



Information Commissioner's Office

## Response from the Information Commissioner's Office to the Review of the Code of Practice on Protecting the Confidentiality of Service User information

### **Introduction**

The Information Commissioner ('the Commissioner') has responsibility in the UK for promoting and enforcing the Data Protection Act 1998 ('DPA') and the Freedom of Information Act 2000. The Information Commissioner's Office ('ICO') is the UK's independent authority set up to uphold information rights in the public interest, promoting openness by public bodies and data privacy for individuals. The Commissioner does this by providing guidance to individuals and organisations, solving problems where he can, and taking appropriate action where the law is broken. The Commissioner's response to this consultation is primarily based on the practical experience he has gained in regulating compliance with the DPA and recent amendments to that legislation.

### **Background**

The Commissioner welcomes the opportunity to input into the review of the Code of Practice on Protecting the Confidentiality of Service User Information ('the Code') being carried out by the Privacy Advisory Committee in Northern Ireland. The Commissioner understands that the health and social care services in Northern Ireland depend upon the existence and the efficient running on information from those who use its service. He is equally aware of the volume and often the complexity of the information required for these services to function. Often the ability to match identifying information from several sources will be needed so that the patient gets the best treatment possible. However patients seeking treatment entrust sensitive information to those who provide their healthcare. They do so in confidence, and have the legitimate expectation that their privacy will be respected, and that their health records will be used in an appropriate way by the health service to support their healthcare.

The Commissioner acknowledges that the existing code is a very comprehensive document aimed at health and social care professionals. He notes the Code stresses the importance of it being a living document which will require regular review and update to take account of new and changing issues in relation to confidentiality and privacy. In light of this aim the Commissioner has based his comments on his experience of regulating the DPA, taking into account its recent amendments as well as his awareness of evolving best practice with the health service.

## The ICO data sharing code of practice

Most of the existing Code highlights the legal and ethical requirements of sharing service user information, including keeping service users informed, when consent is required, the purposes of the sharing and giving individual access to this information.

On the 28<sup>th</sup> June 2011 the Commissioner launched his Data Sharing Code of Practice<sup>1</sup> in Northern Ireland ('the data sharing code '). This Data Sharing Code covers data sharing in the context of the disclosure of personal data<sup>2</sup> from one or more organisations to a third party organisation or organisations, or the sharing of data between different parts of an organisation. If data sharing does not involve personal data - for example where only statistics that cannot identify anyone are being shared - neither the DPA, nor the data sharing code, apply.

The Data Sharing Code was prepared and published under section 52 of the DPA<sup>3</sup>. This is a statutory code which means that it has been approved by the Secretary of State and laid before Parliament. Although the Data Sharing Code is not legally binding, it adds details and guidance around how to interpret the 'bare minimum requirements' of the DPA in this area. The code does not impose additional legal obligations nor is it an authoritative statement of the law. However the Data Sharing Code can be used in evidence in any legal proceedings, not just proceedings under the DPA. The approach suggested is therefore recommended practice but, if not followed, data controllers are likely to face criticism and harsher sanctions if any relevant DPA breach is considered by the ICO or the courts<sup>4</sup>.

---

<sup>1</sup> Available at [www.ico.gov.uk](http://www.ico.gov.uk)

<sup>2</sup> S.1(1) DPA ' Personal data means data which relate to 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 in to 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;”

<sup>3</sup> ss. 52A – 52E DPA inserted by Coroners and Justice Act 2009.

<sup>4</sup> S 52E 'Effect of data-sharing code'

(1) A failure on the part of any person to act in accordance with any provision of the data-sharing code does not of itself render that person liable to any legal proceedings in any court or tribunal.

(2) The data-sharing code is admissible in evidence in any legal proceedings.

(3) If any provision of the data-sharing code appears to—

(a) the Tribunal or a court conducting any proceedings under this Act,

(b) a court or tribunal conducting any other legal proceedings, or

(c) the Commissioner carrying out any function under this Act,

The Commissioner considers that any data controller<sup>5</sup> (organisation) who is involved in the sharing of personal data should use his data sharing code to help them understand how to adopt good practice. Adopting the good practice recommendations of the data sharing code will help to ensure that any sharing of personal information is undertaken in a manner that is fair, transparent and in line with the rights and expectations of the people whose information is being shared. The Commissioner recommends that the Privacy Advisory Committee as part of their review of their Code, take into account the Commissioner's Data Sharing Code. The Commissioner has outlined a brief summary of the key features of the new data sharing code for the benefit of this consultation response.

### **Key features of the Data Sharing Code of Practice**

The first step for compliant data sharing is to determine the legality of the proposal and the organisation's authority to pursue it. This means considering the statutory or other authority of public bodies to undertake activities.

Private companies are advised to check industry specific regulation or guidance and company formation documents. The Commissioner has noted that within the Preface to the Code it states:

*"In Northern Ireland there is no equivalent to section 251 of the National Health Service Act 2006, which allows the setting aside of the common law duty of confidentiality for such essential health and social care purposes. The need for statutory provision for health and social care information governance including the uses and disclosures of confidential identifiable service user information is presently being considered by the Department."*

---

to be relevant to any question arising in the proceedings, or in connection with the exercise of that jurisdiction or the carrying out of those functions, in relation to any time when it was in force, that provision of the code must be taken into account in determining that question.

(4) In this section "the data-sharing code" means the code issued under section 52B(5) (as altered or replaced from time to time)."

<sup>5</sup> S 1 (1) DPA data controller "means, subject to subsection (4) , 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:"

The Commissioner advises that before sharing any personal data, organisations will need to consider all the legal implications of doing so. The ability to share information is subject to a number of legal constraints which go beyond the requirements of the DPA such as the common law test of confidentiality.<sup>6</sup> If an organisation or individual wishes to share information with another person, whether by way of a one-off disclosure or as part of a large-scale data sharing arrangement, they will need to consider whether they have the legal power or ability to do so. The Commissioner's Data Sharing Code has further guidance on the law in relation to data sharing for both the public and private sector.

### **Factors to be taken into account before sharing personal information**

The Data Sharing Code lists those factors which should be considered before entering into a data sharing arrangement. To help identify data protection issues, the use of Privacy Impact Assessments is recommended. The Commissioner suggests that organisations consider the following questions before sharing any personal information:

- What the sharing is meant to achieve?
- What information needs to be shared?
- Who requires access to the shared personal data?
- When should it be shared?
- How should it be shared?
- What checks can be carried out to ensure the data sharing is achieving its objectives?
- The risks posed by the data sharing.
- Whether objectives could be achieved without sharing the data or by disclosing only anonymous data.
- Whether the organisation will have to amend its data protection notification.
- Whether any of the data will be transferred outside of the EEA.

---

<sup>6</sup> If a party is to be held liable for breach of confidence it must be shown that (1) the material communicated to him had the necessary quality of confidence; (2) it was communicated or became known to him in the circumstances entailing an obligation of confidence; and (3) there was an unauthorised use of that material – See *Coco v AN Clark (Engineers) Ltd* [1969] RPC 41

## Keeping Service Users informed

The Commissioner has noted that chapter 2 of the Code includes a section on keeping service users informed. In particular the Commissioner has noted paragraph 2.2 of the Code which states:

*"... Service users must be kept informed in an accessible manner (including making use of appropriate communication supports) about the uses and disclosures of their information. It is important that service users are informed of the limitations of confidentiality, both in terms of any relevant statutory obligations to disclose confidential information and of the duty of health and social care staff to disclose information in the public interest."*

The Commissioner's Data Sharing Code sets out further guidance about when and how to issue Privacy Notices telling individuals what is happening to their personal information. The DPA requires that personal data be processed fairly, meaning that people should generally be aware of which organisations are sharing their personal data and what it is being used for. In a broader sense, fairness also requires that where personal data is shared, this happens in a way that is reasonable and that people would be likely to expect and would not reasonably object to if given the chance. This applies equally to routine data sharing or a single, one-off disclosure. In his new data sharing code the Commissioner has set out that in the data sharing context the Privacy notice should include the following:

- The identity of the organisation
- The reasons why personal data is to be shared
- The identity of other organisations with whom personal data will be shared, either individually named organisations or types of organisation

In particular, the attention of data subjects should be drawn to data sharing involving

- sharing sensitive personal data
- data sharing that is likely to be unexpected or objectionable
- data sharing that may have a significant effect on the individual
- data sharing that is particularly widespread
- data sharing that is being carried out for a range of different purposes

## **Data Sharing Agreements/protocols**

In his Data Sharing Code, the Commissioner recommends that organisations enter into data sharing agreements or protocols in relation to those regular or systemic data sharing arrangements. The Commissioner considers that a data sharing agreement should outline the following:

- the purpose of data sharing
- potential recipients or types of recipient of the personal data and the circumstances in which they will have access
- a description of the personal data to be shared
- provisions around data quality
- data security requirements
- how long shared data should be retained
- how individuals' rights will be met
- provision for a review of the effectiveness of the data sharing arrangements

## **Consent and Conditions for processing**

The Code is clear to outline the importance of gaining service user consent to disclose personal data. The Commissioner notes that at paragraph 2.7 the Code states:

*"if the service user refuses to consent to disclosure of personal information, the information cannot be disclosed, unless, exceptionally a justification other than consent exists... Unless there is an overriding public interest justification, information should not be disclosed on a 'best interest' basis where an adult with capacity refuses to consent to disclosure."*

The Commissioner would like to draw attention to the conditions (including consent) for processing personal information which is present in the DPA. Satisfying a condition goes towards making the processing 'fair' and compliant with the DPA. It is important to note that consent is not the only condition which can be relied upon to share personal information.

The DPA requires that you to process personal data fairly and lawfully and in compliance with the first principle which states:

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

*(a) at least one of the conditions in Schedule 2 is met, and*

*(b) in the case of sensitive personal data, at least one of the conditions in Schedule 3 is also met.”*

## **Conditions for processing**

The first data protection principle requires, among other things, that you must be able to satisfy one or more “conditions for processing” in relation to your processing of personal data<sup>7</sup>. Many (but not all) of these conditions relate to the purpose or purposes for which you intend to use the information. For ease of reference the conditions for processing found at schedules 2 and 3 of the DPA are set out at Annex A of this consultation response.

The conditions for processing take account of the nature of the personal data in question. The conditions that need to be met are more exacting when the information being processed is sensitive personal data<sup>8</sup>, such as information about an individual’s health or criminal record.

---

<sup>7</sup> The conditions for processing are set out in Schedules 2 and 3 to the Data Protection Act, available at Annex A of this consultation response. Unless a relevant exemption applies, at least one of the following conditions must be met whenever you process personal data:

<sup>8</sup> Section 2 DPA - In this Act “sensitive personal data” means 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.

However, the Commissioner's view in determining if you have a legitimate reason for processing personal data, is to focus on whether what you intend to do is fair. If it is, then you are very likely to identify a condition for processing that fits your purpose.

Being able to satisfy a condition for processing will not on its own guarantee that the processing is fair and lawful – fairness and legality must still be looked at separately.

Where the individual has consented to their personal data being collected and used in the manner and for the purposes in question, it is the Commissioner's view that you will need to examine the circumstances of each case to decide whether consent has been given. Often this will be obvious, but at other times, the particular circumstances will need to be examined closely to decide whether adequate consent has been given.

Consent is not defined in the Data Protection Act. However, the European Data Protection Directive (to which the Act gives effect) defines an individual'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 an individual must "signify" their agreement means that there must be some active communication between the parties. An individual may "signify" agreement other than in writing, but organisations should not infer consent if an individual does not respond to a communication – for example, from a patient's failure to return a form or respond to a leaflet. Consent obtained under duress or on the basis of misleading information does not adequately satisfy the condition for processing.

Consent must also be appropriate to the age and capacity of the individual and to the particular circumstances of the case. For example, if an organisation intends to continue to hold or use personal data after the relationship with the individual ends, then the consent should cover this. Even when consent has been given, it will not necessarily last forever. Although in most cases consent will last for as long as the processing to which it relates continues, you should recognise that the individual may be able to withdraw consent, depending on the nature of the consent given and the circumstances in which you are collecting or using the information. Withdrawing consent does not affect the validity of anything already done on the understanding that consent have been given.

The Commissioner considers that an organisation should review whether a consent which has been given remains adequate as an organisation's relationship with an individual develops, or as the individual's circumstances change.

The Data Protection Act distinguishes between:

- the nature of the consent required to satisfy the first condition for processing; and
- the nature of the consent required to satisfy the condition for processing sensitive personal data, which must be “explicit”.

This suggests that the individual’s consent should be absolutely clear. It should cover the specific processing details; the type of information (or even the specific information); the purposes of the processing; and any special aspects that may affect the individual, such as any disclosures that may be made.

As explained above, a particular consent may not be adequate to satisfy the condition for processing (especially if the individual might have had no real choice about giving it), and even a valid consent may be withdrawn in some circumstances. For these reasons an organisation should not rely exclusively on consent to legitimise its processing. Consent is the first in the list of conditions for processing set out in the Act, but each condition provides an equally valid basis for processing personal data. Other conditions relevant to the processing of personal information for health and social services purposes may include (but not limited to), legitimate interests, the vital interests condition, the medical purposes condition. In our view, it is better to concentrate on making sure that individuals are informed fairly rather than on obtaining consent in isolation.

All of the conditions are set out in Annex A of this consultation response and further detail on each of the conditions can be found on the ICO website at [www.ico.gov.uk](http://www.ico.gov.uk).

## The Article 29 Opinion

The Commissioner would also like to draw the Privacy Advisory Committee's attention to the recent opinion from the Article 29 working group adopted on the 13 July 2011<sup>9</sup> on the definition of consent (WP187 – Opinion 15/2011). It gives a steer on the properties that consent must have if it is to be used to legitimise the processing of personal data. The Commissioner considers that the opinion is consistent with the guidance the Commissioner has produced in his Guide to Data Protection available at [www.ico.gov.uk](http://www.ico.gov.uk). The key features of the opinion include:

- Consent must be freely given. There must be no deception, intimidation or risk of significant negative consequences for the data subject if he or she does not consent.
- Consent must be specific. Blanket consent without establishing exact purposes is not specific enough.
- Consent must be informed. Enough information must be provided to individuals to guarantee that they can make well informed decisions about the processing of their personal data.
- Where explicit consent is required to process sensitive personal data, there must be an active response, oral or in writing, whereby the individual demonstrates agreement to his or her personal data being processed for certain purposes.
- Consent based on an individual's inaction or silence does not normally constitute valid consent.
- There is a difference between the consent principle and the right to prevent processing after it has started – consent must cover the whole processing operation from start to finish.
- Individuals who have consented should be able to withdraw their consent, preventing further processing of their personal data.
- It can be unfair or misleading to use consent to legitimise processing initially, but to then 'switch' conditions in order to continue processing even though the individual has since withdrawn consent.

---

<sup>9</sup> Available at [http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187\\_en.pdf](http://ec.europa.eu/justice/policies/privacy/docs/wpdocs/2011/wp187_en.pdf)

## **Supporting the service user's right to access their records.**

The Commissioner has noted that at paragraph 2.10 of the Code it is stated:

*"Information in the record about third parties (other than relevant health professionals) should not in general be disclosed without the consent of the third party. Information should not be disclosed where its release may cause serious harm to the physical or mental health or condition of the service user or any other person."*

The Commissioner has issued guidance entitled 'Dealing with subject access requests which contain third party information', available on his website at: [http://www.ico.gov.uk/for\\_organisations/guidance\\_index/data\\_protection\\_and\\_privacy\\_and\\_electronic\\_communications.aspx#subject](http://www.ico.gov.uk/for_organisations/guidance_index/data_protection_and_privacy_and_electronic_communications.aspx#subject)

Section 7(1) of the Data Protection Act 1998 (the Act) gives individuals the right to access their personal data. By making a written request and paying a fee, an individual is entitled to see (among other things):

- the information which is the personal data; and
- any information available to the data controller about the source of the data.

Responding to such subject access requests may involve providing information relating to another individual (a 'third party individual'). For instance, a health record may contain details of those members of staff involved in the individual's treatment. Section 7(4) of the DPA provides that if an organisation cannot comply with the request without disclosing information relating to another individual who can be identified from that information, then it does not have to comply with the request unless:

- the third party has consented to the disclosure; or
- it is reasonable in all the circumstances to comply with the request without the consent of the third party individual.

If the information can be anonymised to protect the identity of the third party, then this should be done and the information released.<sup>10</sup> However, the organisation must have regard to any other identifying information which it believes is reasonably likely to be in or come into the applicant's possession<sup>11</sup>.

---

<sup>10</sup> S 7(5) DPA

<sup>11</sup> S 8(7) DPA

The Commissioner's guidance sets out a series of steps to follow if it is not possible to anonymise the personal information including seeking if:

- (i) has the third party consented
- (ii) Would it be reasonable in all of the circumstances to disclose without consent

Section 7(6) of the DPA provides a non-exhaustive list of factors to be taken into account when deciding what would be 'reasonable in all the circumstances'. These are:

- any duty of confidentiality owed to the third party individual;
- any steps you have taken to try to get the consent of the third party individual;
- whether the third party individual is capable of giving consent; and
- any express refusal of consent by the third party individual.

In all cases when deciding to release or not to release personal information containing third party data the Commissioner advises that an organisation justify and keep a record of its course of action and reasoning, including, for example, why it chose not to try to get consent or why it was not appropriate to try to do so in the circumstances.

### **Maintaining the confidentiality of information after a service user's death**

The Commissioner has noted that at paragraph 2.20 of the Code highlights the importance of maintaining the confidentiality of a service user's information if they are deceased. The Commissioner wishes to draw attention to his guidance entitled "*Practical guidance information about the deceased*" – Access to deceased person's records' which is available on his website<sup>12</sup>. This guidance sets out the Commissioner's view on dealing with requests for deceased persons records. When an individual is deceased the DPA will no longer apply to them or their records. If a request is received for these records by a public authority it triggers the Freedom of Information Act 2000, and the Commissioner has set out in this guidance those considerations and exemptions he considers are most appropriate to take into account. For ease of reference this response highlights those exemptions at section 40 and section 41 of the Freedom of Information Act 2000 which are detailed further in the guidance.

---

<sup>12</sup>

[http://www.ico.gov.uk/for\\_organisations/guidance\\_index/freedom\\_of\\_information\\_and\\_environmental\\_information.aspx#deceased](http://www.ico.gov.uk/for_organisations/guidance_index/freedom_of_information_and_environmental_information.aspx#deceased)

## Section 40 exemption

The exemption for personal information (section 40) only applies to living individuals. This exemption cannot be used for information about someone who has died. However, the exemption may still apply if the information in question is also personal information about another identifiable living person, such as genetic information which may also relate to a surviving relative, or parts of social work records may contain information about other members of a family (see ICO decision notice FS50082251<sup>13</sup> for an example).

## Section 41 exemption

The exemption for confidential information (section 41) may apply if the information was originally obtained from the deceased. An organisation should first consider whether it has the ingredients for a duty of confidence and if so whether there is a public interest defence to disclosure.<sup>14</sup>

If a duty of confidence arises, the Commissioner's view is that the exemption will continue to apply after the death of the person concerned. This has been confirmed by the First Tier Tribunal (Information Rights) in the case of Bluck<sup>15</sup>. The duty would be legally enforceable by the deceased's personal representative (the person or people who administer the deceased's estate under the law relating to wills and probate). The organisation does not need to identify the relevant person. The important thing is to establish in principle that a personal representative might exist who can take action.

---

<sup>13</sup> See [www.ico.gov.uk](http://www.ico.gov.uk) – decision notices

<sup>14</sup> See 'Section 41: information provided in confidence' available at: [http://www.ico.gov.uk/for\\_organisations/guidance\\_index/freedom\\_of\\_information\\_and\\_environmental\\_information.aspx#exemptions](http://www.ico.gov.uk/for_organisations/guidance_index/freedom_of_information_and_environmental_information.aspx#exemptions)

for more detail on the approach to take. See also ICO decision notice FS5012480 for an example of how the ICO has applied s41 in these circumstances.

<sup>15</sup> EA/2006/0090 - Pauline Bluck v IC and Epsom & St Helier University Hospitals NHS Trust. In this case the appellant was seeking the disclosure of her deceased daughter's medical record, but the daughter's next of kin, her widower who was also her personal representative, had objected.

## **Conclusion**

The Commissioner has welcomed the opportunity to respond to the consultation being undertaken by the Privacy Advisory Committee in Northern Ireland. The Commissioner is happy to provide any clarification or further assistance on any of the issues he has raised in the above response.

August 2011

## **Annex A - Schedule 2 DPA conditions**

### SCHEDULE 2 CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF ANY PERSONAL DATA

1The data subject has given his consent to the processing.

2The 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.

3The processing is necessary for compliance with any legal obligation to which the data controller is subject, other than an obligation imposed by contract.

4The processing is necessary in order to protect the vital interests of the data subject.

5The processing is necessary—

(a)for the administration of justice,

(aa)for the exercise of any functions of either House of Parliament,

(b)for the exercise of any functions conferred on any person 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(d)for the exercise of any other functions of a public nature exercised in the public interest by any person.

6 (1) The processing is necessary for the purposes of the 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 by reason of prejudice to the rights and freedoms or legitimate interests of the data subject.

(2) The Secretary of State may by order specify particular circumstances in which this condition is, or is not, to be taken to be satisfied.”

## **Schedule 3 conditions**

### **SCHEDULE 3 CONDITIONS RELEVANT FOR PURPOSES OF THE FIRST PRINCIPLE: PROCESSING OF SENSITIVE PERSONAL DATA**

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

2(1)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.

(2)The Secretary of State may by order—

(a)exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b)provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

3The 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.

4The processing—

(a)is carried out in the course of its legitimate activities by any body or association which—

(i)is not established or conducted for profit, and

(ii)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 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.

7(1) The processing is necessary—

(a) for the administration of justice,

(aa) for the exercise of any functions of either House of Parliament,

(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—

(a) exclude the application of sub-paragraph (1) in such cases as may be specified, or

(b) provide that, in such cases as may be specified, the condition in sub-paragraph (1) is not to be regarded as satisfied unless such further conditions as may be specified in the order are also satisfied.

7A(1) The processing—

(a) is either—

(i) the disclosure of sensitive personal data by a person as a member of an anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation; or

(ii) any other processing by that person or another person of sensitive personal data so disclosed; and

(b) is necessary for the purposes of preventing fraud or a particular kind of fraud.

(2) In this paragraph “an anti-fraud organisation” means any unincorporated association, body corporate or other person which enables or facilitates any sharing of information to prevent fraud or a particular kind of fraud or which has any of these functions as its purpose or one of its purposes.

8(1) 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.

(2) In this paragraph “medical purposes” includes the purposes of preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of healthcare services.

9(1) 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.

(2) The Secretary of State may by order specify circumstances in which processing falling within sub-paragraph (1)(a) and (b) is, or is not, to be taken for the purposes of sub-paragraph (1)(c) to be carried out with appropriate safeguards for the rights and freedoms of data subjects.