



Home Office

Data Sharing for the Prevention of Fraud

Code of practice for public authorities disclosing information to a specified anti-fraud organisation under sections 68 to 72 of the Serious Crime Act 2007



Data Sharing for the Prevention of Fraud

Code of practice for public authorities
disclosing information to a specified anti-fraud
organisation under sections 68 to 72 of the
Serious Crime Act 2007

Presented to Parliament pursuant to
section 71 of the Serious Crime Act 2007

© Crown copyright 2008

The text in this document (excluding the Royal Arms and other departmental or agency logos) may be reproduced free of charge in any format or medium providing it is reproduced accurately and not used in a misleading context. The material must be acknowledged as Crown copyright and the title of the document specified.

Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned.

For any other use of this material please write to Office of Public Sector Information, Information Policy Team, Kew, Richmond, Surrey TW9 4DU or e-mail: xxxxxxxxx@xxxx.xxx.uk

Contents

Foreword by the Parliamentary Under-Secretary of State for Crime Reduction	3
Foreword by the Information Commissioner	4
Introduction	5
Background	5
The effect of section 68 of the SCA	6
Deciding to share personal information	6
Fairness and transparency	7
Information sharing standards	9
Rights of data subjects	9
Retention of shared information	9
Security of shared information	10
Access to personal information under the FOIA and the DPA	10
Review	11
Compliance with the Code	11
Role of the Information Commissioner	12
Appendix 1: Legislative summary	13
Appendix 2: Extracts from statutory provisions	14
Appendix 3: Good practice examples of layered fair processing notices for public authorities	19

Foreword by the Parliamentary Under- Secretary of State for Crime Reduction

Fraud costs the UK at least £13.9 billion a year. Preventing fraud is clearly better than tackling it once it has happened. Sharing data about fraud or suspected fraud is a very good way – and often the only practical way – to prevent further fraudulent activity and help identify those responsible.

Public authorities have a particular responsibility to ensure that taxpayers' money is not taken out of the system fraudulently. Losses suffered by public authorities as a result of fraud reduce their ability to provide cost-effective public services. We believe that more can and should be done through the proper sharing of data to prevent fraud. The specification of anti-fraud organisations under the Serious Crime Act 2007 will enable public authorities to share data with the private sector in order to reduce the opportunity for criminals to profit at the taxpayer's expense.

Of course, it is vital that the benefits of sharing data for the purposes of fraud prevention are balanced against the rights of the individual. By following the requirements of this Code of Practice, public authorities will be able to ensure that the sharing of data is necessary and proportionate, and that both individuals' rights and the public purse are protected.



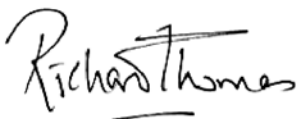
Vernon Coaker
Parliamentary Under-Secretary of State
for Crime Reduction

Foreword by the Information Commissioner

Fraud prevention is a key priority for the public and private sectors alike. The powers under the Serious Crime Act 2007 allow public sector information to be exchanged with the private sector so that fraud can be detected, targeted and prevented on a much wider scale. However, the powers under the Act must be considered in the context of any Data Protection Act requirements. Specifically, information must be shared in a manner that is proportionate, and any organisations using this information sharing gateway must take steps to ensure that they only share such data as is necessary for the prevention of fraud.

Where multiple partners engage in information sharing, being transparent and enabling individuals to exercise their rights to know how their information is being used is crucial. Equally, the importance of security when sharing personal information has never been as prominent as in recent months, and this must remain a major priority for any organisation wishing to share personal information.

I welcome this high-level Code of Practice in terms of setting out some broad principles and considerations for participants. I also welcome the Home Office's commitment to make any organisation participating in these information sharing arrangements subject to audit by the Information Commissioner's Office. The next key step is for organisations to define and agree the detail around what data will be shared and how any data protection risk will be minimised. Personal information is both an asset and a liability, and I expect any organisation involved in sharing personal information under the Serious Crime Act to treat it as such. Complying with the requirements of this Code will allow participants to identify those individuals involved in fraudulent activity while protecting the rights of the majority who are not.



Richard Thomas
Information Commissioner

Introduction

1. This Code of Practice is a requirement of the Serious Crime Act 2007 (the SCA). Public authorities must have regard to it when disclosing information for the purposes of preventing fraud, either as a member of a specified anti-fraud organisation (SAFO) specified by order under the SCA, or otherwise in accordance with any arrangements made by such an organisation. It does not apply to the disclosure of information by a relevant public authority when the subject matter of the information is within the legislative competence of the Scottish Parliament. For these purposes, a relevant public authority is one that has functions (whether alone or in addition to other functions) that are exercisable with devolved competence (within the meaning of section 54 of the Scotland Act 1998).¹
2. Personal information must be processed in a manner that complies with the Data Protection Act 1998 (DPA) and in accordance with the requirements of this Code of Practice. Specifically, information must be processed in line with an information sharing document agreed with the SAFO (see paragraph 18).
3. Section 68 of the SCA enables public authorities to disclose information for the purposes of preventing fraud in accordance with arrangements with a SAFO. However, not all public authorities will need to rely on section 68 to disclose information under arrangements with a SAFO, because they may already have a common-law or statutory power. As a consequence, this Code applies not only to disclosures under arrangements with a SAFO that use the gateway in the SCA (section 68) but also to disclosures that are lawful under other statutory or common-law powers. In all circumstances the disclosure must still be lawful and fair in terms of the DPA.
4. Neither this Code nor the provisions of the SCA authorises disclosures that contravene the DPA. The purpose of this Code is to provide an overarching code of practice for disclosing information in order to prevent fraud under arrangements with a SAFO. It will complement good data sharing policy and practice guidance, which already exists in many individual public authorities.
5. The Code does not provide guidance to public authorities on what they should do in circumstances where the disclosure of information under arrangements with a SAFO reveals information indicative of actual or potential fraud. In such cases, public authorities should decide what to do in the light of their own policies and practice and those of the relevant SAFO.
6. The Information Commissioner has been consulted in the drafting of this Code. We have also consulted organisations that have shown an interest in being specified as SAFOs.

Background

7. Fraud costs the UK at least £13.9 billion a year. It affects the private and public sectors alike, with many individuals perpetrating frauds against both. It is in all our interests to prevent fraud, and public authorities have a particular responsibility to ensure that taxpayers' money is not taken out of the system fraudulently.
8. The mechanism provided by the SCA for disclosing information under arrangements with a SAFO gives public authorities an opportunity to share data with the private sector for the purposes of preventing fraud; for many of them, this opportunity has not been available before. For example, the legislation will enable data concerning individuals suspected (on the balance of probability) of committing fraud against the public sector to be shared with other public and private sector bodies, to help protect these bodies against future frauds.

¹ See section 68(5) and (6) of the SCA.

9. This Code, combined with data protection legislation, will ensure that data is shared in a way that is necessary and proportionate, and that takes place within a framework that properly protects individuals' rights and the security of the data.

The effect of section 68 of the SCA

10. Section 68 provides authority for disclosure by a public authority to a SAFO. It is not concerned with the powers of a SAFO or any person who may receive a disclosure under the power in section 68. However, in order to be specified under the SCA, anti-fraud organisations will be assessed against specific criteria. SAFOs must also meet the requirements of the DPA. A disclosure under section 68 can be to any of the persons identified in section 68(2)(b) (a SAFO, any member of a SAFO or any other person permitted to receive a disclosure under arrangements with a SAFO), so long as it:
 - (a) is for the purposes of preventing fraud or a particular kind of fraud; and
 - (b) takes place as part of a public authority's membership of a SAFO or under some other arrangements with a SAFO (this second possibility is to provide maximum flexibility and takes account of the fact that not all SAFOs will operate a membership scheme); and
 - (c) does not contravene the DPA.

In this Code of Practice we have used the term “arrangements with a SAFO” to mean a disclosure that meets this test.

11. Appendix 1 provides further details of the legislative scheme.

Deciding to share personal information

12. The DPA requires that personal information must be processed in a way that is fair, lawful and not incompatible with the purposes for which it was obtained.² Furthermore, any information that is processed should be relevant and not excessive in relation to the purpose for which it is being shared.³
13. The processing of sensitive personal data will not be regarded as fair and lawful (in accordance with the first data protection principle) unless it meets one of the conditions in Schedule 2 and one of the conditions in Schedule 3 to the DPA. Section 72 of the SCA amends Schedule 3 to the DPA to add to the possible conditions covering the permissible processing of sensitive personal data for the prevention of fraud. The new condition will be met if:
 - (a) the processing is:
 - (i) a disclosure by a person as a member of, or otherwise under arrangements with, an anti-fraud organisation, or
 - (ii) any other processing (by the person who made the disclosure or some other person) of sensitive personal data disclosed in that way; and
 - (b) the processing is necessary for the purposes of preventing fraud or a particular kind of fraud.
14. Under the SCA, “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.

² See data protection principles 1 and 2 – www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9#sch1

³ See data protection principle 3 – www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9#sch1

15. The new condition covers a wide range of processing in addition to disclosures under section 68 of the SCA. Sensitive personal data is defined in section 2 of the DPA and includes, for example, the commission or alleged commission by the data subject of any offence, his racial or ethnic origin, his political opinions and his religious beliefs.⁴ Public authorities must ensure that any sensitive personal data is handled appropriately and in accordance with data protection legislation.
16. The information disclosed may be of any kind. Types of information could include, for example, the identifying details of individuals suspected of fraudulently obtaining services.
17. However, public authorities must not disclose excessive information and must only disclose the minimum information necessary for the purposes of preventing fraud or a particular kind of fraud.
18. In practice the information disclosed will be governed to a large extent by the requirements of the arrangements with a SAFO under which the public authority intends to disclose information. Public authorities should prepare an **agreed information sharing document** with the SAFO, setting out mutually agreed standards on areas such as the use, handling and security of information. This should incorporate the requirements of this Code of Practice and follow the Information Commissioner's Office's (ICO) information sharing framework code.⁵
19. When deciding whether or not to disclose information under arrangements with a SAFO, public authorities should consider:
 - the types and levels of fraud that they may be subject to;
 - whether disclosing information to a SAFO would be a good use of their resources in reducing fraud;
 - the type of information they will be disclosing and how this can be minimised to that which is necessary to prevent fraud or a particular kind of fraud; and
 - whether the information sharing mechanisms of the SAFO will suit the purposes of the public authority.
20. The SAFO may be able to provide advice on the disclosure of information based on previous experience, or may be willing to undertake a trial or a pilot exercise ahead of final decisions being made. Any trial or pilot exercise must be DPA-compliant. Under the DPA, a data controller is defined as "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". Both the public authority and the SAFO will have obligations as data controllers under their information sharing arrangements. The SAFO will also have had to meet certain requirements in order to be specified under the SCA.

INFORMATION SHARING DOCUMENT

18. In practice the information disclosed will be governed to a large extent by the requirements of the arrangements with a SAFO under which the public authority intends to disclose information. Public authorities should prepare an **agreed information sharing document** with the SAFO, setting out mutually agreed standards on areas such as the use, handling and security of information. This should incorporate the requirements of this Code of Practice and follow the Information Commissioner's Office's (ICO) information sharing framework code.⁵
19. When deciding whether or not to disclose information under arrangements with a SAFO, public authorities should consider:
 - whether in their own individual circumstances it would be sensible to take part in the arrangements;
 - whether in their own individual circumstances they can meet the requirements of the DPA in participating;
20. The SAFO may be able to provide advice on the disclosure of information based on previous experience, or may be willing to undertake a trial or a pilot exercise ahead of final decisions being made. Any trial or pilot exercise must be DPA-compliant. Under the DPA, a data controller is defined as "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". Both the public authority and the SAFO will have obligations as data controllers under their information sharing arrangements. The SAFO will also have had to meet certain requirements in order to be specified under the SCA.

Fairness and transparency

21. Public authorities will be required to ensure that their data sharing practices are fair and transparent. SAFOs will also be required to have fair and transparent processes in place for disclosing and receiving data. Public authorities must satisfy themselves that these processes are satisfactory before any data is shared. Public authorities that disclose information to SAFOs will need to be aware of and comply with these processes when sharing information under arrangements with them.

⁴ See DPA section 2 – www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_2#pt1-l1g2

⁵ www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf

FAIR PROCESSING NOTICES

22. The DPA requires data controllers to inform individuals of how their personal information is being used. Specifically, the first data protection principle requires the following details to be provided:
- (a) the identity of the data controller (together with the identity of any nominated representative for the purposes of the DPA, if the authority has one);
 - (b) the purpose or purposes for which the data is intended to be processed; and
 - (c) any further information that is necessary to enable the processing to be fair.
23. The provision of this information is known as a fair processing notice.
24. Participating public authorities should, so far as is practicable, ensure that fair processing notices are actively provided, or at least made readily available, to the individuals whose personal data the public authority will or may share. The notice should clearly state that their data may be disclosed for the purposes of preventing fraud, and that the data may be provided to other persons under arrangements with a SAFO for this purpose. The notice should also contain details of how individuals can find out more about the sharing of their data. Where a public authority is only likely to use one SAFO, the public authority should consider whether it would be appropriate to name that SAFO in the fair processing notice. In any event, details of the SAFO should be available on enquiry.
25. If the public authority is transparent in terms of how personal information is processed, individuals will be able to understand what their information is being used for and who is using it. They will also know who to contact if they have concerns or queries. Furthermore, transparency can have the beneficial side-effect of deterring fraud, as

people become aware of the measures taken by the organisations involved to detect fraud.

LAYERED NOTICES

26. The Information Commissioner recommends a layered approach to fair processing notices; this involves giving a relatively simple first explanation backed up by a more detailed explanation. Public authorities should make clear where individuals can obtain further information about the type of fraud they are trying to prevent, and how, why and with whom their information is being shared (by, for example, providing web links to more detailed information, or contact details for a named person such as the key contact on data sharing or a data protection officer).
27. Arrangements should be in place for dealing with questions and complaints about data sharing. Roles and responsibilities in both the public authority and the SAFO should be agreed and defined within the information sharing document.
28. Examples of layered fair processing notices can be found in Appendix 3.

RETROSPECTIVE NOTICES

29. Sometimes it will not be possible to provide a fair processing notice at the point when data is collected. In such cases, public authorities must issue retrospective fair processing notices as soon as practicable, unless it is impracticable to do so (because, for example, disproportionate effort would be required).⁶ The term “disproportionate effort” is not defined in the DPA. 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, public authorities will need to take into account a number of factors including the nature of the data and the time and cost involved in issuing a retrospective fair processing notice. These factors will need to be balanced against the prejudicial or potential prejudicial effect on the data subject of failing to issue such a notice.

⁶ See DPA Schedule 1, Part II, paragraphs 2 and 3 – www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9/sch1-pt2

Information sharing standards

30. Public authorities should disclose information to a SAFO under an information sharing document that has been agreed with the SAFO. This should specify agreed arrangements for, among other things, fair processing, data minimisation, retention and use of the data, security of the data and the rights of data subjects. It should follow this Code of Practice and the ICO's own information sharing framework code.
31. Public authorities should ensure that any data they share with a SAFO is in accordance with the DPA.⁷ Among other things, the DPA principles require that the data shared must be up to date, accurate, relevant, and no more than is required for the purpose. The requirements of the SAFO will largely determine what information is relevant. Public authorities must also ensure that there are agreed standards, set out within their information sharing document, for the secure transmission of data to and from SAFOs.
33. Every public authority must ensure that:
 - (a) there is someone with specific responsibility for data protection issues within the organisation; and
 - (b) there are members of staff who are nominated to handle subject access requests, enquiries and complaints from data subjects about the organisation's handling of personal data.
34. If identified, any inaccurate information in the public authority's records should be corrected and any SAFO to which the data has been passed should be notified, so that its record of the data can also be corrected.
35. Public authorities should periodically quality-assure data that could be shared. Arrangements for doing so should be set out in the agreed information sharing document.

Rights of data subjects

32. It is important that the rights of data subjects are recognised in any information sharing arrangement. If information is processed in a manner that does not comply with the DPA (for example, where subject access requests are not handled correctly) or is processed unlawfully or inaccurately, this will breach data protection legislation. It could also breach libel laws and have a potentially serious effect on the data subject; for example, the sharing of inaccurate data could lead to services being withheld from an individual who qualifies for them. Data must be processed in line with the rights of data subjects, and public authorities must ensure that arrangements for doing this are specified in their information sharing arrangements with SAFOs.
36. It is a requirement of the DPA that personal information should be kept only for as long as necessary. How long it is "necessary" to hold such information will depend on the purpose for which the public authority holds the information, and its own policies and practices.
37. Public authorities and SAFOs should agree in their information sharing document a maximum period of time for which information shared under their arrangements can be held.
38. The SAFO should ensure that data no longer required is destroyed promptly and rendered irrecoverable. The same will apply to data derived or produced from the original data, except where section 33 of the DPA applies (in relation to data processed for research purposes).

Retention of shared information

⁷ See DPA Schedule 1 – www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9#sch1

Security of shared information

39. Much of the information handled by public authorities and SAFOs will be of a sensitive nature. It is essential to have appropriate technical and organisational measures in place to assure the security of such information. This should be set out and agreed in the information sharing document between the public authority and the SAFO. When creating the information sharing document, public authorities will want to carry out a risk assessment to identify the type of security problems that could occur and the effectiveness of their current security measures.
40. The DPA requires that organisations have appropriate technical and organisational measures in place to protect personal data.⁸
41. When dealing with information that is indicative of actual or potential fraud following data sharing under arrangements with a SAFO, a public authority should consider technical and organisational measures such as:
 - establishing role-based access to personal data, i.e. only allowing staff access to the information they need to do their jobs;
 - providing specialised training and supervision for staff who have access to sensitive personal data;
 - limiting the availability of data to selected, named individuals within the organisation who have been suitably trained;
 - ensuring that all computers and buildings used for data processing have physical and logical access controls limiting access to certain individuals (for example, firewalls, computer passwords and secure premises);
 - taking regular back-ups of the information held electronically if it will cause damage or distress if lost or stolen;
 - having agreed, secure methods for transferring data; and
 - undertaking periodic audits of its security arrangements, involving the SAFO as appropriate.
42. SAFOs will have their own security safeguards, and public authorities that choose to share data under arrangements with them should satisfy themselves that these safeguards are adequate for their purposes.
43. Public authorities must also have procedures in place to deal with any breaches of security. Examples of measures that public authorities should consider in relation to security breaches include:
 - having procedures in place to contain the situation and limit the damage that any security breach can cause;
 - carrying out a risk assessment of the potential adverse consequences for individuals of any security breach;
 - assessing who to notify, if necessary, that a security breach has occurred; and
 - having procedures in place to investigate the causes of any breach and the effectiveness of the response to it.

Access to personal information under the FOIA and the DPA

44. Individuals whose data is shared under arrangements with a SAFO will also have rights of access to information under the DPA or the Freedom of Information Act 2000 (FOIA).

⁸ See data protection principle 7 – www.opsi.gov.uk/acts/acts1998/ukpga_19980029_en_9#sch1-pt1

45. SAFOs will have their own policies and practices for dealing with requests for personal information under the DPA, as will public authorities. Where public authorities share data under arrangements with a SAFO, they will need to ensure that their practice is consistent with that organisation to ensure that requests are handled in accordance with the DPA.
46. As data will be shared under this Code to prevent fraud, there may be times when it is appropriate to use section 29 of the DPA to prevent access by an individual to the data. However, this exemption applies on a case-by-case basis and only where it is likely to prejudice the processing in question.
47. Under the FOIA, a person has the right to be told whether information is held by a public authority and to be given a copy (unless it is exempt). Public authorities should have in place practices and procedures in order to fulfil the requirements of the legislation.
48. Under the data sharing arrangements covered by this Code, it is likely that public authorities and the private sector will share personal data with one another. In dealing with FOIA requests, public authorities must comply with the FOIA while at the same time being mindful of the potential interests of the private sector organisations with which they share information. Arrangements should be put in place to ensure consultation between the relevant parties when such requests are made and before a reply is given.
51. Public authorities will be able to assess whether and to what extent they wish to take part in the data sharing arrangements made possible by the SCA. They may wish to take part in a pilot exercise with a SAFO before making a final judgement. Any pilot exercise must comply with the DPA.
52. Having entered into such a scheme, public authorities should, in consultation with SAFOs as appropriate, periodically review whether:
 - their information sharing agreements are working in practice;
 - the arrangements are an appropriate and effective anti-fraud measure;
 - fair processing notices are relevant and appropriate;
 - the quality of the data held by the public authority and any partner organisations is of agreed standards;
 - retention periods are being complied with and continue to meet business needs;
 - security remains adequate;
 - any security breaches are investigated, with lessons learned and acted on in an appropriate fashion; and
 - individuals are being given access to the information they are entitled to.

Review

BY THE HOME OFFICE

49. The Home Office will periodically review, by sample, arrangements between public authorities and SAFOs to ensure their compliance with this Code.

BY PUBLIC AUTHORITIES

50. This Code covers the disclosure of data by public authorities under arrangements with a SAFO for the purpose of preventing fraud.

Compliance with the Code

53. Where the Home Office becomes aware that the requirements of this Code are not being followed in practice, it will notify the public authority and ask it to introduce measures to comply. The Home Office may unspecify SAFOs that do not comply with the SCA or data protection legislation, and may notify the ICO.
54. Any general questions and concerns should be addressed to the Home Office in the first instance.

Role of the Information Commissioner

55. Questions and concerns relating to the DPA should be referred to the ICO, which may be contacted at:

The Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire SK9 5AF

ICO helpline:
08456 30 60 60
01625 54 57 45

E-mail: mail@ico.gsi.gov.uk

Website: www.ico.gov.uk (use the online enquiries form rather than the above e-mail address for questions regarding the legislation for which the Information Commissioner is responsible)

56. During the Parliamentary passage of the SCA, the Government gave an undertaking that the Information Commissioner would be given access to audit and inspect data sharing arrangements between public authorities and SAFOs. It is a condition of being specified that anti-fraud organisations will give the Information Commissioner such access. Participating public authorities must also provide access so that the Commissioner can assess compliance with the DPA generally.

APPENDIX 1

Legislative summary

Section 68 of the SCA provides for public authorities to disclose information for the purposes of preventing fraud, or a particular kind of fraud, as a member of a specified anti-fraud organisation or otherwise in accordance with any arrangements made with such an organisation.

An anti-fraud organisation is defined in the SCA as “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”.⁹ An anti-fraud organisation becomes specified by an order made by the Secretary of State. At present there are six specified anti-fraud organisations:

- CIFAS;
- Experian Limited;
- Insurance Fraud Investigators Group;
- N Hunter Limited;
- the Insurance Fraud Bureau; and
- the Telecommunications United Kingdom Fraud Forum Limited.

The SCA provides that the information disclosed can be of any kind and may be disclosed to the SAFO, any member of it, or any other person to whom disclosure is permitted by the arrangements concerned.

The SCA further provides that disclosure under the arrangements does not breach any obligation of confidence owed by the public authority disclosing the information, or any other restriction on the disclosure of information. It does not, however, authorise any disclosure that contravenes the DPA (or is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000, which deals with the interception of communications).

The power of disclosure in section 68 can be used by any public authority in the UK except a relevant public authority in relation to information whose subject matter would be within the legislative competence of the Scottish Parliament.

“Public authority” means any public authority within the meaning of section 6 of the Human Rights Act 1998.

Wrongful disclosure of information held by a public authority is usually covered by the DPA. Section 69 of the SCA creates an offence relating to making a further disclosure of information that has been disclosed by a public authority under arrangements with a SAFO, other than in certain specified circumstances listed in section 69(2). In practice, this provision currently relates only to HM Revenue and Customs (HMRC) information, disclosed by HMRC itself, which reveals the identity of the person to whom it relates. The offence could be extended to information held by other public authorities by order under the SCA, but there are no current plans to do so.

Finally, the SCA also amended Schedule 3 to the DPA by adding a new condition, relating to the sharing of data under arrangements with an anti-fraud organisation, for the processing of sensitive personal data.

This Code has been prepared in accordance with section 71 of the SCA, which requires the Secretary of State to prepare and keep under review a code of practice with respect to the disclosure, for the purposes of preventing fraud, of information by public authorities as members of SAFOs or otherwise in accordance with any arrangements made by such organisations. The Secretary of State must consult any SAFO, the Information Commissioner and such other persons as he considers appropriate in preparing the Code. Public authorities sharing data under the arrangements are required to have regard to the Code. A copy, and any alteration to it, must be laid before Parliament.

⁹ See section 68(8) of the SCA – www.opsi.gov.uk/acts/acts2007/ukpga_20070027_en_6#pt3-ch1-pb1-11g68

Extracts from the relevant legislation can be found at Appendix 2.

The full text of the Act is available at:
www.opsi.gov.uk/acts/acts2007/pdf/ukpga_20070027_en.pdf

APPENDIX 2

Extracts from statutory provisions

This appendix sets out extracts from the following statutory provisions:

- Schedules 1–3 of the Data Protection Act 1998 regarding fair processing requirements;
- section 29 of the Data Protection Act 1998;
- section 68 of the Serious Crime Act 2007;
- section 71 of the Serious Crime Act 2007; and
- section 72 of the Serious Crime Act 2007.

1. FAIR PROCESSING REQUIREMENTS IN THE DATA PROTECTION ACT 1998

The first data protection principle

Schedule 1, Part I, paragraph 1

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.

Schedule 1, Part II

Interpretation of the principles in Part I

The first principle

1

- (1) In determining for the purposes of the first principle whether personal data are processed fairly, regard is to be had to the method by which they 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.
- (2) Subject to paragraph 2, for the purposes of the first principle data are to be treated as obtained fairly if they consist of information obtained from a person who –

(a) is authorised by or under any enactment to supply it, or

(b) is required to supply it by or under any enactment or by any convention or other instrument imposing an international obligation on the United Kingdom.

2

(1) Subject to paragraph 3, for the purposes of the first principle personal data are not to be treated as processed fairly unless –

(a) in the case of data obtained 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 specified in sub-paragraph (3), and

(b) in any other case, the data controller ensures so far as practicable that, before the relevant time or as soon as practicable after that time, the data subject has, is provided with, or has made readily available to him, the information specified in sub-paragraph (3).

(2) In sub-paragraph (1)(b) “the relevant time” means –

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

(b) in a case where at that time disclosure to a third party within a reasonable period is envisaged –

- i. if the data are in fact disclosed to such a person within that period, the time when the data are first disclosed,
- ii. 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
- iii. in any other case, the end of that period.

(3) The information referred to in sub-paragraph (1) is as follows, namely –

(a) the identity of the data controller,

(b) if he has nominated a representative for the purposes of this 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, 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

(1) Paragraph 2(1)(b) does not apply where either of the primary conditions in sub-paragraph (2), together with such further conditions as may be prescribed by the Secretary of State by order, are met.

(2) The primary conditions referred to in sub-paragraph (1) are –

(a) that the provision of that information would involve a disproportionate effort, or

(b) that the recording of the information to be contained in the data by, or the disclosure of the data 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

[text omitted from this extract]

Schedule 2 **Conditions relevant for purposes of the first principle: processing of any personal data**

1–2

[text omitted from this extract]

3

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

4

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

5

The processing is necessary –

- (a) for the administration of justice,
- (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 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 relevant for purposes of the first principle: processing of sensitive personal data

1

[text omitted from this extract]

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) *[text omitted from this extract]*

3–6

[text omitted from this extract]

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 –
 - (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.

8–10

[text omitted from this extract]

2. RELEVANT PARTS OF SECTION 29 OF THE DATA PROTECTION ACT 1998

29 Crime and taxation

- (1) Personal data processed for any of the following purposes –
 - (a) the prevention and detection of crime,
 - (b) the apprehension or prosecution of offenders, or
 - (c) the assessment or collection of any tax or duty or of any imposition of a similar nature,are exempt from the first data protection principle (except to the extent to which it requires compliance with the conditions in Schedules 2 and 3) and section 7 in any case to the extent to which the application of those provisions to the data would be likely to prejudice any of the matters mentioned in this subsection.
- (2) *[text omitted from this extract]*

- (3) Personal data are exempt from the non-disclosure provisions in any case in which –
- (a) the disclosure is for any of the purposes mentioned in subsection (1), and
 - (b) the application of those provisions in relation to the disclosure would be likely to prejudice any of the matters mentioned in that subsection.
- (4)–(5) *[text omitted from this extract]*

3. RELEVANT SECTIONS OF THE SERIOUS CRIME ACT 2007

Sharing information with anti-fraud organisations

68 Disclosure of information to prevent fraud

- (1) A public authority may, for the purposes of preventing fraud or a particular kind of fraud, disclose information as a member of a specified anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation.
- (2) The information –
- (a) may be information of any kind; and
 - (b) may be disclosed to the specified anti-fraud organisation, any members of it or any other person to whom disclosure is permitted by the arrangements concerned.
- (3) Disclosure under this section does not breach –
- (a) any obligation of confidence owed by the public authority disclosing the information; or
 - (b) any other restriction on the disclosure of information (however imposed).
- (4) But nothing in this section authorises any disclosure of information which –
- (a) contravenes the Data Protection Act 1998 (c. 29); or
 - (b) is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23).
- (5) Nothing in this section authorises any disclosure by a relevant public authority of information whose subject-matter is a matter about which provision would be within the legislative competence of the Scottish Parliament if it were included in an Act of that Parliament.
- (6) In subsection (5) “relevant public authority” means a public authority which has (whether alone or in addition to other functions) functions which are exercisable within devolved competence (within the meaning given by section 54 of the Scotland Act 1998 (c. 46)).
- (7) This section does not limit the circumstances in which information may be disclosed apart from this section.
- (8) In this section –
- “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;
 - “information” includes documents;
 - “public authority” means any public authority within the meaning of section 6 of the Human Rights Act 1998 (c. 42) (acts of public authorities); and
 - “specified” means specified by an order made by the Secretary of State.

71 Code of practice for disclosure of information to prevent fraud

- (1) The Secretary of State must prepare, and keep under review, a code of practice with respect to the disclosure, for the purposes of preventing fraud or a particular kind of fraud, of information by public authorities as members of specified anti-fraud organisations or otherwise in accordance with any arrangements made by such organisations.

- (2) Before preparing or altering the code, the Secretary of State must consult –
- (a) any specified anti-fraud organisation;
 - (b) the Information Commissioner; and
 - (c) such other persons as the Secretary of State considers appropriate.
- (3) A public authority must have regard to the code in (or in connection with) disclosing information, for the purposes of preventing fraud or a particular kind of fraud, as a member of a specified anti-fraud organisation or otherwise in accordance with any arrangements made by such an organisation.
- (4) Nothing in this section applies in relation to any disclosure by a relevant public authority of information whose subject-matter is a matter about which provision would be within the legislative competence of the Scottish Parliament if it were included in an Act of the Scottish Parliament.
- (5) The Secretary of State must –
- (a) lay a copy of the code, and of any alterations to it, before Parliament; and
 - (b) from time to time publish the code as for the time being in force.
- (6) In this section –
- “information” and “public authority” have the same meaning as in section 68;
 - “relevant public authority” has the meaning given by section 68(6); and
 - “specified anti-fraud organisation” means any person which is a specified anti-fraud organisation for the purposes of section 68.
- “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.”

72 Data protection rules

In Schedule 3 to the Data Protection Act 1998 (c. 29) (conditions for processing sensitive personal data), after paragraph 7, insert –

APPENDIX 3

Good practice examples of layered fair processing notices for public authorities

The Information Commissioner recommends that a layered approach is adopted when issuing fair processing notices. The purpose of each layer is described in paragraph 26.

Public authorities wishing to enter into data sharing arrangements with a SAFO must decide for themselves the content and means of issue of fair processing notices, but good practice examples are set out below. They should seek to incorporate notices into existing forms of communication wherever possible.

LEVEL 1: SUMMARY TEXT – EXAMPLE FOR APPLICATION FORMS (for benefits, housing tenancies or employment, for example)

This authority is under a duty to protect the public funds it administers, and to this end may use the information you have provided on this form for the prevention and detection of fraud. It may also share this information under arrangements with a specified anti-fraud organisation under section 68 of the Serious Crime Act 2007.

For further information, see {web link to Level 2 notice on authority's website} or contact {name and contact details}

LEVEL 2: FULL TEXT – TO BE PUBLISHED ON THE PUBLIC AUTHORITY'S WEBSITE

Sharing of data with a specified anti-fraud organisation

Fraud costs the public sector an estimated £6.47 billion a year. It is in all our interests to prevent it. Public authorities have a particular responsibility to ensure that taxpayers' money is not taken out of the system fraudulently.

Public authorities are required by law to protect the public funds they administer. Section 68 of the Serious Crime Act 2007 was introduced as part of the Government's commitment to preventing fraud. Section 68 enables public authorities to disclose information for the purposes of preventing fraud, as a member of a specified anti-fraud organisation or otherwise in accordance with any arrangements made with such an organisation.

A specified anti-fraud organisation enables or facilitates the sharing of information for the prevention of fraud and is specified by an order made by the Secretary of State. A full list of specified anti-fraud organisations can be found at {web link}

{Name of public authority} may disclose the information you provide to a specified anti-fraud organisation for the purposes of preventing fraud.

Disclosures of information from a public authority to a specified anti-fraud organisation are subject to a Code of Practice. This may be found at {web link}

In addition, all disclosures must be made in accordance with the Data Protection Act 2008.

Further information

For further details, please contact {name and contact details}

Details of the organisations we share information with are as follows: {detail SAFO(s)}

