which may be made of the data.

3.1.6 In what circumstances is processing necessary?

The majority of the Schedule 2 and 3 conditions stipulate that the processing must be "necessary" for the purpose set out in that particular condition. The requirement is an important safeguard for the rights of data subjects.

The Commissioner takes the view that data controllers will need to consider objectively whether:

- the purposes for which the data are being processed are valid,
- such purposes can only be achieved by the processing of personal data and,
- the processing is proportionate to the aim pursued.

3.1.7 Fairness of processing

As well as requiring data controllers to ensure that they have at least one legitimate basis for processing personal data, the First Principle also requires data controllers to ensure that such processing is fair. The Act assists with the interpretation of the fairness requirement of the First Principle in paragraphs 1 to 4 of Part II of Schedule 1 (the "fair processing requirements").

When considering the fair processing requirements it is worth remembering the wide scope of the definition of processing in the Act which now includes "obtaining" information or data.

It is important to note that compliance with the fair processing requirements will not of itself ensure fair processing.

The Commissioner takes the view that in assessing fairness, the first and paramount consideration must be given to the consequences of the processing to the interests of the data subject. This view was supported by the Data Protection Tribunal in the context of the 1984 Act in the cases of CCN Systems Limited and CCN Credit Systems Limited .v. The Data Protection Registrar [Case DA/90 25/49/9] and Infolink v The Data Protection Registrar [Case DA/90 25/49/9]. The Commissioner will also look at the purposes and nature of the processing in assessing fairness.

Even though a data controller may be able to show that information was obtained and personal data processed fairly and lawfully in general and on most occasions, if it has

been obtained unfairly in relation to one individual there will have been a contravention of the First Principle.

Automated processing can be unfair either where the program is itself operating correctly, but results in the unfair use of data, or where a program is of poor quality and contains errors which mean that it does not operate as the data controller intended.

Compliance with the fair processing requirements of the Act provides an opportunity for data controllers to obtain consent (as to which, see above) but such compliance will not, in itself, ensure that any purported consent is both "specific" and "informed".

3.1.7.1 The fair processing requirements (Schedule 1, Part II, paragraphs 1 to 4) - Paragraph 1

Paragraph 1 provides that in deciding whether or not processing is fair, the way in which personal data are obtained will be considered.

This will include particular reference to whether any person from whom the personal data are obtained is deceived or misled as to the purpose or purposes for which the personal data are to be processed. As has been explained previously, this may also have a bearing on the validity of any consent given by the data subject to the processing, which in turn may remove the basis for processing which was being relied upon by the data controller.

Notwithstanding the fact that a data subject may be authorised or required to supply information by virtue of any enactment, the data controller still has to comply with the provisions of paragraph 2 of Part II of Schedule I (referred to in 3.1.7.3 below) unless the data controller can legitimately claim exemption from compliance with these provisions.

3.1.7.2 Paragraphs 2 and 3 – Information to be provided to data subjects

Paragraphs 2 and 3 provide that personal data are not to be treated as processed fairly unless the requirements set out in paragraphs 3.1.7.3 and 3.1.7.4 below are observed, subject to certain exceptions (as set out in paragraph 3.1.7.5 below). Again, it should be noted that observance of these requirements will not ensure fair processing where there are other factors present which would render the processing unfair. There is a general duty of fairness, which consists in part of the fair processing requirements of the Act.

It should be noted that certain processing of personal data may be exempt from the requirement to provide this information and these exemptions are dealt with in Chapter 5.

3.1.7.3 Information to be provided to data subjects – data obtained from data subjects

When data are obtained from data subjects the data controller must ensure, so far as practicable, that the data subjects have, are provided with, or have made readily available to them, the following information (referred to as the "fair processing information"):-

(a) the identity of the data controller,

(b) if the data controller has nominated a representative for the purposes of the Act, the identity of that representative,

(c) the purpose or purposes for which the data are intended to be processed, and

(d) any further information which is necessary, taking into account the specific circumstances in which the data are or are to be processed, to enable processing in respect of the data subject to be fair.

In deciding whether, and if so, what, further information is "necessary" to satisfy (d) above, data controllers should consider what processing of personal data they will be carrying out once the data have been obtained and consider whether or not data subjects are likely to understand the following:-

(a) the purposes for which their personal data are going to be processed;

(b) the likely consequences of such processing such that the data subject is able to make a judgement as to the nature and extent of the processing; and

(c) whether particular disclosures can reasonably be envisaged.

It would be expected that the more unforeseen the consequences of processing the more likely it is that the data controller will be expected to provide further information. This aspect also has a bearing on the question of what amounts to consent (see specific consideration of this issue at paragraph 3.1.5 above); in the same way that consent must be "informed", so data subjects themselves must be fully aware of the ways in which their personal data may be processed in order for that processing to be considered fair.

In the context of the 1984 Act, the Data Protection Tribunal has supported the Commissioner's view that personal information will not be fairly obtained unless the individual has been informed of the non-obvious purpose or purposes for which it is required, before the information is obtained. (Innovations (Mail Order) Limited v The Data Protection Registrar (September 1993)).

Where an individual effectively has no choice other than to use the service of a particular data controller, for example, where an individual attends an NHS appointment, (subject to any legitimate exemption applying to such processing) the data controller should give individuals the opportunity to limit the extent to which their data may be used and disclosed beyond the primary purpose for which it was supplied.

Where the data controller already holds information obtained for a specific purpose, it can only be used for a different purpose that would not have been envisaged by the data subject at the time of the collection of the information if the data controller has the consent of the data subject.

A data controller cannot infer consent from a lack of response from the data subject. If data have already been collected and another purpose is subsequently envisaged that would not have been obvious to the data subject, again, consent must be obtained before the data can be used for the new purpose.

3.1.7.4 Information to be provided to data subjects – data obtained other than from data subjects

The fair processing information (see paragraph 3.1.7.3 above) should also be provided to data subjects (within the timescale set out in paragraph 3.1.7.7 below) in cases where the data have been obtained from someone other than the data subject, unless one of the exceptions in paragraph 3.1.7.5 below applies.

The data controller must also always be fair to the person from whom the information was obtained. The information might be about an individual different from the person from whom it was obtained. In some circumstances the concept of fairness may require the data controller to give some thought to the individual to whom the information relates as well as the person from whom it is obtained. The fairness of the obtaining has to be judged in each case in relation to a particular piece of information, in relation to the particular individual and taking into account all the circumstances. If different pieces of information are obtained separately, each must be fairly obtained.

3.1.7.5 Exceptions available to data controllers

The following exceptions from the provision of the fair processing information can only be relied upon by data controllers where they have obtained personal data from someone other than the data subject. It should be stressed that the ability to rely on any exception does not absolve the data controller from the overriding duty to process personal data fairly.

The exceptions referred to are:-

(a) where providing the fair processing information would involve a disproportionate effort (see paragraph 3.1.7.6 below), or

(b) where it is necessary for the data controller to record the information to be contained in the data, or to disclose the data, to comply with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

The Secretary of State has prescribed further conditions, by way of "appropriate safeguards", which must also be met for the exception to be

available. These are contained in the Data Protection (Conditions Under Paragraph 3 of Part II of Schedule I) Order 2000 ("S.I. No 185").

In both (a) and (b) above S.I. No 185 provides that any data controller claiming the benefit of the disapplication of the requirement to provide the fair processing information must still provide this information to any individual who requests it.

If the data controller does not have sufficient information about the individual making the request to readily determine whether he is processing information about that person because of a lack of identifying information, that data controller must write to the individual explaining the position.

Where a data controller relies upon the disproportionate effort ground in (a) above, the data controller must keep a record of the reasons why he believes the disapplication of the fair processing requirements is necessary.

3.1.7.6 What is disproportionate effort?

The term "disproportionate effort" is not defined in the Act. In assessing what does or does not amount to disproportionate effort the starting point must be that data controllers are **not** generally exempt from providing the fair processing information because they have not obtained data directly from the data subject.

What does or does not amount to disproportionate effort is a question of fact to be determined in each and every case.

In deciding this the Commissioner will take into account a number of factors, including the nature of the data, the length of time and the cost involved to the data controller in providing the information. The fact that the data controller has had to expend a substantial amount of effort and/or cost in providing the information does not necessarily mean that the Commissioner will reach the decision that the data controller can legitimately rely upon the disproportionate effort ground. In certain circumstances, the Commissioner would consider that a quite considerable effort could reasonably be expected. The above factors will always be balanced against the prejudicial or effectively prejudicial effect to the data subject and in this respect a relevant consideration would be the extent to which the data subject already knows about the processing of his personal data by the data controller.

3.1.7.7 Timescale

As the Act makes no specific provision relating to timescale in the case of data obtained from a data subject, it should be presumed that the fair processing information must be provided to the data subject at the time that the data are obtained.

In circumstances where the data controller has obtained data from someone other than the data subject, so far as practicable, the fair processing

information must be given (or made readily available) to the data subject **before or as soon as possible after** –

(a) the time when the data controller first processes the data, or

(b) in a case where at the time **disclosure** to a third party (which does not include employees or agents of the data controller) within a reasonable period is envisaged –

- the time when the data are first disclosed to a third party, if the data are in fact disclosed within a reasonable period of time;

- the time when the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to a third party within a reasonable period of time, if within a reasonable period of time the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed, or

- in any other case, after a reasonable period of time.

Accordingly, data controllers cannot simply obtain personal data from sources other than the data subject and then do nothing else with the data except hold the data indefinitely. Before a reasonable period of time has elapsed the data controller must go through the process of informing the data subject in accordance with the fair processing requirements unless one of the exceptions referred to in paragraph 3.1.7.5 above applies or unless the data are received from another data controller who provided the data subject with all the information relating to the new data controller before passing the data on.

3.1.7.8 Paragraph 4 General Identifiers

Paragraph 4 of the fair processing requirements provides for the use of personal data which contain a "general identifier" such as a number or code used for identification purposes as defined in the Act. The Secretary of State may provide conditions, which must be complied with to ensure the fair and lawful processing of personal data containing a general identifier of a description to be prescribed. No order has been made to date to this effect.

3.2 Second Principle

"Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes".

Compliance with the Second Principle cannot be established simply by notification of the purpose(s) for which personal data are processed, as was possible under the 1984 Act. The link between compatibility and notification has now been removed by the Act.

It is to be noted that the Commissioner takes a strict view of the concept of compatibility of processing of personal data.

Part II of Schedule I of the Act provides guidance in interpreting the Second Principle. In particular, there are two means by which a data controller may specify the purpose or purposes for which the personal data are obtained, namely:-

(a) in a notice given by the data controller to the data subject in accordance with the fair processing requirements (see paragraph 3.1.7.2 above) or,

(b) in a notification given to the Commissioner under the notification provisions of the Act (contained in The Data Protection (Notification and Notification fees) Regulations 2000 (S.I. No 188)). It should be noted that notification to the Commissioner alone will not satisfy the fairness element of the First Principle.

The interpretation of the Second Principle further provides that in deciding whether any disclosure of personal data is compatible with the purpose or purposes for which the data were obtained, consideration will be given to the purpose or purposes for which the personal data are intended to be processed by any person to whom they are disclosed. Such decisions cannot be made retrospectively by data controllers once the data are obtained.

For the purposes of the Second Principle, the further processing of personal data in compliance with the conditions set out in section 33 of the Act is not to be regarded as incompatible with the purposes for which they were obtained.

Adherence to paragraph I of Part II of Schedule I is clearly material in this context (see 3.1.7.1) in that data subjects must not be deceived or misled as to the purposes for which their personal data are to be processed.

3.3 Third Principle

Personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed".

The wide definition of processing should be borne in mind when considering the Third Principle.

In complying with this Principle, data controllers should seek to identify the minimum amount of information that is required in order properly to fulfil their purpose and this will be a question of fact in each case. If it is necessary to hold additional information about certain individuals, such information should only be collected and recorded in those cases.

This guidance has been endorsed by the Data Protection Tribunal in the context of the 1984 Act in the case of Runnymede Borough Council CCRO and Others v The Data Protection Registrar (November 1990). Where a data controller holds an item of information on all individuals which will be used or useful only in relation to some of them, the information is likely to be excessive and irrelevant in relation to those

individuals in respect of whom it will not be used or useful and should not be held in those cases.

It is not acceptable to hold information on the basis that it might possibly be useful in the future without a view of how it will be used. This is to be distinguished from holding information in the case of a particular foreseeable contingency which may never occur, for example, where an employer holds details of blood groups of employees engaged in hazardous occupations.

Data controllers should continually monitor compliance with this Principle, which has obvious links with the Fourth and Fifth Principles. Changes in circumstances or failure to keep the information up to date may mean that information that was originally adequate becomes inadequate. If the data are kept for longer than necessary then they may well be both irrelevant and excessive. In most cases, data controllers should be able to remedy possible breaches of the Principle by the erasure or addition of particular items of personal data so that the information is no longer excessive, inadequate, or irrelevant.

The data controller should consider for all data:-

- the number of individuals on whom information is held;
- the number of individuals for whom it is used;
- the nature of the personal data;
- the length of time it is held;
- the way it was obtained;
- the possible consequences for individuals of the holding or erasure of the data;
- the way in which it is used;
- the purpose for which it is held.

3.4 Fourth Principle

"Personal data shall be accurate and, where necessary, kept up to date".

Data are inaccurate if they are incorrect or misleading as to any matter of fact.

The Act provides guidance in interpreting this Principle as follows:

The Principle is not to be taken as being contravened because of any inaccuracy in personal data which accurately record information obtained by the data controller from the data subject or a third party in a case where:-

(a) taking account of the purpose or purposes for which the data were obtained and further processed, the data controller has taken reasonable steps to ensure the accuracy of the data, **and**

(b) if the data subject has notified the data controller of the data subject's view that the data are inaccurate, the data indicate that fact.

It is important to note that by virtue of (a) above it is not enough for a data controller to say that, because the information was obtained from either the data subject or a third party, they had done all that they could reasonably have done to ensure the accuracy of the data at the time. Now data controllers may have to go further and take reasonable steps to ensure the accuracy of the data themselves and mark the data with any objections. The extent to which such steps are necessary will be a matter of fact in each individual case and will depend upon the nature of the data and the consequences of the inaccuracy for the data subject. This approach exceeds the requirements of the Fifth Principle in the 1984 Act.

The second part of the Principle, which refers to keeping personal data up to date, is qualified. Updating is only required "where necessary". The purpose for which the data are held or used will be relevant in deciding whether updating is necessary. For example, if the data are intended to be used merely as an historical record of a transaction between the data controller and the data subject, updating would be inappropriate. To change the data so as to bring them up to date would defeat the purpose of maintaining the historical record. However, sometimes it is important for the purpose that the data reflect the data subject's current circumstances, for example, if the data are used to decide whether to grant credit or confer or withhold some other benefit. In those cases either steps should be taken to ensure that the data are kept up to date, or when the data are used, account should be taken of the fact that circumstances may have changed.

A data controller will need to consider the following factors:-

- Is there a record of when the data were recorded or last updated?

- Are all those involved with the data – including people to whom they are disclosed as well as employees of the data controller – aware that the data do not necessarily reflect the current position?

- Are steps taken to update the personal data – for example, by checking back at intervals with the original source or with the data subject? If so, how effective are these steps?

- Is the fact that the personal data are out of date likely to cause damage or distress to the data subject?

The right contained in section 14 of the Act, by which a data subject can request that personal data be rectified, blocked, erased or destroyed, applies whether or not the data accurately record information received or obtained by the data controller from the data subject or a third party. The powers of the Court in respect of such an application are dealt with in Chapter 4.

3.5 Fifth Principle

"Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes".

To comply with this Principle, data controllers will need to review their personal data regularly and to delete the information which is no longer required for their purposes.

Statutes may make specific provision relating to the retention of certain categories of data, for example, the Police and Criminal Evidence Act 1984. Recommendations with regard to the retention of certain information can be found in the CCTV Code of Practice published by the Commissioner which contains guidance on the retention periods of recorded material.

If personal data have been recorded because of a relationship between the data controller and the data subject, the need to keep the information should be considered when the relationship ceases to exist. For example, the data subject may be an employee who has left the employment of the data controller. The end of the relationship will not necessarily cause the data controller to delete all the personal data. It may well be necessary to keep some of the information so that the data controller will be able to confirm details of the data subject 's employment for, say, the provision of references in the future or to enable the employer to provide the relevant information in respect of the data subject's pension arrangements. It may well be necessary in some cases to retain certain information to enable the data controller to defend legal claims, which may be made in the future. Unless there is some other reason for keeping them, the personal data should be deleted when the possibility of a claim arising no longer exists i.e when the relevant statutory time limit has expired. The data controller may wish to consider the value of records for historical purposes. The Act provides that personal data processed only for historical, statistical or research purposes in compliance with the conditions set out in section 33, may be kept indefinitely. (Section 33(3)).

3.6 Sixth Principle

"Personal data shall be processed in accordance with the rights of data subjects under this Act".

The Act provides guidance in interpreting this Principle. A person will contravene this Principle if, but only if:-

(a) he fails to supply information pursuant to a subject access request under section 7 of the Act, or

(b) he fails to comply with notices given under the following provisions of the Act:-

(i) section 10 (right to prevent processing likely to cause damage or distress);

(ii) section 11 (right to prevent processing for the purposes of direct marketing); or

(iii) section 12 (rights in relation to automatic decision-taking); or

(c) he fails to comply with a notice given under section 12A of the Act (right to require data controller to rectify, block, erase or destroy inaccurate or incomplete data or cease holding such data in a way incompatible with the data controller's legitimate purpose) in respect of exempt manual data only during the transitional period up to and including 23 October 2007. (See Chapter 6 on Transitional Relief).

3.7 Seventh Principle

"Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data".

The Act gives some further guidance on matters which should be taken into account in deciding whether security measures are "appropriate". These are as follows:-

(i) Taking into account the state of technological development at any time and the cost of implementing any measures, the measures must ensure a level of security appropriate to:

(a) the harm that might result from a breach of security; and

(b) the nature of the data to be protected.

(ii) The data controller must take reasonable steps to ensure the reliability of staff having access to the personal data.

With regard to the technical and organisational measures to be taken by data controllers, the Directive states that such measures should be taken " both at the time of the design of the processing system and at the time of the processing itself, particularly in order to maintain security and thereby to prevent any unauthorised processing." Data controllers are, therefore, encouraged to consider the use of privacy enhancing techniques as part of their obligations under the Seventh Principle.

It is clear from (i) above that there can be no standard set of security measures that is required for compliance with the Seventh Principle. The Commissioner's view is that what is appropriate will depend on the circumstances, in particular, on the harm that might result from, for example, an unauthorised disclosure of personal data, which in itself might depend on the nature of the data. The data controller, therefore, needs to adopt a risk-based approach to determining what measures are appropriate. (In fact, the Directive refers to "a level of security appropriate to the risks represented by the processing"). Management and organisational measures are as important as technical ones.

Standard risk assessment and risk management techniques involve identifying potential threats to the system, the vulnerability of the system to those threats and the counter-

measures to put in place to reduce and manage the risk. In many cases, a simple consideration of these matters will be sufficient. On the other hand, there are well-established formal methodologies which will assist any data controller to assess and manage the security risks to the system.

Some of the security controls that the data controller is likely to need to consider are set out below. (This is not a comprehensive list but is illustrative only.)
Security management:

- does the data controller have a security policy setting out management commitment to information security within the organisation?

- is responsibility for the organisation's security policy clearly placed on a particular person or department?

- are sufficient resources and facilities made available to enable that responsibility to be fulfilled?

Controlling access to information:

- is access to the building or room controlled or can anybody walk in?

- can casual passers-by read information off screens or documents?

- are passwords known only to authorised people and are the passwords changed regularly?

- do passwords give access to all levels of the system or only to those personal data with which that employee should be concerned?

- is there a procedure for cleaning media (such as tapes and disks) before they are reused or are new data merely written over old? In the latter case is there a possibility of the old data reaching somebody who is not authorised to receive it? (e.g. as a result of the disposal of redundant equipment).

- is printed material disposed of securely, for example, by shredding?

- is there a procedure for authenticating the identity of a person to whom personal data may be disclosed over the telephone prior to the disclosure of the personal data?

- is there a procedure covering the temporary removal of personal data from the data controller's premises, for example, for staff to work on at home? What security measures are individual members of staff required to take in such circumstances?

- are responsibilities for security clearly defined between a data processor and its customers?

Ensuring business continuity:

- are the precautions against burglary, fire or natural disaster adequate?
- is the system capable of checking that the data are valid and initiating the production of back-up copies? If so, is full use made of these facilities?
- are back-up copies of all the data stored separately from the live files?
- is there protection against corruption by viruses or other forms of intrusion?

Staff selection and training:

- is proper weight given to the discretion and integrity of staff when they are being considered for employment or promotion or for a move to an area where they will have access to personal data?
- are the staff aware of their responsibilities? Have they been given adequate training and is their knowledge kept up to date?
- do disciplinary rules and procedures take account of the requirements of the Act? Are these rules enforced?
- does an employee found to be unreliable have his or her access to personal data withdrawn immediately?
- are staff made aware that data should only be accessed for business purposes and not for their own private purposes?

Detecting and dealing with breaches of security:

- do systems keep audit trails so that access to personal data is logged and can be attributed to a particular person?
- are breaches of security properly investigated and remedied; particularly when damage or distress could be caused to an individual?

The Act introduces express obligations upon data controllers when the processing of personal data is carried out by a data processor on behalf of the data controller. In order to comply with the Seventh Principle the data controller must –

- choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures they take,
- take reasonable steps to ensure compliance with those measures, and
- ensure that the processing by the data processor is carried out under a contract, which is made or evidenced in writing, under which the data processor is to act only on instructions from the data controller. The contract must require the data processor to comply with obligations equivalent to those imposed on the

data controller by the Seventh Principle.

Further advice may be found in BS 7799 and 1S0/IEC Standard 17799.

It is important to note that the Seventh Principle relates to the security of the processing as a whole and the measures to be taken by data controllers to provide security against any breaches of the Act rather than just breaches of security.

3.8 Eighth Principle

"Personal data shall not be transferred to a country or territory outside the European Economic Area, unless that country or territory ensures an adequate level of protection of the rights and freedoms of data subjects in relation to the processing of personal data".

For a legal analysis by the Commissioner and a suggested "good practice approach" to assessing adequacy, refer to the guidance published by the Commissioner entitled, "The Eighth Data Protection Principle and Transborder Data Flows". For compliance advice on the Eighth Data Protection Principle refer to the guidance entitled, "International Transfers of Personal Data".

The European Economic Area ("The EEA") consists of the fifteen EU Member States together with Iceland, Liechtenstein and Norway.

The interpretation to the Eighth Principle provides that an adequate level of protection is one which is adequate in all the circumstances of the case, having regard in particular to:-

- the nature of the personal data,
- the country or territory of origin of the information contained in the data,
- the country or territory of final destination of that information,
- the purposes for which and period during which the data are intended to be processed,
- the law in force in the country or territory in question,
- the international obligations of that country or territory,
- any relevant codes of conduct or other rules which are enforceable in that country or territory (whether generally or by arrangement in particular cases), and
- any security measures taken in respect of the data in that country or territory

This is not an exhaustive list.

The Act provides that, where the European Commission makes a finding that a country or territory outside the EEA does, nor does not, ensure an adequate level of protection within the meaning of Article 25(2) of the Directive, any question which may arise as to whether an adequate level of protection is met in relation to the transfer of any personal data to a country or a territory outside the EEA shall be determined in accordance with that finding. (For up to date information on those findings, contact the Commissioner's office or see the website).

Schedule 4 of the Act provides for circumstances in which the Eighth Principle does not apply to a transfer. These are where:-

(i) The data subject has given their consent to the transfer

(ii) The transfer is necessary:-

(a) for the performance of a contract between the data subject and the data controller, or

(b) for the taking of steps at the request of the data subject with a view to the data subject entering into a contract with the data controller.

(iii) The transfer is necessary:-

(a) for the conclusion of a contract between the data controller and a person other than the data subject which:-

- is entered into at the request of the data subject, or

- is in the interests of the data subject, or

(b) for the performance of such a contract.

(iv) The transfer is **necessary** for reasons of substantial public interest.

The Secretary of State may specify by order the circumstances in which a transfer is to be taken to be necessary for reasons of substantial public interest. No order to this effect has been made to date.

(v) The transfer:-

(a) is **necessary** for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings),

(b) is **necessary** for the purpose of obtaining legal advice, or

(c) is otherwise **necessary** for the purposes of establishing, exercising or defending legal rights.

(vi) The transfer is **necessary** in order to protect the vital interests of the data subject.

(vii) The transfer is part of the personal data on a public register and any conditions subject to which the register is open to inspection are complied with by any person to whom the data are or may be disclosed after the transfer.

(viii) The transfer is made on terms which are of a kind approved by the Commissioner as ensuring adequate safeguards for the rights and freedoms of data subjects. It is not the practice of the Commissioner to consider or approve individual draft contracts submitted to her.

(ix) The transfer has been authorised by the Commissioner as being made in such a manner as to ensure adequate safeguards for the rights and freedoms of data subjects.

Chapter 4: Individuals' Rights

Introduction

The Act gives rights to individuals in respect of personal data held about them by others. The rights are:-

a. Right to subject access (section 7 to 9).

b. Right to prevent processing likely to cause damage or distress (section 10).

c. Right to prevent processing for the purposes of direct marketing (section 11).

d. Rights in relation to automated decision taking (section 12).

e. Right to take action for compensation if the individual suffers damage by any contravention of the Act by the data controller (section 13).

f. Right to take action to rectify, block, erase or destroy inaccurate data (section 14, section 12A and section 62).

4.1 Right of Subject Access

Sections 7 to 9 provide that upon making a request in writing (which includes transmission by electronic means) and upon paying the appropriate fee to the data controller, an individual is entitled to be told by the data controller whether they or someone else on their behalf is processing that individuals' personal data, and if so, to be given a description of:-

- the personal data;
- the purposes for which they are being processed; **and**
- those to whom they are or may be disclosed.

The individual is also entitled to have communicated to him in an intelligible form, all the information which forms any such personal data. This information must be supplied in permanent form by way of a copy, except where the supply of a copy in permanent form is not possible or would involve disproportionate effort, or the data subject agrees otherwise.

"Disproportionate effort" is not defined in the Act. Accordingly, it will be a question of fact in each case as to whether the supply of information in permanent form amounts to disproportionate effort. Matters to be taken into account by the Commissioner may be the cost of provision of the information, the length of time it may take to provide the information, how difficult or otherwise it may be for the data controller to provide the information and also the size of the organisation of which the request has been made. Such matters will always be balanced against the effect on the data subject.

If any of the information in the copy is not intelligible without explanation, the data subject should be given an explanation of that information, e.g. where the data controller holds the information in coded form which cannot be understood without the key to the code and, subject to third party information referred to below, any information as to the source of those data.

Where a decision significantly affecting a data subject is, or is likely to be, made about that data subject by fully automated means, for the purpose of evaluating matters about that data subject such as his performance at work, his creditworthiness, his reliability or his conduct he is entitled to be told of the logic involved in the process. In order to obtain this information the data subject must specifically request it when making the subject access request by virtue of the Data Protection (Subject Access)(Fees and Miscellaneous Provisions) Regulations 2000 (S.I. No. 191). The data controller is not required to supply this information where it constitutes a trade secret. The Act does not define "trade secret".

A data controller may charge a fee for dealing with subject access. Currently, the maximum fee chargeable is £10, or £2 if it is a request for limited information from a credit reference agency. There are special rules that apply to fees for access to manual health records (where the maximum fee is currently £50) and education records (where there is a sliding scale ranging from £1 to £50 depending upon the number of pages to be provided). Details can be found in S.I. No. 191 referred to above (as amended by S.I. No 3223) and on the Commissioner's website.

A data controller must comply with a subject access request promptly, in other words as quickly as he can, and in any event within forty days of receipt of the request or, if later, within forty days of receipt of –

(a) the information required to satisfy himself as to the identity of the person making the request to enable him to locate the information which that person seeks; and

(b) the fee.

There are different time limits for credit files, which must be provided within 7 working days of the receipt of the request, or, if later, within 7 working days of receipt of the information in (a) and (b) above, and school pupil records which must be provided within 15 school days of the receipt of the request or, if later, within 15 days, of the information referred to in (a) and (b) above.

Unless the data controller has received a request in permanent form, the prescribed fee and, if necessary, the information referred to above, the data controller need not comply with the request. However, the Commissioner's advice is that a data controller should act promptly in requesting the fee or any other further information necessary to fulfil the request. A deliberate delay on the part of the data controller is not acceptable.

The Commissioner might make an adverse assessment of a data controller where the data controller delays requesting payment of any required fee, or the provision of any further information to enable him to comply with the request, where such delays result

in the response to the subject access request being provided after forty days from receipt of the original subject access request.

An amendment to section 7 of the Act has been brought in by paragraph 1 of Schedule 6 to the FoIA which provides that where a data controller:-

(a) reasonably requires further information in order to satisfy himself as to the identity of the person making a subject access request and to locate the information which that person seeks; and

(b) has informed him of that requirement,

(c) the data controller is not obliged to comply with the request unless he is supplied with that further information.

The amendment does not address the situation where the data subject may have failed to provide the requisite fee.

Data controllers do not need to comply with a request where they have already complied with an identical or similar request by the same individual unless a reasonable interval has elapsed between compliance with the previous request and the making of the current request. In deciding what amounts to a reasonable interval, the following factors should be considered:

- the nature of the data;
- the purpose for which the data are processed; and
- the frequency with which the data are altered.

The information given in response to a subject access request should be all that which is contained in the personal data at the time the request was received. However, routine amendments and deletions of the data may continue between the date of the request and the date of the reply. To this extent, the information revealed to the data subject may differ from the data which were held at the time the request was received, even to the extent that data are no longer held. But, having received a request, the data controller must not make any special amendment or deletion which would not otherwise have been made. The information must not be tampered with in order to make it acceptable to the data subject.

4.1.1 Disclosures relating to the physical or mental health or condition of the data subject

If the information requested consists of information as to the physical or mental health of the data subject and the data controller is not a health professional (as defined in The Data Protection (Subject Access Modification)(Health) Order 2000 (S.I. No. 413)) the information should not be provided unless the appropriate health professional (also defined) has been consulted. The exception to the rule is where the data controller already has a written opinion from the appropriate health professional obtained within the previous six months that an exemption to the right of subject access exists because

the disclosure is likely to cause serious harm to the physical or mental health of the data subject or any other person.

If the data controller intends to rely upon an existing opinion obtained within the previous six months, the data controller must consider whether it is reasonable in all the circumstances to re-consult the health professional. The exemption does not apply to the extent that the subject access request relates to information which the data controller is satisfied has previously been seen by the data subject or is already within the knowledge of the data subject.

4.1.2 Credit Reference Agencies

Where the data controller is a credit reference agency, a subject access request may be limited to personal data relevant to the individual's financial standing and, unless the request shows a contrary intention, will be deemed to be so limited. A request for a credit file should be made to the three main credit reference agencies namely,

Equifax Plc Credit File Advice Service PO Box 300 Glasgow G81 2DT	Experian Limited Consumer Help Service PO Box 8000 Nottingham NG1 5GX	Callcredit plc Park Row House 5th Floor 19-20 Park Row Leeds LS1 5JF

and should include the data subject's name, address, postcode, any other addresses the data subject has had in the last 6 years and any other names used in that period. Further information may be obtained from the Commissioner's publication "No Credit".

4.1.3 How does the data controller satisfy himself as to the identity of the person making the request?

If accidental disclosure of the information held by the data controller to an individual other than the data subject would not be likely to cause damage or distress to the data subject, the data controller may rely upon the usual signature of the individual as proof of identity and the information may be sent to an address known to the data controller as being the address of the person making the request.

If the information is such that its accidental disclosure to an individual impersonating the data subject would be likely to cause damage or distress to the real data subject, the data controller might reasonably require better proof. Possible methods of checking identity in these circumstances include:

- asking the individual to give information which has been recorded as personal data by the data controller and which the individual might be expected to know;

- asking the individual to have their signature witnessed by another person who is over 18 and is not a relative;

- asking the individual to produce a document that might reasonably be expected to be in only their possession.

4.1.4 What about information relating to a third party?

A particular problem arises for data controllers who may find that in complying with a subject access request they will disclose information relating to an individual other than the data subject who can be identified from that information, including the situation where the information enables that other individual to be identified as the source of the information. The Act recognises this problem and sets out only two circumstances in which the data controller is obliged to comply with the subject access request in such circumstances, namely –

- where the other individual has consented to the disclosure of the information; or

- where it is reasonable in all the circumstances to comply with the request without the consent of the other individual.

The Act assists in interpreting whether it is reasonable in all the circumstances to comply with the request without the consent of the other individual concerned. In deciding this question regard shall be had, in particular, to –

- any duty of confidentiality owed to the other individual;

- any steps taken by the data controller with a view to seeking the consent of the other individual;

- whether the other individual is capable of giving consent; and

- any express refusal of consent by the other individual.

If a data controller is satisfied that the data subject will not be able to identify the other individual from the information, taking into account any other information which, in the reasonable belief of the data controller, is likely to be in (or to come into) the possession of the data subject, then the data controller must provide the information. If the data controller can protect the identity of the other individual just by deleting the actual name or referring to, for example, "Mr X", the data controller must provide the information amended in this way.

Where the information requested consists of certain records or reports relating to the physical or mental health or condition of the data subject, education or social work there are special rules regarding subject access and third party information. These rules are set out in The Data Protection (Subject Access Modification)(Health) Order 2000 (S.I. No. 413, The Data Protection (Subject Access Modification) (Education) Order 2000 (S.I No 414) and The Data Protection (Subject Access Modification)(Social Work) Order 2000 (S.I. No. 415) .

Access to a record containing information as to the data subject's physical or mental health or condition cannot be denied on the grounds that the identity of a third party would be disclosed if the third party is a health professional (as defined in S.I. No. 413 referred to above) who has compiled, or contributed to, the health record or has been involved in the care of the data subject in his capacity as a health professional, unless serious harm to that health professional's physical or mental health or condition is likely to be caused by giving access.

Access to an education record or a social work record cannot be denied on the grounds that the identity of a third party would be disclosed where the third party is a "relevant person" as defined by the Act, unless serious harm to that person's physical or mental health or condition is likely to be caused by giving access.

In the context of an education record The Data Protection(Subject Access Modification) (Education) Order (S.I. No. 414) referred to above defines a "relevant person" as:

- an employee of the local education authority which maintains the school, a teacher or other employee of an education and library board, or in the case of a voluntary aided, foundation or foundation special school or special school not maintained by a local education authority, a teacher or other employee of the school;

- a person employed by an education authority (within the meaning of paragraph 6 of Schedule 11 of the Act) in pursuance of its function relating to education and the information relates to him, or he supplied the information in his capacity as such employee; or

- the person making the request.

Where the information being requested constitutes social work as defined by The Data Protection (Subject Access Modification) (Social Work) Order (S.I. No. 415) and:

- (except in relation to Scotland) the data subject is a child and the request is made by someone with parental responsibility who is enabled to make the request by some enactment or rule of law; or

- in relation to Scotland, the data subject is a person under 16 and the request is made by someone with parental responsibility who is enabled to make the request by some enactment or rule of law; or

- the data subject is incapable of managing his own affairs and the person making the request has been appointed by a court to manage those affairs;

the information should **not** be supplied if:

(a) the information was supplied in expectation that it would not be disclosed to that person; or

(b) the information results from an examination or investigation to which the data subject consented in the expectation that it would not be disclosed; or

(c) the data subject has expressly indicated that the information should not be disclosed.

4.1.5 Subject Access requests made by an agent on behalf of an adult

There is no reason why an intellectually capable adult should not make a request through an agent. If a data controller who receives such a request is satisfied that the individual has authorised the agent to make the request, the data controller should reply to it. It is the agent's responsibility to produce satisfactory evidence that he or she has such authority. This might, for example, consist of a written authority signed by the individual either limited to this particular request or a general authority to make subject access requests, or it might consist of a general power of attorney given by the individual to the agent.

4.1.6 Subject Access requests made on behalf of children

All individuals have the right to make subject access requests. In relation to the capacity of a child to make subject access requests, the position was difficult under the 1984 Act because of the difference in the law in Scotland from the law in England, Wales and Northern Ireland.

In Scotland, a child is not deemed to have legal capacity until the age of 16, whereas in England, Wales and Northern Ireland, the guidance has been that by the age of 12 a child can be expected to have sufficient maturity to understand the nature of the request. A child may, of course, reach sufficient maturity earlier and it will be a question of fact in each case.

The position in England, Wales and Northern Ireland is unchanged with the Act but section 66 of the Act brings the position in Scotland into line with the rest in that it provides that a person under 16 may exercise any right under the Act when he has a general understanding of what it means to exercise that right and that a person of 12 years or more shall be presumed to be of sufficient age and maturity to have such understanding.

Accordingly, a data controller who receives a subject access request on behalf of a child will need to judge whether the child understands the nature of the request. If the child understands, he or she is entitled to exercise the right and the data controller should reply to the child.

If the child does not understand the nature of the request, someone with parental responsibility for the child, or a guardian, is entitled to make the request on behalf of the child and to receive the response.

4.1.7 Requests made on behalf of mentally incapacitated adults

Where an adult is, or becomes, incapable of making decisions on his own behalf, the law provides that another may be appointed to act on his behalf as his agent.

(a) **An Enduring Power of Attorney**

Individuals who make provision for a specified party to be appointed to act as their attorney should they become mentally incapacitated do so by way of an enduring power of attorney. The donor may confer general authority or specific authority on an attorney. The scope of the general powers is limited to "the management of the property and affairs" of the donor.

(b) **The Court of Protection**

Where a person loses mental capacity or, indeed, never had mental capacity, the management of his property and affairs falls to the Court of Protection.

It is the view of the Commissioner that an application to exercise a statutory right to obtain information, such as the subject access rights under section 7 of the Act, is a legal process which might, in an appropriate case, form part of the affairs of the mentally disordered patient. Therefore, an attorney or agent appointed by the Court of Protection with general authority to manage the property and affairs of the patient would, in such a case, have, under his general powers, appropriate authority to make a subject access request on the patient's behalf.

4.1.8 Application to the Court in relation to Subject Access

If a Court is satisfied on the application of:-

- any person who has made a subject access request, or
- any other person to whom serious harm to his physical or mental health or condition would be likely to be caused by compliance with such a request in contravention of section 7 of the Act or The Data Protection (Subject Access Modification)(Health) Order 2000 (S.I. No. 413), The Data Protection (Subject Access Modification) (Education) Order (S.I. No 414) and The Data Protection (Subject Access Modification)(Social Work) Order 2000 (S.I. No. 415),

that the data controller in question is about to comply with or has failed to comply with the request in contravention of section 7 or the orders referred to above, the Court may order him to comply or, as the case may be, not to comply with the request. (See Chapter 5 on exemptions and modifications for an explanation of the above mentioned orders).

4.2 Prevention of Processing Causing Damage or Distress (section 10)

If an individual believes that a data controller is processing personal data in a way that causes, or is likely to cause, substantial unwarranted damage or substantial, unwarranted distress to them or to another, section 10 of the Act provides that the individual has the right to send a notice to the data controller requiring him, within a reasonable time, to stop the processing (the "data subject notice").

This right to serve a data subject notice applies whether the individual objects to the processing taking place at all, or whether the objection relates specifically to processing for a particular purpose or in a particular way.

When a data controller receives a data subject notice he must, within 21 days, give the individual a written notice stating either:-

- that he has complied with the data subject notice, or intends to comply with it; or

- the extent to which he intends to comply with the data subject notice (if at all) and explaining the parts of the data subject notice he considers to be unjustified in any way.

4.2.1 Does this right apply to all data?

An individual can only serve a data subject notice that relates to personal data in respect of which he is the data subject. However, an individual is not entitled to serve a notice if any of the first four conditions of processing contained in Schedule 2 apply i.e.

- he has given a valid consent to the processing (although consent may be withdrawn);

- the processing is necessary for the taking of steps, at the data subject's request, with a view to entering into a contract, or the processing is necessary for the performance of a contract to which the data subject is a party;

- the processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract;

- the processing is necessary to protect the individual's vital interests (i.e. it is a life or death situation).

The Secretary of State may prescribe additional circumstances where this right is not exercisable. No order has been made to date to this effect.

What is "substantial, unwarranted damage/distress"?

It is for a court to decide in each case whether the damage or distress is substantial and unwarranted.

The Commissioner takes the view that a data subject notice is, therefore, only likely to be appropriate where the particular processing has caused, or is likely to cause, someone to suffer loss or harm, or upset and anguish of a real nature, over and above annoyance level, and without justification.

4.3 Right to prevent processing for purposes of direct marketing (section 11)

An individual is entitled by written notice, to require a data controller to cease, or not to begin, processing his personal data for the purpose of direct marketing. When a data controller receives such a notice, he must comply as soon as he can. There are no exceptions to this.

The data subject may apply to Court for an order if the data controller fails to comply with the notice.

"Direct marketing" is defined in the Act for the purposes of this provision as meaning the communication (by whatever means) of any advertising or marketing material which is directed to particular individuals. The Commissioner regards the term "direct marketing" as covering a wide range of activities which will apply not just to the offer for sale of goods or services, but also the promotion of an organisation's aims and ideals. This would include a charity or a political party making an appeal for funds or support and, for example, an organisation whose campaign is designed to encourage individuals to write to their MP on a particular matter or to attend a public meeting or rally.

An individual who wishes to prevent personally addressed marketing material being sent to him may register with the Mailing Preference Service. They can be contacted at:

Freepost 22
London
W1E 7EZ

or by telephone on: 0207 766 4410

Uninvited telesales calls and uninvited telemarketing faxes can be prevented by registering with the Telephone Preference Service on 0845 070 0707 and the Fax Preference Service on 0845 070 0702.

4.4 Rights in relation to automated decision taking (section 12)

An individual is entitled, by written notice, to require a data controller to ensure that no decision which significantly affects that individual is based solely on the processing by automatic means of personal data of which that individual is the data subject.

The Act includes specific examples of the purposes for which such automated decision-taking might be employed, i.e. evaluating matters relating to the data subject such as his performance at work, his creditworthiness, his reliability or his conduct. This is not an exhaustive list.

Where no notice has effect and where a decision which significantly affects an individual is based solely on such automatic processing, the data controller must notify the individual that the decision was taken on that basis as soon as reasonably practicable. In addition, within 21 days of receiving such notification, an individual is entitled by written notice (the "data subject notice") to require the data controller to reconsider the decision or to take a new decision on a different basis. Within 21 days of receiving the data subject notice the data controller must give the data subject a

written notice specifying the steps the data controller intends to take to comply with the data subject notice.

The Act provides for the exemption from such provisions of certain decisions reached in this way. These are called "exempt decisions". To qualify as an exempt decision certain conditions must be met as follows:-

Firstly,

(a) the decision must be taken in the course of steps taken:

- for the purpose of considering whether to enter into a contract with the data subject;
- with a view to entering into such a contract; **or**
- in the course of performing such a contract; **or**

(b) the decision must be authorised or required by or under any enactment;

Secondly,

(c) the effect of the decision must be to grant a request of the data subject; **or**

(d) steps have been taken to safeguard the legitimate interests of the data subject (for example, by allowing, the data subject to make representations).

In addition, the Secretary of State may prescribe other circumstances in which an automated decision may qualify as an exempt decision. No order to this effect has been made to date.

What can the Court do?

The Court may make an order requiring a person taking a decision in respect of the data subject (referred to in the Act as "the responsible person") to reconsider the decision or to take a new decision which is not based solely on processing by automatic means. The Court will only make such orders if it is satisfied that the responsible person has failed to comply with the data subject notice.

4.5 Right to Compensation (section 13)

An individual who suffers damage, or damage **and** distress, as the result of any contravention of the requirements of the Act by a data controller, is entitled to compensation where the data controller is unable to prove that he had taken such care as was reasonable in all the circumstances to comply with the relevant requirement.

"Damage" includes financial loss or physical injury. Unless processing is for the "special purposes", (as to which see below) compensation is not payable for distress alone. If the individual can prove that damage has been suffered, the Court may award compensation for any distress which has also been suffered by reason of the breach of the Act.

Damages for distress alone can be claimed where the contravention relates to the processing of personal data for the "special purposes", which are referred to in Chapter 5 and which comprise journalistic, artistic or literary purposes. Again, it is a defence for the data controller to prove that he had taken such care as in all the circumstances was reasonably required to comply with the requirement concerned. There are, however, reduced circumstances in which a contravention may occur as processing only for "special purposes" is, in certain circumstances, exempt from all but one of the Data Protection Principles and some sections of the Act. (See Chapter 5 for a full analysis of this exemption).

4.5.1 Making a claim for compensation

Unless a payment of compensation is agreed between the data controller and the data subject as a result of negotiations between them, the application may be made by the data subject to the Court for compensation alone, or it may be combined with an application in respect of any breach of the Act.

All claims for compensation must be made to the Court (unless the matter is settled between the parties) even where the Commissioner has made an assessment that it is likely that the processing has not been or is not being carried out in compliance with the provisions of the Act. The Commissioner has no power to award compensation.

4.5.2 How much will the Court award if a claim for compensation is successful?

There are no guidelines as to appropriate levels of compensation for a claim under the Act and the Commissioner is not routinely advised of the outcome of cases where individuals have made a successful claim for compensation under the Act. The Judge hearing the case has discretion in these matters and would have to take into consideration many factors including the seriousness of the breach and the effect upon the claimant, particularly when considering damages for distress.

4.6 Dealing with inaccuracy (section 14)

A data subject may apply to the Court for an order requiring the data controller to rectify, block, erase or destroy such data relating to that data subject as are inaccurate together with any other personal data relating to the data subject which contain an expression of opinion which the Court finds is based on the inaccurate data. Data are inaccurate if they are incorrect or misleading as to any matter of fact. A Court may also make such an order if it is satisfied, on the application of a data subject, that the data subject has suffered damage by reason of any contravention by a data controller of any of the requirements of the Act in respect of personal data, entitling the data subject to compensation under section 13, **and** that there is a substantial risk of further contravention in respect of those data in such circumstances.

In either case, the Court may, where it considers it reasonably practicable, order the data controller to notify third parties to whom the data have been disclosed of the rectification, blocking, erasure or destruction. In deciding whether it is reasonably practicable to require such notification the Court shall have regard, in particular, to the number of persons who would have to be notified.

If the data are incorrect but accurately record the information given to the data controller by the data subject or a third party, the Court may consider the requirements set out in the interpretation of the Fourth Data Protection Principle contained in paragraph 7 of Part II of Schedule I to the Act namely:

- whether the data controller took reasonable steps to ensure that the data were correct, having regard to the purpose or purposes the data were obtained and further processed; and

- if the data subject has already notified the data controller of his view that the data are inaccurate, and whether the data indicate that fact.

If the Court considers that these requirements have been complied with the Court may, as an alternative, order that the data be supplemented by a Court approved statement of the true facts.

If the Court considers that any or all of the above requirements have not been complied with, the Court may make such order as it sees fit.

If the data subject has suffered damage or damage and distress as a result of the data controller's processing of inaccurate data, compensation may be awarded.

4.6.1 Right to correct or remove incorrect data by a credit reference agency

Section 159 of the Consumer Credit Act 1974 ("CCA"), as amended by section 62 of the Act, provides that where an individual (an "objector") has been given information by a credit reference agency pursuant to a subject access request (under s.7 of the Act) or pursuant to a request under s.158 or s.160 of the CCA, and the objector believes that the information is incorrect, and that unless it is corrected he is likely to be prejudiced, he can serve a notice on the credit reference agency requiring it to remove or amend the entry.

The rights of an objector are set out in The Consumer Credit (Credit Reference Agency) Regulations 2000 (S.I. No. 290) (the "Credit Reference Regulations").

The Credit Reference Regulations provide that the credit reference agency has 28 days to respond by way of notice, indicating that it has removed the entry, amended the entry (including a copy of the amended entry), or that it has taken no action.

Twenty-eight days after either (1) the objector's notice, if no response has been sent by the data controller, or (2) the credit reference agency's notice, if he has responded and has indicated that he has not removed the entry, the objector can serve a further notice on the credit reference agency requiring it to add to the file an accompanying notice of correction (not exceeding 200 words) drawn up by the objector and to include a copy of it when furnishing information included in or based on the entry.

Within 28 days of receiving a notice containing notice of correction, the credit reference agency shall either:

- inform the objector by notice that he intends to comply with his notice,

- if it appears to the credit reference agency that it would be improper to publish the notice of correction because it is incorrect, or unjustly defames any person, or is frivolous or scandalous, or is for any other reason unsuitable, apply to the Commissioner or the Director General of Fair Trading (DGFT), as appropriate, who may make such order as she/he thinks fit.

If the objector receives no response to his notice of correction he can also apply to the Commissioner or, in appropriate cases, the DGFT for an order. Where an order is made, a person who fails to comply with it in the specified period, commits an offence.

The Commissioner may vary or revoke any order she makes.

4.6.2 Dealing with inaccuracy – exempt manual data (section 12A)

Eligible manual data (i.e. manual data which are subject to processing which was already under way immediately before 24th October 1998) forming part of an accessible record (as defined in section 68) are subject to specific rights of rectification during the first and second transitional periods where such data are inaccurate or incomplete ("exempt manual data").

Section 12A provides that a data subject may serve a notice in writing on a data controller requiring that data controller to rectify, block, erase or destroy exempt manual data which are inaccurate or incomplete, or to cease holding exempt manual data in a way incompatible with the legitimate purposes pursued by the data controller. In the event that the data controller fails to comply with the notice served by the data subject, the data subject may make an application to the Court which may order the data controller to take such steps to comply with the notice as the Court thinks fit.

Chapter 5: Exemptions and Modifications

5.1 The Exemptions

There are a number of exemptions from, and modifications to, various provisions of the Act. These are contained in Part IV (sections 28-36) and Schedule 7 and in various S.I.'s (as referred to below). The exemptions contained in Schedule 7 are referred to in the Act as "the miscellaneous exemptions".

The exemptions cannot easily be categorised into classes which enjoy the same type of exemptions. However, a number of categories of exemptions consist of, or include, an exemption from one or other of the following categories of provisions:

"the subject information provisions" which are:-

- paragraphs 2 and 3 of Part II of Schedule I which refer to the provision of the fair processing information (as to which see Chapter 3);

- section 7, subject access (as to which see Chapter 4).

"the non-disclosure provisions", which are defined as:-

- the First Data Protection Principle, **except** where it requires compliance with the conditions in Schedules 2 and 3 of the Act (the conditions for processing and conditions for processing sensitive data);

- the Second, Third, Fourth and Fifth Data Protection Principles;

- section 10 (right to prevent processing likely to cause damage or distress); and

- sections 14 (1) to (3) (rectification, blocking, erasure and destruction (as to which see Chapter 4).

to the extent to which they are inconsistent with the disclosure in question.

Exemption from the non-disclosure provisions is available in circumstances where the Act recognises that the public interest requires disclosure of personal data which may otherwise be in breach of the Act. Where an exemption from the non-disclosure provisions properly applies, such disclosure would not be in breach of the Act.

A data controller should be aware that in order to rely upon an exemption from the non-disclosure provisions he must satisfy a two-stage test:

1. The data controller must be satisfied that the disclosure falls within one of the following sections, namely, section 29(3) (the third crime and taxation exemption) section 34 (information made available to the public by or under any enactment), or section 35 (disclosures required by law or made in connection with legal proceedings).

2. If the disclosure does fall within one of the above categories, the data controller must consider each of the non-disclosure provisions in turn and decide which, if any, would be inconsistent with the disclosure in question. The data controller is then entitled to disapply only those provisions, the application of which would give rise to an inconsistency, and only then to the extent of that inconsistency.

Data controllers should, therefore, exercise caution when relying upon an exemption from the non-disclosure provisions and should not regard the proper application of the exemption as providing an automatic exemption from each of the non-disclosure provisions.

5.2 National Security (section 28)

Personal data are exempt from any of the provisions of:-

- the Data Protection Principles;
- Part II (individuals' rights), Part III (notification) and Part V (enforcement); and
- section 55 (which prohibits the unlawful obtaining of personal data as to which see Chapter 9 on Offences)

if the exemption from that provision is required for the purpose of safeguarding national security.

A certificate of exemption, signed by a Minister of the Crown, is conclusive evidence of the fact that the exemption is required for safeguarding national security. Such a certificate may identify the personal data by describing it in general terms and may have effect at a time in the future. The Data Protection Tribunal (National Security Appeals) Rules 2000 (S.I. No. 206) sets out a detailed procedure for appealing against a certificate of exemption.

5.3 Crime and Taxation (section 29)

Section 29 of the Act contains four categories of exemption which may be claimed under this heading. The first three are referred to as "the crime and taxation purposes", namely –

- the prevention or detection of crime:
- the apprehension or prosecution of offenders; or
- the assessment or collection of any tax or duty or of any imposition of a similar nature.

5.3.1 The first crime and taxation exemption (section 29(1))

Personal data processed for any of the crime and taxation purposes are exempt from –

- the First Data Protection Principle **except** that part which requires compliance with the conditions for processing and the conditions for processing sensitive data; and

- subject access

to the extent to which the application of those provisions to the data would be likely to prejudice any of the crime and taxation purposes. In other words the data controller must not disregard those provisions unless their application would be likely to prejudice any of the crime and taxation purposes.

5.3.2 The second crime and taxation exemption (section 29(2))

Personal data which –

- are processed for the purpose of discharging statutory functions; and

- consist of information obtained for such a purpose from a person who had it in his possession for any of the crime and taxation purposes,

are exempt from the subject information provisions **to the extent** to which the application of the subject information provisions to the data would be likely to prejudice any of the crime and taxation purposes.

5.3.3 The third crime and taxation exemption (section 29(3))

Personal data are exempt from the non-disclosure provisions **in any case** where the disclosure is for any of the crime and taxation purposes and where the application of those provisions in relation to the disclosure would be likely to prejudice any of the crime and taxation purposes.

5.3.4 In the case of Equifax Europe Limited v The Data Protection Registrar (case DA/90/25/49/7) decided on 28th June 1991, the Tribunal held that in the context of the equivalent provisions in the 1984 Act, "in any case" means "in any particular case" and the provision would only apply, therefore, on a case by case basis.

These three exemptions only apply where there is likely prejudice to one of the crime and taxation purposes. The Act does not explain the meaning of "likely to prejudice".

Therefore, this is not to be regarded as a blanket exemption that would justify the withholding of subject access to whole categories of data where in fact those purposes would not be likely to be prejudiced in the case of all data subjects. It would also not justify the withholding of all the personal data about a particular data subject when only part of the personal data would be likely to prejudice those purposes.

The Commissioner takes the view that, for any of these three exemptions to apply there would have to be a substantial chance rather than a mere risk that in a particular case the purposes would be noticeably damaged. The data controller needs to make a judgement as to whether or not prejudice is likely in relation to the circumstances of each individual case.

With regard to the first, second and third crime and taxation exemptions, the data controller should note the limitations on the use of this exemption. The data controller must consider each of the provisions in turn and decide which, if any, would be likely to prejudice any of the crime and taxation purposes, if they were applied.

The data controller can only disapply those provisions which would be likely to prejudice one or more of the crime and taxation purposes and then only to the extent to which prejudice would be likely to result.

If challenged, the data controller must be prepared to defend the decision to rely upon the exemption either to the Commissioner or to the Court. It would, therefore, be advisable for the data controller to ensure that each such decision is taken at an appropriately senior level within the data controller's organisation and for the reasons to be documented.

5.3.5 The fourth crime and taxation exemption (section 29(4))

This exemption can only be claimed where personal data are processed for any of the crime and taxation purposes and:-

- when the data controller is a relevant authority; i.e. a government department, a local authority, or any other authority administering housing benefit or council tax benefit; and

- where the personal data consist of a classification applied to the data subject as part of a system of risk assessment which is operated by that authority for,

- the assessment or collection of any tax or duty or any imposition of a similar nature, or

- the prevention or detection of crime, or apprehension or prosecution of offenders where the offence concerned involves any unlawful claim for any payment out of, or any unlawful application of public funds and the personal data are processed for either of those purposes.

Where the exemption applies, personal data are exempt from the subject access provisions **to the extent** to which such exemption is required in the interests of the operation of the system.

Again, the data controller should exercise caution when seeking to rely upon this exemption and should ensure that the subject access provisions are disapplied only where required in the interests of the operation of the system.

5.4 Orders Made in Relation to Health, Education and Social Work (section 30)

5.4.1 Health (The Data Protection (Subject Access Modification)(Health) Order 2000 - (S.I. 2000 No. 413) (the "Health Order")

The Health Order provides for exemptions from section 7 of the Act (subject access) for data relating to the physical or mental health or condition of the data subject **to the extent** to which the application of section 7 would be likely to cause serious harm to the physical or mental health or condition of the data subject or any other person.

Before deciding whether this exemption applies, a data controller who is not a health professional (as defined in the Act) is obliged to consult the health professional responsible for the clinical care of the data subject, or if there is more than one, the most suitable one.

The Commissioner recognises that in many cases there will be more than one health professional responsible for the patient's clinical care at the time a subject access request is made. Data controllers should ensure that they have systems in place to enable the most suitable health professional to be identified and consulted to enable the data controller to comply with a subject access request within the statutory time limit of 40 days.

Where a request for subject access is made by someone other than the data subject (i.e. by someone with parental responsibility for a child or, in relation to Scotland, by such a person on behalf of someone under the age of 16, or by a person appointed by a court to manage the affairs of the data subject) the data controller should consider any expectation of confidentiality the data subject may have had at the time the information was provided or obtained, and any wishes expressed by the data subject with regard to the disclosure of personal data relating to his physical or mental health or condition.

In specific circumstances set out in the Health Order where certain personal data are processed by the Court, there is also an exemption from the subject information provisions.

5.4.2 Education (The Data Protection (Subject Access Modifications) (Education) Order 2000 - (S.I. No. 414) (the "Education Order")

The Education Order provides for modifications and exemptions where the personal data consist of information constituting an education record (as defined), where disclosure of the information pursuant to a subject access request would be likely to cause serious harm to the physical or mental health or condition of the data subject, or to some other person or, in some circumstances, where disclosure would reveal that the data subject is, or may be at risk of child abuse (as defined in the Education Order).

The Education Order does not apply to personal data to which the Health Order applies.

5.4.3 Social Work (The Data Protection (Subject Access Modifications)(Social Work) Order 2000 - (S.I. No. 415) (the "Social Work Order")

The Social Work Order provides for modifications and exemptions where the personal data relate to social work falling within any of the descriptions set out in the Social Work Order.

The Social Work Order does not apply to personal data to which the Health Order and the Education Order apply.

5.5 Regulatory Activity (section 31)

Section 31 of the Act provides an exemption from the **subject information provisions** for the processing of personal data by reference to numerous different categories of regulatory function exercised by public "watch-dogs" which are all variously concerned with the protection of members of the public, charities or fair competition in business. Again, this is not a blanket exemption from the subject information provisions and is only available, in any case, **to the extent** that the application of any or all of such provisions would be likely to prejudice the proper discharge of those functions.

Certain provisions only apply to functions conferred by enactment upon specified individuals or organisations, but others apply to any "relevant function". A "relevant function" is a function conferred on any person by or under any enactment, any function of the Crown, a Minister of the Crown or a government department, or "any other function which is of a public nature and is exercised in the public interest".

The phrase, "function which is of a public nature and in the public interest" is not defined in the Act.

5.6 Processing for the Special Purposes (section 32)

"Special purposes" means any one or more of the following:-

- the purposes of journalism;
- artistic purposes;
- literary purposes.

Section 32 of the Act provides four conditions ("the conditions") which must all be present before the processing of personal data for the special purposes can qualify for any exemption from the Act under this section. The conditions are that –

- the personal data are processed only for the special purposes;
- the processing is undertaken with a view to the publication by any person of any journalistic, literary or artistic material;
- the data controller reasonably believes that, taking account in particular of the special importance of the public interest in freedom of expression, publication would be in the public interest, **and**
- the data controller reasonably believes that, in all the circumstances, compliance with the provision in respect of which the exemption is claimed is incompatible with the special purposes.

If **all** the conditions are satisfied, the exemption available is from the following provisions of the Act:-

- the Data Protection Principles **except** the Seventh Data Protection Principle (concerning security and other measures);

- section 7 - subject access;

- section 10 - right to prevent processing likely to cause damage or distress;

- section 12 - rights in relation to automated decision-taking;

- section 12A - the rectification, blocking, erasure or destruction of certain inaccurate manual data during the transitional periods (see Chapters 4 and 6); and

- section 14, subsections (1) to (3) - provisions relating to rectification, blocking, erasure and destruction of inaccurate data.

It should be noted that the data controller must ensure that he can satisfy the conditions in respect of each provision of the Act from which he seeks to claim an exemption.

If a person brings proceedings against a data controller under certain provisions of the Act [section 7(9) (subject access), section 10(4) (right to prevent processing), section 12(8) (automated decision-taking), section 13 (compensation) and sections 14 and 12A(3) (rectification, blocking, erasure and destruction)] the data controller may claim, or the court may decide, that the personal data in question are being processed –

- only for the special purposes; and

- with a view to the publication by any person of any journalistic, literary or artistic material which had not previously been published by the data controller 24 hours immediately preceding the claim/finding of the court.

Where this happens, the court is obliged to stay the proceedings until one of the following circumstances occur –

a) the Commissioner determines that the personal data –

    - are not being processed only for the special purposes; or

    - are not being processed with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller; or

    - the claim is withdrawn.

Where the Commissioner makes a determination, she is required to give the data controller notice of such determination. There is a right of appeal against this notice of determination. A determination by the Commissioner as to the special purposes may be made at any time and not just in the above circumstances or as a result of the

service of a special information notice (see Chapter 7 on Powers and Duties of the Commissioner).

The Data Protection (Designated Codes of Practice) (No.2) Order 2000, S.I. No. 1864 (revoking The Data Protection (Designated Codes of Practice) Order 2000 (S.I. No. 418)) specifies certain media related Codes of Practice, compliance with which may be taken into account when considering whether the belief of the data controller that publication would be in the public interest, was reasonable.

5.7 Research, History and Statistics (section 33)

Save for clarifying that it includes statistical or historical purposes, the term "research purposes" is not defined in the Act.

Section 33 of the Act provides for various exemptions in respect of the processing (or further processing) of personal data for research purposes provided that the processing (or further processing) is exclusively for those purposes and, also, that the following conditions are met –

- the data are not processed to support measures or decisions relating to particular individuals; **and**

- the data are not processed in such a way that substantial damage or substantial distress is, or is likely to be, caused to any data subject.

Where the exemption applies:

- the further processing of personal data will not be considered incompatible with the purposes for which they were obtained, (see Chapter 3 at paragraph 3.13), and

- personal data may be kept indefinitely despite the Fifth Data Protection Principle; and

- subject access does not have to be given provided that the results of the research or any resulting statistics are not made available in a form which identifies data subjects.

It is important to note that even where the exemption properly applies, the data controller is still required to comply with the rest of the Act, including the First and Second Principles. The data controller should, therefore, ensure that, at the time the data are collected, the data subject is made fully aware of what the data controller intends to do with the data. If the data controller subsequently decides to process the data in order to carry out further research of a kind that would not have been envisaged by the data subject at the time the data were collected, the data controller will need to comply with the fair processing requirements of the Act in respect of this further processing.

The exemption will not be lost just because the data are disclosed –

- to any person, for research purposes only;
- to the data subject or someone acting on his behalf;
- at the request, or with the consent, of the data subject or someone acting on his behalf;
- where the person making the disclosure has reasonable grounds for believing the disclosure falls within (a), (b) or (c) above.

As a matter of good practice, when processing for research, historical or statistical purposes, data controllers should always consider whether it is necessary to process personal data in order to achieve their purpose. Wherever possible, data controllers should only process data that has been stripped of all identifying features.

See Chapter 6 for further exemptions which may apply during the transitional period.

5.8 Information made available to the public by or under enactment (section 34)

Section 34 of the Act provides that when data consist of information which the data controller is obliged by, or under, any enactment to make available **to the public**, personal data are exempt from –

- **the subject information provisions;**
- the Fourth Data Protection Principle (accuracy);
- section 12A of the Act (applicable to exempt manual data during transitional periods) (see Chapters 4 and 6);
- section 14, sub-sections (1) to (3) of the Act (rectification, blocking, erasure and destruction); and
- **the non-disclosure provisions**

In addition, there is no requirement for a data controller to submit a notification to the Commissioner where the sole purpose of any processing is the maintenance of a public register, for example the Register of Births, Deaths and Marriages. (Section 17(4)). (See Chapter 8 - Notification).

The exemption only applies to the information that the data controller is required to publish. If the data controller holds additional personal data about the individuals concerned, the additional data is not exempt even where, in practice, the data controller does publish them.

5.9 Disclosures required by law (section 35(1))

Where the disclosure is required by or under any enactment, by any rule of law or by the order of a court, personal data are exempt from **the non-disclosure provisions.**

In these circumstances, the legal obligation overrides any objection which the data subject may have, but an element of fairness can still be applied.

For example, if the data controller is well aware when he collects the data that at some point he is likely to have to make disclosures of those data under statute, it would not be incompatible with the disclosure to notify data subjects at the time the data are collected from them, that such disclosure is likely. The First Principle should not, be disapplied generally.

5.10 Disclosures made in connection with legal proceedings (section 35(2))

Where the disclosure is **necessary** –

- for the purpose of, or in connection with, any legal proceedings (including prospective legal proceedings); or
- for the purpose of obtaining legal advice; or
- is otherwise necessary for the purposes of establishing, exercising or defending legal rights,

personal data are exempt from **the non-disclosure provisions.**

A data controller is **not obliged** to disclose personal data pursuant to a request made by a third party under section 35(2).

This provision affords the data controller exemption from any or all of the non-disclosure provisions in cases where:

- the data controller is satisfied that the nature of the request is such that the disclosure of the personal data falls within this section i.e. the disclosure is **necessary** for one or more of the above, **and**
- the data controller is satisfied that to apply the particular provision would be inconsistent with the disclosure in question.

The data controller has to remember that Schedule 2 and (where the processing is of sensitive personal data) Schedule 3 still have to be complied with. In many cases, the data controller will not be in a position to make a decision as to whether the necessity test can be met, or will not wish to make the disclosure because of his relationship with the data subject, with the result that the requesting party will have to rely upon a Court order to obtain the information.

5.11 Domestic purposes (section 36)

This is a wide-ranging exemption whereby personal data are exempt from the Data Protection Principles and the provisions of Part II (individuals' rights) and Part III (notification) of the Act where they are processed by an individual **only** for the

purposes of that individual's personal, family or household affairs (including recreational purposes).

This exemption does not extend to Part V of the Act which means that the Commissioner retains her powers of investigation and enforcement where someone appears to have exceeded the scope of the exemption.

5.12 Exemptions contained within The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000 - (S.I. No 419)

Statutory Instrument 2000 No. 419 (as amended by The Data Protection (Miscellaneous Subject Access Exemptions) (Amendment) Order, S.I. No 1865 contains a list of enactments and instruments which restrict disclosure of certain personal data or information within personal data such as: information relating to human fertilisation and embryology, adoption records and reports, statements of a child's special educational needs and parental order records and reports. Wherever those restrictions or prohibitions apply, those data or information within those data are also exempt from section 7 of the Act. (Subject Access)

5.13 The Miscellaneous Exemptions (Schedule 7) - confidential references given by the data controller

Personal data which consist of a confidential reference given, or to be given, by the data controller for specified purposes (education, training or employment, appointment to office or provision of any service) are exempt from subject access.

This exemption is not available to the data controller who receives such references. In other words, where company A provides an employment reference concerning one of its employees to company B, if the employee makes a subject access request to company A, the reference will be exempt from the disclosure. If the employee makes the request to company B, the reference is not automatically exempt from disclosure and the usual subject access rules apply. (See Chapter 4 – Subject Access)

5.14 Armed Forces

Where the application of the subject information provisions to personal data would be likely to prejudice the combat effectiveness of any of the armed forces then such personal data are exempt from **the subject information provisions.**

5.15 Judicial Appointments and Honours

Personal data processed for three specific purposes –

- assessing suitability for judicial office;
- assessing suitability for the office of Queen's Counsel; or
- the conferring of any honour

are exempt from **the subject information provisions.**

5.16 Crown Employment and Crown or Ministerial Appointments

The Act provides for exemption from **the subject information provisions** in the case of personal data processed for the purposes of assessing suitability for employment by the Crown or Ministerial appointments as listed in The Data Protection (Crown Appointments) Order 2000, S.I. No 416.

5.17 Management Forecasts/Management Planning

This exemption is available to businesses to protect confidentiality of personal data processed for the purposes of management forecasting or management planning. In any case **to the extent** to which the application of any of the subject information provisions to personal data processed for such purposes would be likely to prejudice the conduct of the business or other activity of the data controller, such personal data are exempt from **the subject information provisions.**

5.18 Negotiations

In a similar way, where personal data consist of records of the intentions of the data controller in relation to any negotiations with the data subject, such personal data are exempt from **the subject information provisions** to the extent to which the application of the subject information provisions would be likely to prejudice those negotiations.

This exemption may, for example, cover the situation where an organisation is in dispute with a former employee and records a potential settlement figure for the purpose of the organisation's own budget forecasting. If the figure was disclosed to the former employee it may prejudice negotiations between those parties.

5.19 Corporate Finance

The Act provides for an exemption from **the subject information provisions** of personal data processed for the purposes of, or in connection with, "a corporate finance service" (specifically defined in Schedule 7 paragraph 6) provided by "a relevant person" (also specifically defined in Schedule 7). The exemption is only available to the extent to which the application of the subject information provisions could, or in the reasonable belief of the data controller could, affect the price or value of particular instruments of a price-sensitive nature. "Instrument" is specifically defined in Schedule 7 paragraph 6(3) and includes, for example, company shares.

This exemption may be material in due diligence enquiries arising from company takeovers or mergers.

The exemption is also available if required for the purpose of safeguarding an important economic or financial interest of the United Kingdom. The Act provides that the Secretary of State may by order specify matters to be taken into account when determining whether exemption from the subject information provisions is required for the purpose of safeguarding an important economic or financial interest of the United Kingdom are specified in The Data Protection (Corporate Finance Exemption) Order 2000 (S.I. 2000 No 184). This provides that one such matter is the inevitable prejudicial effect on the orderly functioning of financial markets or the efficient

allocation of capital with the economy resulting from the occasional or regular application of the subject information provisions to data specified in the order.

5.20 Examination Scripts

Where personal data consist of information recorded by candidates during an examination they are exempt from subject access. However, any comments recorded by the examiner in the margins of the script are not exempt and as such should be provided even though they may not appear to the data controller to be of much value without the script itself.

5.21 Examination Marks

This is not an exemption as such but is rather an adaptation of the requirements in Section 7 of the Act to comply with a subject access request within a specified period of time (forty days from receipt of the request or, if later, receipt of the information required to comply with the request and the fee). In the case of a subject access request made in relation to examination marks or results, the timescale is extended to either –

- five months from the day on which the data controller received the request (or, if later, from the first day on which the data controller has both the required fee and the information necessary to act on the request); or

- forty days from the announcement of the examination results,

whichever is the earlier, in circumstances where, before the examination results are announced, the data subject makes the request (or provides the information required by the data controller and pays the fee).

Where the timescale is extended in accordance with the above, the information to be supplied pursuant to the request must be supplied both by reference to the data in question at the time the request is received, and (if different) by reference to the data as from the time to time held in the period beginning when the request is received and ending when it is complied with.

5.22 Legal Professional Privilege

If personal data consist of information in respect of which a claim to legal professional privilege (in Scotland, confidentiality as between client and professional legal adviser) could be maintained in legal proceedings, the personal data are exempt from **the subject information provisions** forever unless the privilege is waived.

Information a lawyer receives in the course of advising his client is confidential and should usually only be disclosed with the client's authority.

5.23 Self-incrimination

If by complying with any subject access request or order under Section 7 of the Act a person would reveal evidence of the commission of any offence, other than an offence

under the Act or the 1984 Act, exposing them to proceedings for that offence, that person need not comply with a subject access request or order.

If in complying with any subject access request or order under Section 7 of the Act a person discloses information, which is proposed to be used in evidence against them in proceedings for an offence under the Act, or the 1984 Act then such information shall not be admissible in evidence against them.

5.24 Transitional Exemptions

The Act provides transitional relief in the form of various exemptions as set out in Schedule 8 of the Act. See Chapter 6 on Transitional Provisions in this respect.

Chapter 6: Transitional Provisions

Introduction

Throughout this publication, reference has been made to transitional provisions which might apply in respect of certain processing, whereby the data controller may not necessarily have had to comply with all provisions of the Act immediately ("transitional relief"). This chapter now focuses on these transitional provisions which are found in Schedule 8 to the Act.

6.1 The Transitional Periods

The Act created an initial transitional period, in respect of manual and automated data, which started on 1st March 2000 and which ends on 23rd October 2001. This is known as the "first transitional period". A further transitional period of 6 years from 24 October 2001 may in some circumstances apply but this relates only to certain categories of manual data or personal data processed for the purpose of historical research. This is known as the "second transitional period". Where transitional relief does not apply, data controllers may nevertheless be exempt from certain provisions of the Act by virtue of other substantive exemptions in the Act (see Chapter 5 on Exemptions).

The purpose of transitional relief was to facilitate a progressive move by data controllers to the regime created by the Act. However, transitional relief only applies during the relevant transitional period for so long as, and to the extent that, personal data are subject to processing already under way (as to which, see below). Therefore, if a data controller introduces new practices or systems involving processing which is not already under way and which are applied to such personal data, then transitional relief will be lost even if this occurs before expiry of the relevant transitional period.

Personal data which are subject to processing already under way are known as **"eligible data".** Transitional relief applies to eligible data which may be either manual or automated. However, different provisions apply in respect of each. These are examined separately later in this chapter.

6.2 What is "processing already under way"?

In the first instance, data controllers must themselves decide whether processing was already under way immediately before 24 October 1998. Whether processing was already under way will be a matter of fact in each case. The term "processing" is defined in the Act (see Chapter 2 on Definitions), but the phrase "processing already under way" , which is taken directly from the Directive, is not defined in the Act. The Commissioner recognises that it is not entirely clear from the Directive what this means and that it is open to more than one interpretation.

Where data has been processed for a broad business purpose as from 24th October 1998, the Commissioner takes the view that it is likely to be processing already underway, rendering the data eligible data. In deciding whether processing was already under way, data controllers may find it helpful to review their overall processing operation asking a series of questions, including –

- Is there something different about the processing?

- If so, what is different about it? In deciding this, consider what processing was undertaken before and what processing is being undertaken from 24th October 1998.

- If the processing is different, what is the effect of this in relation to the data controller's overall processing operation? For example:-

  - is the processing within a range of activities or business processes already undertaken by the data controller?

  - does the processing result in a new or different application of the data or part of the data?

  - is the processing carried out in order to achieve a new objective?

  - does the processing produce or result in a new or different effect upon the data subject?

This list is not exhaustive – other factors may need to be taken into account depending on the type of processing operation carried out by the data controller.

6.3 What is meant by "immediately before"?

For transitional relief to apply an additional factor must be satisfied, namely, that the processing must have been in existence immediately before 24 October 1998. Therefore, where the data controller previously carried out certain processing but this had ceased at any time up to midnight on 23/24 October 1998, transitional relief would not be available.

The commencement of new processing at any time before midnight on 23/24 October 1998 would be processing already under way.

It is not necessary for the personal data to have been in existence immediately before 24 October 1998 in order for transitional relief to apply, but the actual processing to which the personal data are subject must have been in existence. (N.B. however see 6.10 below).

Example 1

What if I do one of the following from 24 October 1998?

- amend existing personal data;

- add personal data on existing data subjects;

- add personal data on new data subjects;

- carry out essential program and software changes to enable existing operations to continue.

It is unlikely that these things alone will mean that this is **not** processing already under way.

Example 2

Will a change of legal entity or status of the data controller mean in itself that processing is not processing already under way? For example, the conversion of a building society to a bank or the merger or take-over of one company by another.

Provided the processing to which personal data are subject remains the same, a change in legal entity alone will not mean it is not processing already under way. However, a common feature when a change of legal entity occurs is that the "new entity" takes on new or different functions or activities. If these involve processing which was not processing already under way, transitional relief may not apply.

6.4 Dual regime – a problem?

Processing not already under way will be subject to the provisions of the Act immediately and will not be eligible for transitional relief. Data controllers may find that within their overall processing operation, processing of some personal data attracts transitional relief whereas some will not. Different requirements may therefore apply to different data. Data controllers therefore need to ensure that their working practices and systems take account of this. Where this causes practical difficulties, data controllers may find it simpler to observe the requirements of the Act immediately.

Data controllers should be taking a pro-active approach to bring their systems, documentation and procedures into line with the requirements of the Act as soon as possible rather than postponing compliance with the new regime until expiry of any transitional relief.

6.5 The First Transitional Period

Automated data

During the first transitional period, eligible automated data (i.e. which are subject to processing already under way immediately before 24 October 1998) will not be regarded as processed (and, as a result, will not be subject to the Act during that time) **unless** the processing is done by reference to the data subject.

The Commissioner takes the view that processing by reference to the data subject will occur whenever the data controller intends to locate and process information about the data subject whatever the technical means by which this object is achieved. The Data Protection Tribunal endorsed this view in the context of the 1984 Act in the case of Equifax Europe Limited v The Data Protection Registrar (case DA/90/25//49/7) when the Tribunal indicated that processing by reference to the data subject takes place when the data are processed in a way linked to the data subject, that is, when the purpose of the processing is to learn something about the individual.

There are some exemptions in the Act available during the first transitional period which continue certain exemptions contained in the 1984 Act. They are:

- back up data;
- payroll and accounts exemption;
- unincorporated members' club exemption;
- mailing list exemption.

These exemptions only apply where processing was already under way in respect of the exempt purpose.

Further exemptions are also available for eligible automated data during the first transitional period. If the exemption applies, data are exempt from the following provisions of the Act –

- paragraphs 2 and 3 of the fair processing requirements of the Act (Schedule I, Part II);
- that part of the First Principle which requires compliance with one or more of the conditions for processing;
- that part of the First Principle which requires compliance with one or more of the conditions for processing sensitive data;
- that part of the Seventh Principle which requires processing carried out by a data processor on behalf of a data controller to be carried out under a contract made or evidenced in writing and only upon the instruction of the data controller, with obligations on the data processor to take appropriate technical and organisational steps to prevent unauthorised/unlawful processing , accidental loss, destruction or damage of personal data;
- the Eighth Principle (adequacy of protection for transborder data flows)
- the requirement for a data controller to provide any information in response to a subject access request other than confirmation whether personal data of which that individual is the data subject are being processed by or on behalf of that data controller, and the information constituting that personal data;
- the right of an individual to prevent processing likely to cause damage or distress;
- the right of an individual to prevent processing for the purposes of direct marketing;
- the right of an individual to object to automated decision-taking;
- the right of an individual suffering damage or damage and distress to claim compensation for failure to comply with certain requirements of the Act. [N.B. notwithstanding this exemption, claims for the above can still be brought for

breach of the Fourth Principle (accurate/up to date), disclosures without the consent of the data controller, loss or destruction of data without the consent of the data controller and processing for the special purposes (journalism, art and literature)].

Consequently, all eligible automated data are **subject to** the following provisions of the Act –

- personal data shall be processed fairly and lawfully (modified First Principle);
- personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes (Second Principle);
- personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed (Third Principle);
- personal data shall be accurate and, where necessary, kept up to date (Fourth Principle);
- personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes (Fifth Principle);
- personal data shall be processed in accordance with the right of data subjects to be entitled to be supplied with information (see below) in response to a subject access request (modified Sixth Principle);
- appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data (Seventh Principle);
- in response to a subject access request, an individual is only entitled to be informed whether personal data of which that individual is the data subject are being processed by or on behalf of the data controller and, if so, the individual is entitled to have communicated to him (in intelligible form) the information constituting any personal data of which that individual is the data subject. The various supplementary provisions regarding subject access, contained within sections 7 to 9 also apply (see Chapter 4);
- compensation for damage and/or distress is only available in limited circumstances, namely, as a result of:-
  - a contravention of the Fourth Principle (accurate/up to date);
  - a disclosure made without the consent of the data controller; loss or destruction of data without the consent of the data controller; or, processing for the special purposes.

Notwithstanding the exemptions, data controllers remain under a general duty under the First Principle to ensure that processing is fair.

6.6 Non-automated data

Where personal data –

- are recorded as part of a relevant filing system or with the intention that they should form part of a relevant filing system (including accessible records, as defined in section 68, which fall within the definition of relevant filing system) [see Chapter 2 on Definitions], they are eligible for transitional relief provided they are subject to processing already under way immediately before 24 October 1998;

- are otherwise part of a non-automated accessible record (i.e. that data fall within paragraph (d) in the definition of data – Chapter 2), they are eligible for transitional relief whether or not they are subject to processing already under way.

All the above are referred to as non-automated data.

6.7 Eligible Manual Data

All non-automated data are described in the Act as "eligible manual data", with the exception of data that:-

- form part of a non-automated accessible record, but

- do not form part of a relevant filing system, and

- were not recorded with the intention that they should form part of a relevant filing system, and

- are not subject to processing already under way.

6.8 Transitional exemption for limited class of eligible manual data

Except in the case of –

a) accessible records, and

b) records consisting of information as to the financial standing of the data subject where the data controller is a credit reference agency,

where different rules apply (as detailed below), eligible manual data are **exempt** from the following during the first transitional period:-

- the Principles;

- Part II of the Act (Individuals' Rights); and

- Part III of the Act (Notification).

6.9 Transitional exemption for accessible records and credit reference agency records

For the first time the Act governs such data as accessible records (as defined in section 68) and credit reference agency records. These were previously regulated by such statutes as the Access to Health Records Act 1990, Access to Personal Files Act 1987 and Consumer Credit Act 1974. These statutes, together with various other regulations, provided rights of access to such data. The transitional provisions in the Act ensure the preservation of such rights of access for individuals as previously existed for such data.

During the first transitional period:-

a) non-automated data which form part of an accessible record and which are subject to processing already under way, and

b) data that:-

- form part of an accessible record, but
- are not recorded as part (or with the intention that they should form part) of a relevant filing system, and
- are not subject to processing already under way, and

c) records consisting of information as to the financial standing of the data subject where the data controller is a credit reference agency, ("credit reference agency records")

are exempt from the following –

- the Principles,
- Part II of the Act (Individuals' Rights, **except** see below), and
- Part III of the Act (Notification).

The data controller must still comply with:-

- the subject access rights of the data subject, **and**
- the data subject's right to require on notice that the data controller rectify, block, erase or destroy inaccurate or incomplete data (even if the data are eligible data enjoying transitional relief) or that the data controller ceases holding exempt manual data in a way which is incompatible with the legitimate purposes pursued by the data controller (section12A in Schedule 13 as to which see Chapter 4).

Where personal data are processed for the purpose of historical research, further exemptions may apply indefinitely from 24 October 2001 onwards (see section on Historical Research below).

6.10 The Second Transitional Period

Transitional relief during the second transitional period (i.e. 24 October 2001 to 23 October 2007) applies to manual data only (other than in relation to the historical research exemptions, as to which, see below) and is less extensive than that available during the first transitional period.

It applies to:-

a) manual data (including accessible records and credit reference agency records) which were:-

- subject to processing already under way immediately before 24 October 1998, (i.e. eligible manual data) and
- held immediately before that date.

(Therefore manual data added on or after 24 October 1998 will not qualify)

b) data that:-

- form part of a non-automated accessible record, but
- are not recorded as part of (or with the intention that they should form part of) a relevant filing system,

whether or not processing was already under way immediately before 24 October 1998 and whenever held.

The exemption does not apply to manual data processed only for historical research purposes.

The data controller must still comply with section 12A in Schedule 13 (as to which see Chapter 4) in respect of these categories of data.

Data to which this exemption applies are exempt between 24 October 2001 to 23 October 2007 from:-

- the First Principle except Part II, Schedule I, paragraphs 2 and 3 of the fair processing requirements of the Act (see Chapter 3 on Principles);
- the Second, Third, Fourth and Fifth Principles (see Chapter 3);
- section 14 subsections (1) to (3).

For the purpose of being able to identify which data are eligible for transitional relief during the second transitional period, data controllers are advised to put in place audit procedures which enable them to identify which manual data were held by them immediately before 24 October 1998.

In most cases, non-automated data added from 24 October 1998 will become subject to the whole of the Act on 24 October 2001. The only exception in fact will be data that:-

- form part of a non-automated accessible record, **and**
- were not recorded as part of (or with the intention that they should form part of) a relevant filing system, **and**
- are not subject to processing already under way.

6.11 Historical Research (Schedule 8 and section 33)

Where personal data are processed only for the purpose of historical research (which is not defined in the Act) they may qualify for certain exemptions. When assessing whether any exemption applies the data controller will need to consider,

- whether the data were subject to processing already under way, and
- whether the data are automated or manual.

First Transitional Period

1. Processing which was **not** already under way:

   - the exemption at section 33 of the Act may apply (see Chapter 5 at paragraph 5.7).

2. Processing which **was** already under way:

   a) **Automated** data are exempt from:-

   - the First Principle to the extent to which it requires compliance with the fair processing requirements of the Act at Part II, Schedule I, the conditions for processing in Schedule 2 and the conditions for processing sensitive personal data in Schedule 3;
   - the Seventh Principle to the extent to which it requires a data controller to ensure that processing carried out by a data processor on behalf of the data controller is carried out under contract;
   - the Eighth Principle;

- section 7(1)(b), 7(1)(c)(ii) and 7(1)(d);
- sections 10 and 11;
- section 12;
- section 13, except so far as relating to:
  - any contravention of the Fourth Principle
  - any disclosure without the consent of the data controller
  - loss or destruction of data without the consent of the data controller, or
  - processing for the special purposes.

b) **Manual** data are exempt from:

- The Principles
- Part II of the Act (Individuals' Rights), and
- Part III of the Act (Notification).

Second Transitional Period

1. Eligible automated data which **are** processed by reference to the data subject (see above) will be exempt from the requirement in the First Principle for one or more of the conditions for processing to be complied with; and, when sensitive personal data are being processed, for one or more of the conditions for processing sensitive data to be complied with.

2. Eligible automated data which **are not** processed by reference to the data subject will be exempt from:-

   - the First Principle **except** paragraphs 2 and 3 of Part II of Schedule I of the fair processing requirements of the Act (see Chapter 3 on Principles),
   - the Second, Third, Fourth and Fifth Principles (see Chapter 3);
   - section 14 subsections (1) to (3) relating to rectification, blocking, erasure and destruction of inaccurate data (see Chapter 4 on Individuals' Rights).

3. Eligible manual data will be exempt as in 2 above (i.e. eligible automated data not processed by reference to the data subject).

   This exemption will not be lost because the data are disclosed:-

a. to any person, for historical research purposes only;

b. to the data subject or someone acting on her behalf;

c. at the request of, or with the consent of, the data subject or someone acting on his behalf;

d. where the person making the disclosure has reasonable grounds for believing the disclosure falls within (a), (b) or (c) above.

Conclusions

Data controllers will have to decide for themselves whether or not (or to what extent) their processing and their various data are eligible for transitional relief. The Commissioner recognises that there will be cases where it is unclear whether particular data are so eligible or whether they are subject to processing already under way. The data controller will have to make reasoned judgements in those cases. Data controllers should ensure that all processing that attracted transitional relief in the first transitional period but which is not eligible for transitional relief in the second transitional period is fully compliant with the Act from 24 October 2001.

Exemptions from 1984 Act continuing during first transitional period

Data controllers familiar with the 1984 Act will recognise the following exemptions which have been retained in the Act albeit only for the limited period between commencement of the substantive provisions of the Act and 23 October 2001. The following guidance is largely based on that already published in The Guidelines (Fourth Series, September 1997) on the 1984 Act.

Back-up data

Eligible automated data which are processed only for the purpose of replacing other data in the event of the latter being lost, destroyed and impaired, are exempt from subject access in addition to the transitional relief referred to above.

Payrolls and Accounts

Where this exemption applies the data are exempt, during the first transitional period, from the requirement to comply with:-

- *The Data Protection Principles,*
- *Part II of the Act (rights of data subjects and others – see Chapter 4 on Individuals' Rights), and*
- *Part III of the Act (notification by data controllers – see Chapter 8).*

To qualify for this exemption the data must be:

- *Automated*

- *"eligible", i.e. subject to processing which was already under way immediately before 24 October 1998*

- *processed **only** for one or more of the following purposes:-*

The payroll purposes:

- *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, or*
- *paying amounts deducted from remuneration or pensions.*

The accounts purposes:

- *keeping accounts relating to any business or other activity carried on by the data controller, or*
- *keeping records of purchases, sales or other transactions in order to ensure that any necessary payments are made by or to the data controller for those transactions or in order to make financial or management forecasts to assist the data controller in the conduct of any business or activity carried on by them.*

*If the data are processed for any other purpose, the exemption is lost **unless** the data controller can show that they had taken such care to prevent the processing for another purpose as, in all the circumstances, was reasonably required.*

A further condition that must be satisfied is that the data may only be disclosed in very limited circumstances. If any other disclosure is made, then the exemption is lost. To satisfy this condition:-

- *data processed for the accounts purposes or for both the accounts and payroll purposes may only be disclosed:-*

  - *for the purpose of audit, or*
  - *for the purpose of giving information about the data controller's financial affairs.*

*In addition to the above permitted disclosures, data held **only** for the payroll purposes may also be disclosed (provided that they are not also held for the accounts purposes):-*

- *to any person, other than the data controller, by whom the remuneration or pensions in question are payable,*
- *in order to obtain actuarial advice,*
- *for the research into occupational diseases or injuries,*
- *when the data subject (or a person acting on their behalf) has requested or consented to the disclosure of the personal data. In this case the consent need not be to the particular disclosure but may be given generally or may be related to the circumstances of the disclosure, or*
- *if the person making the disclosure has reasonable grounds for believing that the disclosure falls within the circumstances set out in the paragraph above.*

Unincorporated Members' Clubs

An unincorporated members' club is a club whose members usually each contribute, by way of an entrance fee or subscription, to the club's funds. The property and funds of the club belong to the members, who manage the club and its property. The conduct of the club's business is usually delegated by the members to committees in accordance with the rules.

Where this exemption applies the data are exempt, during the first transitional period, from the requirement to comply with:-

- *The Data Protection Principles,*
- *Part II of the Act (rights of data subjects and others – see Chapter 4), and*
- *Part III of the Act (notification by data controllers – see Chapter 8).*

To qualify for this exemption the data must be:-

- *Automated*
- *eligible, i.e. subject to processing which was already under way immediately before 24 October 1998*
- *processed by an unincorporated members' club and must relate only to the members the club.*

In addition,

- *all members of the club must be asked whether they object to the personal data relating to them being held by the club. It should be noted that this requires positive action on the part of the data controller. It is not sufficient for a data controller to assume that a member does not object simply because the member is aware that his\her details are held on the club's computer and the member has never registered an objection. If any member does object then:-*

  - *the personal data relating to that member should not be put onto the computer or, if the objection is received after the data are put onto the computer, the data should be taken off. So far as the Act is concerned, that information can be processed manually subject to the Act and, if applicable, the transitional provisions relating to manual data (see above), and*
  - *the data controller will have to register a notification with the Commissioner in respect of the personal data. Having notified, the data controller may continue to process the personal data whether or not members object.*

  Personal data about members may only be disclosed in very limited circumstances, namely:-

  - *When the member, or a person acting on behalf of the member, has requested or consented to the disclosure. This consent may be given either generally or in the circumstances in which the disclosure in question is made;*

- *If the person making the disclosure has reasonable grounds for believing that the disclosure falls within the circumstances set out in the paragraph above.*

*If the data are disclosed in any other circumstances, the exemption is lost **unless** the data controller can show that they had taken such care to prevent the disclosure as, in all the circumstances, was reasonably required.*

Mailing Lists

Where this exemption applies the data are exempt, during the first transitional period, from the requirement to comply with:-

- *the Data Protection Principles,*
- *Part II of the Act (rights of data subjects and others – see Chapter 4), and*
- *Part III of the Act (notification by data controllers – see Chapter 8).*

To qualify for this exemption the personal data must:-

- *be automated;*
- *be eligible, i.e. subject to processing which was already under way immediately before 24 October 1998;*
- *be processed by a data controller **only** for the purposes of distributing, or recording the distribution of, articles or information to individuals;*
- *consist only of the names and addresses of the individuals or other details needed for making the distribution. These other details might include, for example, telephone or fax numbers. If more information is held, for example as to occupation, status, interests or preferences of the individual, this exemption does not apply.*

In addition,

- *all the individuals must be asked whether they object to the personal data relating to them being held by the data controller. If an individual does object then:-*
  - *the personal data relating to that individual should not be put onto the computer or, if the objection is received after the data are put onto the computer, the data should be taken off. So far as the Act is concerned, that information can be processed manually subject to the Act and, if applicable, the transitional provisions relating to manual data (see above), and*
  - *the data controller will need to register a notification with the Commissioner in respect of the personal data. Having notified, the data controller may continue to process the personal data whether or not the individual objects.*
- *the data must not be processed for any purpose other than the distribution or recording the distribution of, articles of information to individuals **unless** the data controller can show*

that they had taken such care to prevent processing for any other purpose as, in all the circumstances, was reasonably required.

Chapter 7: Powers and Duties of the Commissioner

7.1 The Commissioner's Duties

The Commissioner is an independent officer who is appointed by Her Majesty the Queen and who reports directly to Parliament.

The Commissioner's duties in relation to the Act are to:-

(1) promote the following of good practice by data controllers and, in particular, promote the observance of the requirements of the Act by data controllers,

(2) spread information on the Act and how it works,

(3) encourage, where appropriate, the development of Codes of Practice for guidance as to good practice,

(4) co-operate with foreign designated authorities in the manner prescribed by section 54 of the Act and by The Data Protection (Functions of Designated Authority) Order 2000 (S.I. No 186),

(5) maintain a register of data controllers who are required to notify their processing,

(6) lay annually before each House of Parliament a general report on the exercise of her functions under the Act,

(7) lay before each House of Parliament any Code of Practice prepared pursuant to the Act, and

(8) prosecute persons in respect of offences committed under the Act.

7.2 Requests for Assessment

A request for assessment can be made by any person who is, or believes himself to be, directly affected by any processing of personal data. (Section 42)

On receiving a request for assessment the Commissioner is required to make an assessment as to whether it is likely or unlikely that the processing has been or is being carried out in compliance with the provisions of the Act. The only circumstances in which the Commissioner is not required to make an assessment are where she has not been supplied with sufficient information to enable her to:-

- be satisfied as to the identity of the person making the request, and
- identify the processing in question.

The Commissioner has a wide discretion in deciding the appropriate way in which to make an assessment, namely, in such manner as appears to her to be appropriate. The

matters which the Commissioner may take into account in this respect specifically include:-

- the extent to which the request appears to raise a matter of substance;
- any undue delay in making the request; and
- whether or not the person making the request is entitled to make an application for subject access in respect of the personal data in question.

The Commissioner must notify the person who made the request whether she has made an assessment as a result of the request. In addition, the Commissioner may notify the person who made the request of any view formed or action taken as a result of the request.

Further information is available from the Commissioner's office or on the Commissioner's website in publications entitled "Handling Assessments" and "Requests for Assessment".

7.3 Enforcement Notices

Under the Act the Commissioner is able to serve an **enforcement notice** upon a data controller who the Commissioner is satisfied has contravened or is contravening any of the Data Protection Principles (section 40). An enforcement notice requires a data controller to take, or to refrain from taking, specified steps or to refrain from processing any personal data (or personal data of a specified description) altogether, or from processing for a specified purpose or in a specified manner. Compliance with an enforcement notice should ensure compliance with the Principle(s) in question.

In deciding whether to serve an enforcement notice the Commissioner must consider whether the contravention has caused or is likely to cause any person damage or distress.

An enforcement notice must not require any of the provisions of the notice to be complied with before the end of the period within which an appeal can be brought against the notice unless the enforcement notice contains a statement of urgency. If an appeal is lodged the notice need not be complied with pending the determination or withdrawal of the appeal.

If the Commissioner considers that there are special circumstances which mean that a notice should be complied with as a matter of urgency, the Commissioner may include a statement to this effect in the notice together with her reasons. If there is a statement of urgency included, the notice must not require the provisions of the notice to be complied with before the end of the period of seven days, beginning with the day on which the notice is served. However, the requirement to comply with the notice will not then be suspended if an appeal is lodged against the notice.

An enforcement notice may be cancelled or varied in certain circumstances, for example when the Commissioner considers that the notice (or part of it) need not be

complied with in order to ensure compliance with the Data Protection Principles or Principle in question.

7.4 Processing for the Special Purposes

The Commissioner may make a determination under the Act as to the " special purposes" (see paragraph 5.6 in Chapter 5). Such determination may be made when it appears to the Commissioner that any personal data are not being processed only for the special purposes, or are not being processed with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller. The Commissioner is not able to serve an enforcement notice in the case of processing for the special purposes unless a determination has taken effect and an order for leave has been obtained from the court for the notice to be served.

7.5 Information Notices

The Commissioner may serve an **information notice** on a data controller in response to receiving a request for assessment in respect of any processing of personal data detailing the information she requires from them. The Commissioner may also serve an information notice of her own volition where she reasonably requires any information to decide whether or not the data controller has complied, or is complying, with the Data Protection Principles.

The notice requires the data controller to provide the Commissioner with such information relating to the request or to compliance with the Principles as is so specified, within a specified period of time.

7.6 Special Information Notices

In circumstances where:-

- a request for an assessment is made; or

- the data controller claims the special purposes exemption (as to which see Chapter 5) in any proceedings **and** where the Commissioner has reasonable grounds for suspecting that the personal data to which the proceedings relate,

  - are not being processed only for the special purposes, or

  - are not being processed with a view to the publication by any person of any journalistic, literary or artistic material which has not been previously published by the data controller,

  the Commissioner may serve the data controller with a **special information notice** for the purposes of ascertaining whether or not:-

  a) the personal data are being processed only for the special purposes, or

b) the personal data are being processed with a view to the publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller.

7.7 Right of Appeal from a Notice

A person on whom an **enforcement notice**, or **information notice** or a **special information notice** has been served may appeal to the Information Tribunal against the notice. Detailed rules in relation to the Appeals procedure can be found in The Data Protection Tribunal (Enforcement Appeals) Rules 2000 (S.I. No. 189).

7.8 Failure to Comply with a Notice

Failure to comply with an **enforcement notice**, an **information notice** or a **special information** notice is an offence unless the person charged is able to show that they exercised all due diligence to comply with the notice.

It is also an offence for someone to make a statement which they know to be false in a material respect, or recklessly to make a statement which is false in a material respect, in purported compliance with an information notice or a special information notice.

(See Chapter 9 for further information relating to offences under the Act).

7.9 Provision of Assistance by the Commissioner in cases involving processing for the special purposes (section 53)

Where proceedings relate to personal data processed for the special purposes, the Act enables the Commissioner to provide assistance on application and in appropriate cases, to individuals who are a party (actual or prospective) to such proceedings relating to specified provisions of the Act. These provisions are subject access rights, right to prevent processing, rights in relation to automated decision-taking, rights to rectification, etc., and right to compensation. The Act specifies that such assistance is only available at the Commissioner's discretion.

The Commissioner has a wide discretion as to whether or not and, if so, to what extent she will provide assistance, which would be in terms of legal advice and/or representation and/or financial assistance in relation to the proceedings. However, such assistance may only be given if, in the Commissioner's opinion, the case involves a matter of substantial public importance. This expression is not defined in the Act. It will be for the Commissioner to decide on the particular facts of each case.

7.10 Preliminary Assessment of Assessable Processing

The Act also provides for the Commissioner to make a preliminary assessment as to whether particular types of processing are likely to comply with the provisions of the Act in the case of processing likely:-

- to cause substantial damage or substantial distress to data subjects, or
- otherwise significantly to prejudice the rights and freedoms of data subjects.

Such types of processing (termed "**assessable processing**" in the Act) are to be determined by the Secretary of State by order. However, although a Home Office Consultation Paper dated August 1998 suggested three possible categories of processing which might become subject to preliminary assessment either generally or in certain areas, no order has been made to date.

A preliminary assessment would take place upon the Commissioner receiving notification from a data controller in accordance with section 18 of the Act. This would delay the data controller from commencing assessable processing. The Commissioner would be unable to prevent assessable processing commencing after prescribed time limits had expired notwithstanding that her preliminary assessment had been unfavourable. The Commissioner could only act to prohibit the processing once the assessable processing had commenced.

7.11 Powers of Entry and Inspection

If there are reasonable grounds for suspecting that an offence has been or is being committed under the Act or that any of the Data Protection Principles have been or are being contravened, the Commissioner may apply to a circuit judge for a warrant to enter and search premises on which it is suspected that evidence of the offence or contravention of the Principles is to be found. (Schedule 9).

Before issuing a warrant the judge will need to be satisfied that there are reasonable grounds for the Commissioner's suspicion **and** that:-

a) the Commissioner has already demanded access to the premises by giving seven days written notice to the occupier, and

b) access was demanded at a reasonable hour and was unreasonably refused **or,**

c) although entry to the premises was granted, the occupier unreasonably refused to comply with a request by the Commissioner (including the Commissioner's officers or staff) to allow her to do any of the things mentioned in the paragraph below, and

d) the Commissioner has notified the occupier of the application for the warrant and that the occupier has had an opportunity of being heard by the judge as to whether or not the warrant should be issued.

However, if the judge is satisfied that the case is urgent or that giving notice would defeat the object of the entry, the judge may issue the warrant without notice having been given to the occupier.

The warrant will authorise the Commissioner or any of the Commissioner's officers or staff:-

- to enter and search the specified premises at any time within seven days of the date of the warrant,

- to inspect, examine, operate and test any equipment found there which is used or intended to be used for the processing of personal data, and

- to inspect and seize any documents or other material found there which may be evidence of an offence or contravention of the Principles.

A judge shall not issue a warrant relating to personal data processed for the special purposes unless a determination has been made by the Commissioner whether such data falls within the special purposes exemption (see Chapter 5, at paragraph 5.6).

The powers of inspection and seizure are not exercisable in relation to personal data which are exempt from the Act by virtue of the National Security exemption (see Chapter 5 at paragraph 5.2).

Communications made for the purpose of proceedings under the Act between a professional legal adviser and his\her client are also exempt from inspection and seizure.

It is a criminal offence, triable only in the Magistrates Court, or the Sheriff Court of Scotland :-

- intentionally to obstruct a person in the execution of a warrant, or

- to fail, without reasonable excuse, to give anyone executing a warrant such help as may reasonably be required to execute the warrant.

On conviction an offender is liable to a maximum fine of £5,000.

In Scotland warrants to enter and search premises in this context are issued by the sheriff and in Northern Ireland by a county court judge (see Chapter 9).

Chapter 8: Notification

Introduction

The 1984 Act established the Data Protection Register and the system of registration maintained by the Registrar. The Act introduced a new system of notification which replaced the registration scheme.

Notification is the process by which a data controller informs the Commissioner of certain details about the processing of personal data carried out by that data controller. Those details are used by the Commissioner to make an entry describing the processing in a register which is available to the public for inspection.

The principal purpose of having notification and the public register is transparency or openness. The public should know or should be able to find out who is carrying out processing of personal data and other information about the processing, such as, for what purposes the processing is carried out. The Act places obligations on data controllers in order to achieve transparency.

Notification, therefore, serves the interests of data controllers in providing a mechanism for them to publicise details of their processing activities and also serves the interests of data subjects in assisting them to understand how personal data are being processed by data controllers.

There is a two-tiered notification fee. The two-tiered structure is based on an organisation's size and turnover. A data controller will need to assess which tier they fall in and hence the fee they are required to pay. The fee for tier 1 is £35 and the fee for tier 2 is £500. More information on tiered fees can be found in our guide 'Notification Fee Changes – what you need to know'. (link to booklet) If a person requires a certified copy of the particulars contained in any entry made in the register, the fee payable to the Commissioner is £2.

This Chapter does not provide practical advice as to how to notify. Such advice can be found in the Notification Handbook (available from the Commissioner's Office or via the website).

8.1 Transition

8.1.1 Schedule 14 of the Act deals with the transition from registration to notification. The Data Protection (Notification and Notification Fees) Regulations 2000 (S.I. No.1088) (the "Regulations") sets out a number of arrangements by which the data controller notifies under Part III of the Act.

8.1.2 Anyone who, prior to commencement of the notification regime ("commencement"), was registered as a data user under the 1984 Act (including anyone who was treated as being registered because of a pending application or appeal against refusal of registration), is exempt from the prohibition against processing personal data without notification which is contained in Section 17(1) of the Act (see paragraph 8.5 below). This Act provides that this exemption lasts until the end of the registration period or the date upon which a voluntary notification is made, whichever occurs first. This provision has been amended by paragraph 8 of Schedule 6 to the FoIA, which provides that the transitional exemption from notification contained in paragraph 2 of Schedule 14 to the Act is extended to the end of the registration period, whether or not it ends after 24th October 2001. All exempted persons will be deemed to have notified until the end of the registration period.

8.1.3 Once the transitional exemption from notification ceases to apply, data controllers must notify in accordance with the Act and with the Regulations.

8.1.4 Notwithstanding the exemption from notification afforded to existing registered data users, the Act provides for voluntary notification during the transitional period by data controllers who would otherwise be exempt. If a data controller chooses to notify during the transitional period they will lose their entitlement to exemption from the prohibition against processing personal data without notification.

8.2 Information to be provided

8.2.1 The primary element of every notification and register entry will be what are termed in the Act as "the registrable particulars". These are, in relation to a data controller:-

a) his name and address,

b) if he has nominated a representative, the name and address of the representative,

c) a description of the personal data being/to be processed and of the category(ies) of data subject to which they relate,

d) a description of the purposes(s) for which the data are being/are to be processed,

e) a description of any recipient(s) to whom the data controller intends or may wish to disclose the data,

f) the name or a description of any countries or territories outside the European Economic Area to which the data controller transfers or intends or may wish to transfer the data,

g) where the personal data are of a type which is exempt from the prohibition against processing personal data without notification (see paragraph 8.3) and where the notification does not extend to such data, a statement of that fact.

8.2.3 When a notification is made by a data controller he must also provide, in addition to the registrable particulars, a general description of the security measures taken to protect the personal data; this information will not appear on the register.

8.3 Exceptions to the notification regime

8.3.1 Two important exceptions to the notification requirements are:-

Except where "the assessable processing provisions" apply to the processing (see paragraph 8.4) there is no requirement for a register entry in cases where the **only** personal data held fall into either of these exempt categories. Where data controllers are required to notify in respect of personal data which do not fall into the exempt categories, they are only required to make a statement of the fact that they hold exempt data (if they do), if the notification does not extend to those data (see paragraph 8.2.1(g) above).

8.3.2 There is also a specific exemption from the notification regime for any processing where the sole purpose is the maintenance of a public register. (Section17(4))

8.3.3 The Regulations provide that exempt processing operations also include staff administration, advertising, marketing and public relations, accounts and record keeping and certain processing operations carried out by non-profit making organisations.

8.3.4 Those data controllers who are exempt from the prohibition against processing personal data without notification are nevertheless under a duty to provide the same information as is contained in paragraphs (a) to (f) of the registrable particulars, (see paragraph 8.2.1 above), free of charge, within 21 days of receiving a written request (a "registrable particulars request") from any person. (Section 24).

For further information see the Notification Handbook available from the Commissioner's office or from the Commissioner's website.

8.4 "Assessable processing" provisions

8.4.1 The Act (section 22) introduces "assessable processing" provisions in respect of any processing of a description specified in an order made by the Secretary of State, as being particularly likely to cause substantial damage or substantial distress to data subjects or otherwise significantly to prejudice the rights and freedoms of data subjects. No order has yet been made specifying the types of processing which will be subject to these provisions.

(For further detail, see Chapter 7 on the Powers and Duties of the Commissioner).

8.4.2 The Commissioner is obliged to consider whether any processing that is the subject of a notification is assessable processing and, if so, whether or not the assessable processing is likely to comply with the provisions of the Act. Upon making a notification to the Commissioner involving assessable processing, the data controller is initially subject to an absolute prohibition on assessable processing (see paragraph 8.5.3 below).

8.5 Offences relating to notification

8.5.1 It is an offence to process personal data without notification unless:-

- the personal data fall within either of the national security or domestic purposes exemptions,

- the personal data are exempt under the transitional exemptions,

- the personal data fall within the "relevant filing system"/ "accessible record" or public register exceptions referred to above,

- the processing operation falls within the exemptions referred to in the Regulations

- the processing is of a description which notification regulations provide is exempt from the requirements to notify on the ground that it is unlikely to prejudice the rights and freedoms of data subjects. No such provision was included in the Regulations.

This is a strict liability offence. (See Chapter 9).

8.5.2 It will also be an offence for a person to fail to notify the Commissioner of changes to the register entry. The Regulations provided that such notification must be given as soon as practicable and in any event within a period of 28 days from the date upon which the entry becomes inaccurate or incomplete as a statement of the data controller's registrable particulars or in respect of measures taken with regard to compliance with the Seventh Data Protection Principle. A defence is available to persons charged with such an offence if they can show that they exercised all due diligence to comply with the duty.

8.5.3 Where the "assessable processing" provisions apply (see paragraph 8.4 above), no processing shall take place unless:-

- the data controller has given a notification to the Commissioner, **and**

- the 28 day period from receipt by the Commissioner of notification has expired unless, before that time, the data controller has received a notice from the Commissioner stating the extent to which the Commissioner is of the opinion that the proposed processing is likely or unlikely to comply with the provisions of the Act ("assessable processing notice").

This is a strict liability offence. (See Chapter 9).

8.5.4 Although there will be instances where it will **not** be a criminal offence to process without notifying the Commissioner (see paragraph 8.3 above), the data controller should nevertheless note the requirement to comply with a "registrable particulars request" (see paragraph 8.3.4 above), and that it is a criminal offence to fail to comply with such a request. A defence is available to a data controller charged with this offence, where he can show that he exercised all due diligence to comply with this duty.

Chapter 9: Offences Under the Act

9.1 Who can bring proceedings?

In England and Wales proceedings for a criminal offence under the Act can be commenced by the Commissioner or by or with the consent of the Director of Public Prosecutions

In Scotland criminal proceedings will be brought by the Procurator Fiscal.

In Northern Ireland proceedings for an offence under the Act can be begun by the Commissioner or by or with the consent of the Director of Public Prosecutions for Northern Ireland.

9.2 In which Court can proceedings be brought and what are the penalties?

A person accused of the offences of:

- intentionally obstructing a person in the execution of a search warrant issued in accordance with the Act; or

- failing without reasonable excuse to give any person executing such a warrant such assistance as he may reasonably require for the execution of the warrant

cannot elect a Crown Court trial and will be tried in the Magistrates' Court, or the Sheriff Court of Scotland.

If found guilty of this offence the Court can impose a fine not exceeding level 5 on the standard scale of fines contained in The Criminal Justice Act 1982 (as amended) and the Criminal Procedure (Scotland) Act 1995. At present this is £5,000.

All the other offences are "either way offences", in other words they can be tried:

- in England or Wales either in the Magistrates' court (summary trial) or the Crown Court (on indictment); or

- in Scotland, on indictment in the Sheriff Court or High Court of Justiciary.

A person found guilty of any of these offences can be sentenced on summary conviction to a fine not exceeding the statutory maximum (currently £5,000), or on conviction on indictment, to an unlimited fine.

The offences of processing without notification, processing before the expiry of the assessable processing time limits, and enforced subject access (see below) are strict liability offences. This means that the data controller may be criminally liable even though he did not intend to commit the offence and did not know he was committing an offence.

On conviction of an offender, the Court may order any data apparently connected with the crime to be forfeited, destroyed or erased. Anyone other than the offender

who claims to own the material may apply to the Court that such an order should not be made.

9.3 Personal liability where the data controller is a company or corporate body (section 61)

If a company or other corporation commits a criminal offence under the Act, any director, manager, secretary or similar officer or someone purporting to act in any such capacity is personally guilty of the offence in addition to the corporate body if:-

- the offence was committed with his/her consent or connivance; or
- the offence is attributable to any neglect on his/her part.

Where the affairs of a corporate body are managed by its members, any member who exercises the functions of management as if he were a director can also be guilty of the offence that results from any of his/her acts or omissions.

Where an offence under the Act has been committed by a Scottish partnership and the contravention in question is proved to have occurred with the consent or connivance of, or to be attributable to any neglect on the part of, a partner, he/she, as well as the partnership, shall be guilty of that offence and shall be liable to be proceeded against and punished accordingly.

Government departments are not liable to prosecution under the Act but individual civil servants may be prosecuted if they personally are believed to be guilty of an offence under section 55 (the unlawful obtaining or disclosure of personal data), or obstructing or failing to assist in the execution of a warrant issued in accordance with the Act (Schedule 9 paragraph 12).

9.4 The Offences

This publication has already dealt elsewhere with the following offences under the Act:-

(a) processing without notification (section 21(1)- see Chapter 8),

(b) failure to notify the Commissioner of changes to the notification register entry (section 21(2) – see Chapter 8),

(c) processing before expiry of assessable processing time limits or receipt of assessable processing notice within such time (section 22(6) – see Chapter 8),

(d) failure to comply with written request for particulars (section 24 – see Chapter 8),

(e) failure to comply with an enforcement notice/information notice/special information notice (section 47(1) – see Chapter 7),

(f) knowingly or recklessly making a false statement in compliance with an information notice or special information notice (section 47(2) – see Chapter 7), and

(g) intentional obstruction of, or failure to give reasonable assistance in, execution of a warrant (Schedule 9, paragraph 12 – see Chapter 7).

9.5 Unlawful Obtaining etc., of Personal Data (section 55(1))

It is an offence for a person, knowingly or recklessly, without the consent of the data controller, to:-

- obtain or disclose personal data or the information contained in personal data, or

- procure the disclosure to another person of the information contained in personal data.

The Act provides specific exceptions to liability for this offence where the person can show:

- that the obtaining, disclosing or procuring:

  - was necessary to prevent or detect crime; or
  - was required or authorised by law,

- that he acted in the reasonable belief that he had the legal right to obtain, disclose or procure the disclosure;

- that he acted in the reasonable belief that the data controller would have consented to the obtaining, disclosing or procuring if the data controller had known; or

- that in the particular circumstances the obtaining, disclosing or procuring was justified as being in the public interest.

A person will not be guilty of this offence if the personal data in question fall within the national security exemption at section 28 (see Chapter 5).

It should be noted that an offence under this section, cannot be committed by a data controller in respect of data of which he is the data controller. However, a data controller who discloses personal data of which he is the data controller may breach the First Principle if the disclosure is unfair or unlawful.

Where employees of a data controller organisation have authority to obtain and disclose personal data in the course of their employment (for example bank employees who can access customer accounts for bank purposes), they will commit these offences if they use their position to obtain, disclose, or procure disclosure of personal data for their own purposes.

9.6 Unlawful Selling of Personal Data (sections 55(4) and (5))

If a person has obtained personal data in contravention of section 55(1) above, it is an offence to sell or offer to sell personal data.

It is also an offence to offer to sell personal data which the person subsequently obtains in contravention of section 55(1).

An advertisement indicating that personal data are or may be for sale is an offer to sell the data.

Personal data includes information extracted from personal data for the purposes of these offences.

A person will not be guilty of this offence if the personal data in question fall within the national security exemption at section 28 (see Chapter 5).

9.7 Enforced Subject Access (section 56)

Unless one of the statutory exceptions apply it is an offence for a person to require another person or a third party –

- to supply him with a relevant record (see below); or
- to produce a relevant record to him;

in connection with:-

- the recruitment of that other person as an employee;
- the continued employment of that other person;
- any contract for the provision of services to him by that other person; or
- where a person is concerned with providing (for payment or not) goods, facilities or services to the public or a section of the public, as a condition of providing or offering to provide any goods, facilities or services to that other person.

The statutory exceptions to liability for such offences are:-

a) that the imposition of the requirement was required or authorised by law; or

b) that in the particular circumstances the imposition of the requirements was justified as being in the public interest.

The Act provides that the imposition of the requirement is not to be regarded as being justified in the public interest on the ground that it would assist in the prevention or detection of crime.

The term "relevant record" is defined in section 56 of the Act by reference to a table which lists data controllers and the subject matter of subject access requests that may be made to them by data subjects. Generally, the term relates to records of cautions, criminal convictions and to certain social security records relating to the data subject.

Section 56 will not come into force until the Criminal Records Bureau is in operation. This is unlikely to happen until 2002. However, the practice of requiring subject access may still breach other provisions of the Act, or the Human Rights Act 1998 or the Rehabilitation of Offenders Act 1974.

9.8 Unlawful Disclosure of Information by Commissioner/Staff/Agent (section 59)

This offence applies to the Commissioner, a member of the Commissioner's staff or an agent of the Commissioner, past or present. Below, these are referred to collectively as the "Supervisory Authority".

It is an offence for the Supervisory Authority knowingly or recklessly to disclose information which –

- has been obtained by, or provided to, the Commissioner under or for the purposes of the Act,
- relates to an identified or identifiable individual or business, and
- is not at the time of the disclosure, and has not previously been, available to the public from other sources,

unless the disclosure is made with lawful authority.

A disclosure of information is made with lawful authority in these circumstances only if, and to the extent that –

- the disclosure is made with the consent of the individual or the person carrying on the business,
- the information was provided for the purpose of its being made available to the public under any provision of the Act,
- the disclosure is made for the purposes of, and is necessary for, the discharge of any functions under the Act, or any Community obligation,
- the disclosure is made for the purposes of any criminal or civil proceedings, or
- the disclosure is necessary in the public interest, taking account of the rights and freedoms or legitimate interest of any person.

ANNEX

SUBORDINATE LEGISLATION

The Telecommunications (Data Protection and Privacy) Regulations 1999 Statutory Instrument 1999 No. 2093

The Data Protection Act 1998 (Commencement) Order 2000
Statutory Instrument 2000 No. 183 (C.4)

The Data Protection (Corporate Finance Exemption) Order 2000
Statutory Instrument 2000 No. 184

The Data Protection (Conditions under Paragraph 3 of Part II of Schedule 1) Order 2000 Statutory Instrument 2000 No. 185

The Data Protection (Functions of Designated Authority) Order 2000
Statutory Instrument 2000 No. 186

The Data Protection (Fees under section 19(7)) Regulations 2000
Statutory Instrument 2000 No. 187

The Data Protection (Notification and Notification Fees) Regulations 2000
Statutory Instrument 2000 No. 188

The Data Protection Tribunal (Enforcement Appeals) Rules 2000
Statutory Instrument 2000 No. 189

The Data Protection (International Co-operation) Order 2000
Statutory Instrument 2000 No. 190

The Data Protection (Subject Access) (Fees and Miscellaneous Provisions) Regulations 2000 Statutory Instrument 2000 No. 191

The Data Protection Tribunal (National Security Appeals) Rules 2000
Statutory Instrument 2000 No. 206

The Data Protection (Subject Access Modification) (Health) Order 2000
Statutory Instrument 2000 No. 413

The Data Protection (Subject Access Modification) (Education) Order 2000
Statutory Instrument 2000 No. 414

The Data Protection (Subject Access Modification) (Social Work) Order 2000 Statutory Instrument 2000 No. 415

The Data Protection (Crown Appointments) Order 2000
Statutory Instrument 2000 No. 416

The Data Protection (Processing of Sensitive Personal Data) Order 2000
Statutory Instrument 2000 No. 417

The Data Protection (Designated Codes of Practice) Order 2000
Statutory Instrument 2000 No. 418 – REVOKED as of 27th July 2000 by:-

The Data Protection (Designated Codes of Practice) (No.2) Order 2000
Statutory Instrument 2000 No. 1864

The Data Protection (Miscellaneous Subject Access Exemptions) Order 2000
Statutory Instrument 2000 No. 419

The Data Protection (Miscellaneous Subject Access Exemptions)
(Amendment) Order 2000 Statutory Instrument 2000 No. 1865

The Data Protection (Subject Access) (Fees and Miscellaneous Provisions)
(Amendment) Regulations 2001
Statutory Instrument 2001 No. 3223

Information Commissioner
Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF Telephone:01625 545 700 Facsimile: 01625 524510
e-mail: data@dataprotection.gov.uk Website: www.dataprotection.gov.uk