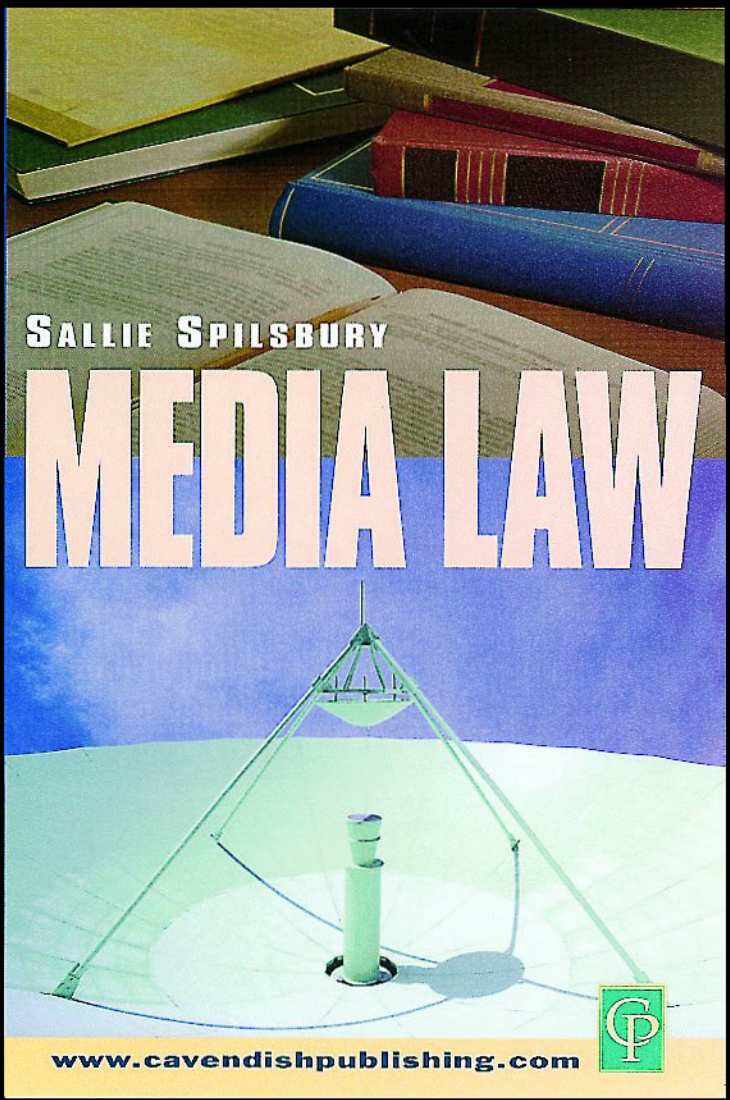
SALLIE SPILSBURY
MEDIA LAW
www.cavendishpublishing.com

DATA PROTECTION AND THE MEDIA

THE DATA PROTECTION ACT 1998

The Data Protection Act 1998 ('the Act') implements the EU Data Protection Directive,[1] which had the twin objectives of: (a) harmonising data protection laws throughout the EC; and (b) protecting the privacy of individuals in relation to the processing of personal data. The preamble to the Act describes it as a measure to provide for 'the regulation of the processing of information relating to individuals, including the obtaining, holding, use or disclosure of such information'. The Act came into force on 1 March 2000, replacing the Data Protection Act 1984. It contains transitional provisions for data processing which was under way prior to 24 October 1998. Processing which postdates 24 October 1998 will be subject to the Act's provisions.

The media makes considerable use of information about individuals. Under the scheme of the Act, this information may be classed as data if it is held on computer or in a structured paper filing system. The Act provides that any use which is made of personal data must be in accordance with the provisions of the Act. The Act contains eight data protection principles with which data controllers must comply.

In addition to the data protection principles, the Act confers legal rights on individuals in respect of personal data held about them. In summary, the individual has the right to control the use to which the data is put and to know the source of the information.

From the above, it is clear that the provisions of the Act are incompatible with the majority of media reporting. In recognition of this fact, the Act contains an important exemption for the media which will apply in the circumstances set out in the Act. The exemption is considered towards the end of the chapter.

Terminology

In order to understand the provisions of the Act, it is necessary to familiarise oneself with its terminology. The Act contains basic interpretative provisions in s 1(1). The key concepts are defined as follows.

1 Directive (95/45/EC) on the protection of individuals, with regard to the processing of personal data and the free movement of such data.

Data – it is important to realise that the Act operates by reference to the way that the information is processed rather than by reference to the content of the information itself.

The Act defines 'data' as 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 of a relevant filing system or with the intention that it should form part of a relevant filing system; or

(d) does not fall within the above provisions but forms part of an accessible record (the meaning of this phrase is considered below).

Relevant filing system – includes paper-based material. It means any set of information relating to individuals to the extent that 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.

The information may be stored in a variety of ways, such as in paper files, on microfiche or card index systems.

The mere fact that data is stored in a file will not automatically make it part of a relevant filing system. The definition of relevant filing system does *not* cover unstructured files. The Commissioner (see below for an explanation of the role of the Commissioner) has given general guidance as to what might fall to be classed as a relevant filing system, although she has emphasised that the final decision in a particular case would lie with the courts. The guidance indicates the following:

- there must be a set of information about individuals. This suggests a grouping of things together by reference to a distinct identifier, for example, a set of information about customers;
- the set of information need not be physically grouped together in files. It may be grouped together in other ways, for example, by prefix codes;
- the set of information does not need to be maintained centrally by the data controller. It may, for example, be dispersed over different branch offices;
- the set must be structured, for example, by reference to the individuals themselves or by reference to criteria relating to the individuals, such as their credit history or their membership of particular organisations;
- the structuring has to enable specific information about a particular individual to be readily accessible. What amounts to specific information will be a question of fact in every case;

- the act does not define 'readily accessible'. The Commissioner points out that, in its ordinary meaning, the phrase means 'information capable of being reached easily by virtue of the structure'. The Commissioner suggests that information referenced to individuals or criteria relating to individuals will be caught by the Act if it is 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.

Information which forms part of a health record, an educational record recorded by a local education authority school or a special school, a local authority housing record or a local authority social services record will also be classed as 'data' for the purposes of the Act, whether or not it meets the above requirements. These types of record are known as 'accessible records'.

Personal data are particular types of data in respect of which the subject has private rights under the Act.[2] These rights are discussed below.

Personal data are data about a living individual who can be identified:

(a) from those data; or

(b) from those data and other information which is in the possession of, or is likely to come into the possession of, the data controller.

Personal data is not confined to factual information. Significantly, it includes any expression of opinion about an individual and any indication of the intentions of the data controller (or any other person) in respect of the individual.

Data controller means a person who determines the purposes for which and the manner in which any personal data are, or are to be, processed.

Data processor means a person who processes the data on behalf of the data controller (other than an employee of the data controller).

Data subject means an individual who is the subject of personal data.

Processing means obtaining, recording or holding information or data or carrying out any operation or set of operations on the information or data including:

(a) organisation, adaptation or alteration of the information or data;

(b) retrieval, consultation or use of the information or data;

(c) disclosure of the information or data by transmission, dissemination or otherwise making available; or

(d) alignment, combination, blocking, erasure or destruction of the information or data.

2 Remember that in order to be classed as data, the information must satisfy the requirements of the Data Protection Act 1998, s 1(1).

This is clearly a wide definition. It extends to pretty much everything which can be carried out in relation to data. So far as the media are concerned, it could extend to journalistic enquiries which lead to the obtaining of information which is then stored on computer or in a relevant filing system. It could also extend to publication or amendment of that data or any other kind of use.

The processing of data will not be lawful unless the data protection principles contained in the Act are complied with. The principles are considered below.

The Data Protection Commissioner

The Data Protection Commissioner has powers to enforce the provisions of the Act. Her detailed powers are outside the scope of this book. Her duties include the promotion of good practice by data controllers and, in particular, the promotion of the observance of the Act's requirements. Reference is made below to a number of guidance documents which the Commissioner has issued in relation to the Act.

The data protection principles

The data protection principles apply to all personal data processed by data controllers.

The principles are set out in Pt 1 of Sched 1 to the Act – Pt 2 of Sched 1 contains interpretation provisions which clarify and supplement the principles.

The principles are as follows.

The first data protection principle

1 Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless at least one of the conditions set out in Sched 2 is met.

Processed fairly and lawfully

The first principle requires that the data must be processed fairly and lawfully.

The Act gives guidance in Part 2 of Sched 1 ('the fair processing code') about the meaning of fair processing.[3] Compliance with the fair processing code will not, in itself, ensure that processing is fair, but if the code is complied with there will be a presumption that the processing was done fairly unless there is evidence to the contrary.

The fair processing code

- The Act indicates that in determining whether data is processed fairly, regard should be had to the method by which data are obtained, including in particular whether any person from whom they are obtained is deceived or misled as to the purpose or purposes for which they are to be processed.
- Data are generally to be treated as being obtained fairly if they consist of information obtained from a person who is *authorised* by or under any enactment to supply it, or is *required* to supply it by or under any enactment.

Providing information to the data subject

Personal data are not to be treated as processed fairly, unless:

(a) in the case of data obtained direct from the data subject, the data controller ensures so far as practicable that the data subject has, is provided with, or has made readily available to him the information set out below;

(b) in any other case, the data controller ensures so far as is practicable that before the relevant time (relevant time is defined below) or as soon as practicable after that time the data subject has or is provided with or has made readily available to him the information set out below.

The information which must be supplied to the data subject

The information required is as follows:

- the identity of the data controller;
- if the data controller has nominated a representative, the identity of that representative;
- the purpose or purposes for which the data are intended to be processed; and
- any further information which is necessary, having regard to 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.

3 The fair processing code – see below.

The relevant time

Where the data controller has obtained data from someone other than the data subject, the fair processing information must be given or made readily available to the data subject at the 'relevant time'. The relevant time means the time when the data controller first processes the data, or in a case where disclosure of the data by the data controller to a third party within a reasonable period is envisaged:

- if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed;
- if, within that period, the data controller becomes, or ought to become, aware that the data are unlikely to be disclosed to such a person within that period, the time when the data controller does become, or ought to become, so aware; or
- in any other case, the end of the reasonable period.

Exceptions to the duty to inform under the fair processing code

The fair processing code provides that the duty to provide the data subject with the information set out above will not apply where it would involve a disproportionate effort on the part of the data controller. This term is not defined in the code. The Commissioner has indicated that she will take into account the following factors in deciding whether informing the data subject would involve a disproportionate effort:[4]

- the cost to the data controller in providing the information, for example, postage, employee time;
- the length of time it would take to provide the information;
- how easy or difficult it would be for the data controller to provide the information.

All these considerations should be weighed against the benefit to the data controller of processing the information *and* the extent to which the withholding of the information may be prejudicial to the data subject.

A second exemption from the duty to inform applies where the recording of the information contained in the data or the disclosure of the information by the data controller is necessary for compliance with any legal obligation to which the data controller is subject (other than an obligation imposed by contract).

4 *Data Protection Act 1998 – An Introduction*, October 1988, available from the Data Protection Registrar.

In addition to providing that data must be processed fairly and lawfully, the first data protection principle provides that at least one of the conditions set out in Sched 2 to the Act must be met.

Failure to meet at least one of the conditions will mean that the processing will be in breach of the first data protection principle.

The Sched 2 conditions

At least one of these conditions has to be met:

1 The data subject has given consent to the processing.

The Act does not define what is meant by 'consent'. However, the directive which the Act is intended to implement defined '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 Commissioner has indicated[5] that 'signifies' entails active communication between the relevant parties and that consent cannot be inferred. The Commissioner takes the view that a blanket consent to the processing of personal data is unlikely to be sufficient (particularly in the case of 'sensitive personal data' – see below). The more ambiguous the consent, the more likely that there will be questions about its validity or existence. The data subject may withdraw consent.

2 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.

3 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 records to a hospital casualty department which is treating the data subject after a serious road accident.

4 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; or

5 *Data Protection Act 1998 – An Introduction*, October 1988, available from the Data Protection Registrar.

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

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

The Sched 2 grounds and sensitive personal data

The Act introduces a category of 'sensitive personal data'.[6] The Act contains additional conditions which must be satisfied before sensitive data can be processed. Sensitive personal data consists of information about:

- the racial or ethnic origin of the data subject;
- their political opinions;
- their religious beliefs or other beliefs of a similar nature;
- their physical or mental health or condition;
- whether they are a member of a trade union;
- their sexual life;
- the commission or alleged commission by them of any offence; or
- any proceedings for any offence committed or alleged to have been committed by them, the disposal of such proceedings or the sentence of any court in such proceedings.

Where the data is sensitive personal data, at least one of the additional conditions listed below must be satisfied *in addition to* at least one of the general Sched 2 conditions listed above. The special conditions are as follows:

1 The data subject has given their explicit consent to the processing of the personal data.

'Explicit' is not defined. The Commissioner has indicated that the word suggests that the consent of the data subject must be absolutely clear, covering the specific detail of the processing, the purposes of the processing and any specific aspects of the processing which may affect the individual.

2 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.

6 Defined in the Data Protection Act 1998, s 2.

The Secretary of State may by order specify cases where this condition is either excluded altogether or only satisfied upon the satisfaction of further conditions.

3 The processing is necessary:

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

- consent cannot be given by or on behalf of the data subject; or
- 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.

4 The processing:

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

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

(c) relates only to individuals who either are members of the body or association or 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.

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

6 The processing:

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

(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.

7 (1) The processing is necessary:

(a) for the administration of justice;

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

(c) for the exercise of any functions of the Crown, a minister of the Crown or a Government department.

(2) The Secretary of State may by order specify cases where this condition is either excluded altogether or only satisfied upon the satisfaction of further conditions.

8 The processing is necessary for medical purposes and is undertaken by:

(a) a health professional; or

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

9 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 by order specify circumstances in which such processing is or is not to be taken to be carried out with appropriate safeguards for the rights and freedoms of data subjects.

10 The personal data are processed in circumstances specified in an order made by the Secretary of State.

So far, we have considered the first data protection principle with which the data controller must comply when processing personal data. The other seven principles which also must be complied with will now be considered.

The second data protection 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.

The purpose or purposes for which personal data are obtained may, in particular, be specified:

(a) in a notice given by the data controller to the data subject; or

(b) in a notification given to the Commissioner.

The third principle

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

The fourth principle

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

The fifth principle

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

The sixth principle

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

The 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 measures taken must ensure a level of security appropriate to:

(a) the harm that might result from any unauthorised or unlawful processing or accidental loss, destruction or damage; and

(b) the nature of the data to be protected having regard to the state of technological development and the cost of implementing any measures.

The data controller must take reasonable steps to ensure the reliability of any employees who have access to the personal data.

Where the processing is carried out by a data processor on behalf of the data controller, the data controller must choose a data processor providing sufficient guarantees in respect of the technical and organisational security measures governing the process and the controller must take reasonable steps to ensure compliance with those measures. The data controller will not be regarded as complying with the seventh principle unless the processing is carried out under contract made or evidenced in writing under which the data processor is to act only on instructions from the data controller. The contract

must also require the data processor to comply with obligations equivalent to those imposed on the data controller under the seventh principle.

The 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 for the rights and freedoms of data subjects in relation to the processing of personal data.

An adequate level of protection is one which is adequate in all the circumstances of the case, having regard 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.

The rights of the data subject in relation to the processing of personal data

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

- right of subject access (s 7).

  The individual is entitled, upon making a request in writing and paying a fee to the relevant data controller, to be told by that data controller whether they or someone on their behalf is processing the individual's data and, if so, to be given a description of the personal data, the purposes for which they are being processed and the persons to whom the data are or may be disclosed.

  The individual is also entitled to be told in an intelligible manner all the information which forms any such data *and any information as to the source of the data*. The disclosure of the identity of their sources is something which journalists are at great pains to prevent. Indeed, journalists are

placed under an obligation not to make such disclosures by the code of practice produced by the National Union of Journalists and by the terms of the code which is enforced by the Press Complaints Commission.[7]

Where a decision significantly affecting a data subject is or is likely to be made about them by fully automated means for the purpose of evaluating matters such as their performance at work or their creditworthiness, the data subject is entitled to know the logic involved in the decision making process (except where the information in question constitutes a trade secret).

The data controller must not make any amendment or deletion to the data which would not otherwise have been made before it is supplied to the data subject. In particular, the data controller may not alter data to make it more acceptable to the data subject.

The data controller must generally supply the above information within 40 days of receipt of the request and fee.

Special rules apply to the provision of data in circumstances where the information contained in the data will enable another individual to be identified.

If the data subject believes that the data controller has failed to comply it may apply to the court for an order requiring compliance;

- the right to prevent processing likely to cause damage or distress (s 10).

  A data subject is entitled to serve on a data controller a written notice (a 'data subject notice') requiring the data controller to cease or not to begin processing personal data concerning the data subject where such processing is likely to cause unwarranted substantial damage or substantial distress to the data subject or to another.

  Where the data subject believes that a data controller has not complied with a data subject notice, it may apply to the court for an order ensuring compliance;

- the right to prevent processing for purposes of direct marketing (s 11).

  'Direct marketing' means the communication by whatever means of any advertising or marketing material which is directed to particular individuals;

- rights in relation to automated decision making (s 12).

  These rights are beyond the scope of this book. Automated decision making includes matters such as evaluating matters relating to the data subject such as their creditworthiness;

7 This is considered further in Chapter 11.

- the right to compensation (s 13).

  An individual who suffers damage or damage and distress (but not simply distress) as a result of any contravention of the provisions of the Act is entitled to compensation where the data controller cannot prove that they have taken such care as was reasonable in the circumstances to comply with the relevant requirement.

  Where the processing of the data is for a 'special purpose',[8] damages can be awarded for distress caused to the data subject, without the need to establish any other type of damage. The special purposes are considered below. *They include the use of data for journalistic purposes*;

- rectification, blocking, erasure and destruction (s 14).

  A data subject may apply to the court for an order requiring the data controller to rectify, block, erase or destroy data relating to them which is incorrect or misleading. This right extends to an expression of opinion which is based on factually inaccurate data. The court may also direct that the data controller notify third parties to whom the data has been disclosed of any rectification, etc, where it is reasonably practicable to do so;

- requests for assessment.[9]

Any person may ask the Commissioner to assess whether it is likely that any processing of personal data has been or is being carried out in compliance with the Act. The Commissioner has information gathering powers in relation to this exercise. Any person who is, or believes themselves to be, directly affected by any processing of personal data can make the request.

Exemptions under the Act

The Act provides for a number of exemptions to the above principles. The *key exemption* for the media is the special purposes exemption.[10]

Special purposes are defined to include any one or more of the following:

- journalism;
- artistic purposes;
- literary purposes.[11]

None of these purposes is defined in the Act. Will the mere fact that the data is for publication by the media mean that it will be deemed to have been

8 Defined in the Data Protection Act 1998, s 4 and discussed further below.

9 *Ibid*, s 42.

10 *Ibid*, s 32.

11 *Ibid*, s 4.

processed for journalistic purposes, or will the media have also to establish that the data is newsworthy or is to be used for reporting current events? This point has to be clarified. It is likely that over time, a body of case law will emerge to define the special purposes with greater precision. The European Court of Human Rights has emphasised the media's role as public watchdogs – media activities which fall within this watchdog role will almost certainly fall within the definition of journalism.

The phrase 'journalistic, literary or artistic works' also appears in s 12 of the Human Rights Act 1998[12] in relation to the grant of relief which might affect freedom of expression. Case law under s 12 might throw help to clarify the material covered by the special purposes exemption.

There are four conditions which must *all* be present before the processing of personal data for any of the above special purposes can qualify for the exemption.[13] They are:

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

In relation to the third of the above criteria (the data controller's reasonable belief that publication would be in the public interest), regard may be had to the data controller's compliance with any relevant industry code designated for these purposes by the Secretary of State. During the passage of the Data Protection Bill through Parliament, reference was expressly made to the PCC Code (the press), the ITC Code (independent television) and the Code of the Broadcasting Standards Commission (all broadcasters). The most relevant provisions of these codes are the privacy provisions, which were set out and considered in Chapter 8. Compliance with the privacy provisions of the codes make it likely that the data controller will be able to demonstrate a reasonable belief that publication of the data is in the public interest (although it will not necessarily be determinative of this question. The Act does not equate reasonable relief to the provisions of the codes. Similarly, non-compliance with the codes ought not to mean that the data controller will be deemed not to be able to show a reasonable belief).

12 Considered in Chapter 1.

13 Data Protection Act 1998, s 32(1).

It is significant that the language used in the Act draws attention to the wider public interest in imparting and receiving information as well as to the public interest in the receipt of the particular information in question.

If the above criteria are not met, the special purposes exemption will not apply and the Act's provisions will apply to regulate the processing of the data.

If *all* the above conditions are met, the exemption will apply to the following provisions of the Act:

- the data protection principles *except* the seventh principle (security measures) which *will continue* to apply;
- the right of subject access and disclosure of sources in s 7;
- the right to prevent processing likely to cause unwarranted damage or distress in s 10;
- rights in relation to automated decision taking in s 12;
- the provisions relating to the right to rectification, blocking, erasure and destruction of inaccurate data in s 14.

Section 32(4) provides that proceedings against a data controller who falls within the special purposes exemption will be stayed if the personal data is being processed only for the special purposes with a view to publication and it has previously been published by the data controller (excluding the 24 hour period prior to the publication of the data). This protection covers proceedings brought before publication of the material and in the immediate 24 hour period following publication. It is intended to provide a safeguard against the provisions of the Act being used as a prior restraint measure to restrain the publication of personal data covered by the special purposes exemption by the media.

Example

X applies to the court for an order under s 10 of the Act to restrain the publication of personal data by the *Daily Tabloid*. X claims that the information is likely to cause him distress.

The publication of the data by the newspaper will be 'processing' for the purpose of the Act, if the information about X falls within the definition of personal data. For example, if it is held in a structured filing system and it would enable X to be identified, X might be able to obtain an order to prevent the publication of the data.

The *Daily Tabloid* can resist the application by demonstrating that the processing of the data falls within the special purposes exemption. It must show that:

- the data is being processed (published) for journalistic purposes only. The more newsworthy the article, the more likely it is that the newspaper will

be able to establish this fact – pending judicial guidance on the meaning of 'journalistic';

- the processing is undertaken with a view to publication of the journalistic material;
- in the reasonable belief of the *Daily Tabloid* the publication would be in the public interest. The newspaper can rely on the nature of the story which it proposes to publish – is it in the public interest? It can also rely on the wider public interest in allowing freedom of expression generally. Any limitation on this freedom must be compatible with the European Convention on Human Rights if it is to be acceptable;[14]
- if the *Daily Tabloid* has complied with the Code of Practice in relation to the data which is enforced by the Press Complaints Commission, that will help the newspaper to establish its reasonable belief;
- in the reasonable belief of the *Daily Tabloid* compliance with the processing requirements Act would be incompatible with the journalistic purpose – for example, agreeing not to publish the data would not be compatible with the news reporting role of the media.

Provided that the *Daily Tabloid* can demonstrate these factors to the satisfaction of the court, X's application under s 10 will be stayed.

The length of the stay

The stay remains in force until the claim is withdrawn or until the Commissioner makes a determination in writing stating either that it appears to her that the data are not being processed for special purposes, or confirming that they 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.[15]

Where the Commissioner makes a determination, she is required to give the data controller notice. There is a right of appeal against her decision to the Data Protection Tribunal and thereafter to the High Court.[16]

14 More detail about this is contained in Chapter 1.

15 Data Protection Act 1998, s 45.

16 *Ibid*, s 48.

A summary of the Commissioner's powers under the provisions of the Act

Assessment

As we have seen, individuals have the right to request the Commissioner for an assessment as to whether the processing of personal data has been or is being or is not being carried out in compliance with the Act.[17]

In addition to her powers of assessment, the Commissioner can issue the following notices under the Act:

- special information notices.[18]

  Where, during an assessment, the data controller claims a special purposes exemption, the Commissioner can serve a special information notice where she 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 publication by any person of any journalistic, literary or artistic material which has not previously been published by the data controller.

  The special information notice can require the controller to provide information to enable her to ascertain whether the special purposes exemption applies.

  There is a right of appeal against a special information notice to the Data Protection Tribunal.

  Material covered by legal professional privilege does not have to be disclosed.

  It is an offence to fail to comply with a special information notice. The offence carries a maximum fine of £5,000 on summary conviction and an unlimited fine on indictment. The controller has a defence if it can show that it exercised all due diligence to comply with the notice;

- information notices.[19]

  If, during the course of an assessment which does not involve the special purposes exemption, the Commissioner requires information from the data controller, the Commissioner may serve an information notice requiring the data controller to provide that information. The consequences of non-compliance with an information notice are the same as not complying with a special information notice;

17 Data Protection Act 1998, s 42.

18 *Ibid*, s 44.

19 *Ibid*, s 43.

- enforcement notices.[20]

  Enforcement notices may be served on a data controller where the Commissioner is satisfied that the controller has contravened or is contravening the Act's provisions. There is a right of appeal against an enforcement notice to the Data Protection Tribunal.

  An enforcement notice may not be served on a data controller with respect to the processing of data for the special purposes without permission from the court.[21] Permission will only be granted where the court is satisfied that the Commissioner has reason to suspect a contravention of the Act which is of substantial public importance. The media should be given notice of the Commissioner's application for permission unless the urgency of the application does not allow notice to be given.

  Failure to comply with an enforcement notice is a criminal offence carrying a maximum fine of £5,000 on summary conviction or an unlimited fine on indictment. The data controller has a defence where it can show that it has exercised all due diligence to comply with the notice.

Powers of entry and inspection[22]

If there are reasonable grounds for suspecting that the data protection principles have or are not being complied with, the Commissioner may apply to the court for a warrant to enter and search premises on which it is suspected that evidence of contravention of the principles is to be found.

No warrant should be issued unless the court is satisfied that there are reasonable grounds for the Commissioner's suspicion and that:

- the Commissioner has already demanded access by giving seven days' notice to the occupier;
- access was demanded at a reasonable hour and was unreasonably refused, or entry was granted but the occupier unreasonably refused to comply with a request of the Commissioner relating to the execution of the warrant; and
- the Commissioner has notified the occupier of the application for the warrant and the occupier has had an opportunity of being heard by the judge as to whether or not the warrant should be issued.

Where the court is satisfied that the case is urgent, or that giving notice would defeat the object of entry (for example, it would lead to destruction of the evidence), the court may issue the warrant without notice to the occupier.

---

20 Data Protection Act 1998, s 40.

21 *Ibid*, s 46.

22 *Ibid*, Sched 9.

It is an offence intentionally to obstruct a person in 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. An offender is liable to a fine not exceeding £5,000.

Other criminal offences[23]

It is a criminal offence for a person knowingly or recklessly to obtain or disclose personal data or the information contained in the data or procure the disclosure to another person of the information contained in the personal data without the consent of the data controller. It is also an offence to sell or offer to sell personal data obtained in contravention of this provision.

Notification[24]

Data controllers are required to notify the Commissioner of certain information relating to their data processing.

The notification requirements do not apply to information recorded in a relevant processing system (that is, structured paper-based filing systems). But where the information is kept on computer, notification must take place.

The following information must be notified:

- the name and address of the data controller;
- the name and address of any nominated representative;
- a description of the personal data being processed and the categories of data to which they relate;
- a description of the purposes for which the data are being processed;
- a description of the recipients to whom the controller intends to disclose the data;
- the name or description of any countries or territories outside the EEA to which the data controller transfers or intends to transfer the data.

The notifications are kept on a public register which is maintained by the Commissioner. The data controller must also provide a general description of the security measures taken to protect the he personal data. These will not appear on the register.

Where the requirement to notify applies, it is an offence to process data without notification.

It is also a criminal offence to fail to notify the Commissioner of changes to the register entry.

---

23 Data Protection Act 1998, s 55.

24 *Ibid*, Pt 3, ss 16–26.