Northern Ireland Audit Office

The Code of Data Matching Practice of the Comptroller and Auditor General for Northern Ireland

Laid before the Northern Ireland Assembly pursuant to Article 4G of the Audit and Accountability (Northern Ireland) Order 2003

NIA 220/07-08 25 July 2008

For information about the Northern Ireland Audit Office please contact:

Northern Ireland Audit Office
106 University Street
BELFAST
BT7 1EU

Tel: 028 9025 1100
Email: info@niauditoffice.gov.uk
Website: www.niauditoffice.gov.uk

TABLE OF CONTENTS

Appendices

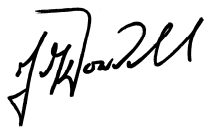
Foreword by the Comptroller and Auditor General

I am pleased to present this Code of Data Matching Practice to the Northern Ireland Assembly in accordance with the Audit and Accountability (Northern Ireland) Order 2003.

Under new statutory provisions inserted in the Audit and Accountability (Northern Ireland) Order 2003 by the Serious Crime Act 2007, I have been given the power to undertake data matching exercises for the purpose of assisting in the prevention and detection of fraud. This is a welcome and significant opportunity to tackle and reduce the scale of fraud against public sector bodies in Northern Ireland and beyond, and should provide a strong deterrent against future fraudulent acts. Data matching is a powerful tool in combating fraud, as demonstrated by the National Fraud Initiative which has helped participating bodies identify fraud and overpayments totalling in excess of £400 million.

In taking forward my new powers, I am aware of the importance of protecting personal information. The purpose of the Code of Data Matching Practice is to promote good practice in data matching and to help ensure that all taking part in data matching exercises comply with the law, especially the provisions of the Data Protection Act 1998. It also lets individuals know why their data is matched, the standards that apply and where they can find further information.

The Code has been drawn up following consultation with a range of stakeholders and has taken account of the Information Commissioner's Information Sharing Framework Code of Practice.



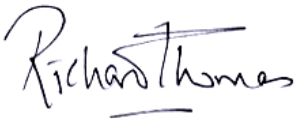
JOHN DOWDALL CB
Comptroller and Auditor General

Foreword by the Information Commissioner

The need to safeguard public funds from those who seek to make fraudulent claims continues to be a public concern. The Audit Commission has shown that data matching exercises go some way towards identifying the fraudulent claims, preventing overpayments, and enabling Participants to address these issues on the ground. On the basis of experiences in England, the National Fraud Initiative is now being expanded to Northern Ireland (through the Northern Ireland Audit Office) and Wales (through the Auditor General Wales). However, the collation and use of large quantities of personal information in this way continues to raise substantial data protection risks. Often personal information used in such exercises will not be implicated in any fraudulent activity, and it is essential that the Northern Ireland Audit Office, Auditor General Wales and their Participants take their obligations under the Data Protection Act seriously.

The Audit Commission involved the ICO in its initial Code of Data Matching in 2006 and both the Northern Ireland Audit Office and Auditor General Wales have involved the ICO in developing their own Codes of Data Matching. Both these bodies have drawn on the experiences of the Audit Commission and have undertaken work to clarify the framework of rules and practices designed to protect personal information in these data matching exercises. We particularly welcome their efforts to clarify the lawful basis for these exercises, the importance of transparency and the need for effective security as the exercises are expanded geographically. This helps to address legitimate concerns that potentially intrusive exercises are carried out in a proportionate, lawful and secure manner. We have also begun auditing the data processing undertaken as part of the National Fraud Initiative and we will continue to take this forward during the course of the year.

The importance of protecting personal information has never been so prominent and it is essential that this Code is followed in practice in order for it to be truly effective. Compliance with this Code should enable the continued identification of those individuals involved in fraudulent activity and, significantly, it should preserve and protect the rights of the majority who are not.



Richard Thomas, Information Commissioner

1. INTRODUCTION TO THE CODE

1.1 Role of the Comptroller and Auditor General

1.1.1 The Comptroller and Auditor General for Northern Ireland (referred to as the Comptroller and Auditor General in this Code) is the independent auditor of central government bodies in Northern Ireland, including Northern Ireland Departments and their Executive Agencies and a wide range of other public sector bodies, including Executive Non-Departmental Public Bodies and health and personal social services bodies. He undertakes financial audit and value for money examinations and the results of his work are reported to the Northern Ireland Assembly.

1.1.2 The Northern Ireland Audit Office supports the Comptroller and Auditor General in fulfilling his responsibilities. Certain Northern Ireland Audit Office staff are designated by the Department of the Environment as local government auditors. Local government auditors are mainly responsible for the audit of Northern Ireland District Councils.

1.1.3 Further information on the Comptroller and Auditor General and the Northern Ireland Audit Office can be found at www.niauditoffice.gov.uk.

1.2 Data Matching

1.2.1 It is essential that public bodies have adequate controls in place to prevent and detect fraud and error. Fraud in central and local government is a major concern of those bodies as well as of the Comptroller and Auditor General and local government auditors.

1.2.2 Data matching exercises, such as the National Fraud Initiative (NFI)[1], assist audited bodies to prevent and detect fraud and error. The exercises also help the Comptroller and Auditor General and local government auditors to assess the arrangements that audited bodies have put in place to deal with fraud.

1.2.3 Data matching involves comparing sets of data, such as the payroll or benefits records of a body, against other records held by the same or another body to see how far they match. This allows potentially fraudulent claims and payments to be identified. Where no match is found, the data matching process will have no material impact on those concerned. Where a match is found it indicates that there is an inconsistency that requires further investigation. In the NFI, for example, participating bodies have received a report of matches that they should follow-up, and investigate where appropriate, to detect

[1] The National Fraud Initiative is a data matching exercise which was established by the Audit Commission and has operated since 1996.

instances of fraud, over or underpayments and other errors, to take remedial action and update their records accordingly.

1.3 The new statutory framework

1.3.1 The Comptroller and Auditor General will conduct data matching exercises under his new statutory powers in the Audit and Accountability (Northern Ireland) Order 2003[2].

1.3.2 Under the new legislation:

a) the Comptroller and Auditor General may carry out data matching exercises for the purpose of assisting in the prevention and detection of fraud, as part of an audit or otherwise;

b) the Comptroller and Auditor General may require certain bodies to provide data for data matching exercises. Currently these are those bodies whose accounts are required to be audited by:

- the Comptroller and Auditor General, other than any body whose accounts are required to be audited by virtue of section 55 of the Northern Ireland Act 1998 which includes North/South Implementation Bodies audited jointly by the Comptroller and Auditor General and the Irish Comptroller and Auditor General; and
- a local government auditor;

c) other bodies may participate in his data matching exercises on a voluntary basis where the Comptroller and Auditor General considers it appropriate. Where they do so, the statute states that there is no breach of confidentiality and generally removes restrictions in providing the data to the Comptroller and Auditor General;

d) the requirements of the Data Protection Act 1998 continue to apply;

e) the Comptroller and Auditor General may disclose the results of data matching exercises where this assists in the prevention and detection of fraud, including disclosure to bodies that have provided the data, and to local government auditors, as appropriate;

f) the Comptroller and Auditor General may disclose both data provided for data matching and the results of data matching to the Audit Commission, the Auditor General for Wales, the Auditor General for Scotland, the Accounts Commission for Scotland and Audit Scotland, for the purposes of preventing and detecting fraud;

[2] The Serious Crime Act 2007 inserted provisions dealing with data matching exercises into the Audit and Accountability (Northern Ireland) Order 2003.

g) wrongful disclosure of data obtained for the purposes of data matching by any person is a criminal offence;

h) the Comptroller and Auditor General may charge a fee to any body participating in a data matching exercise, subject to obtaining the consent of the Department of Finance and Personnel in the case of a body whose functions are discharged on behalf of the Crown;

i) the Comptroller and Auditor General must prepare and publish a Code of Practice. All bodies conducting or participating in his data matching exercises, including the Comptroller and Auditor General himself, must have regard to the Code; and

j) the Comptroller and Auditor General may report publicly on his data matching activities.

1.4 Structure of the Code

1.4.1 The order in which the Code is set out reflects the chronological stages of a data matching exercise. This is designed to make it accessible to participating bodies.

1.4.2 Certain terms used in the Code are defined at Appendix 1. These terms appear in bold text for ease of identification.

1.5 Review of the Code

1.5.1 The Comptroller and Auditor General is required to review the Code periodically. He intends to update the Code in the light of changes in the law and to reflect comments and experience drawn from each data matching exercise.

1.6 Relationship of this Code to other information sharing codes

1.6.1 When participating in data matching exercises, bodies should have regard to any other relevant information sharing codes and guidance, including guidance from the Information Commissioner, as well as this Code.

1.7 Reproducing the Code

1.7.1 Bodies participating in data matching exercises may reproduce the text of this Code as necessary to ensure that all those involved are aware of their obligations in law and under this Code.

1.8 Queries on the Code

1.8.1 Any questions about this Code or a particular data matching exercise should be addressed to the Northern Ireland Audit Office NFI Co-ordinator, Northern Ireland Audit Office, 106 University Street, Belfast, BT7 1EU; email nficoordinator@niauditoffice.go.uk.

1.9 Complaints

1.9.1 Complaints about bodies participating in the Comptroller and Auditor General's data matching exercises should be addressed to those bodies. Complaints about the Comptroller and Auditor General's role in conducting data matching exercises can be made by phone, email or letter. Contact details can be found at www.niauditoffice.gov.uk.

2. THE CODE OF DATA MATCHING PRACTICE

2.1 Status, scope and purpose

2.1.1 This Code has been prepared following a statutory consultation process and has been laid before the Assembly by the Department of Finance and Personnel. It applies from 25 July 2008 until such time as a replacement Code is laid before the Assembly.

2.1.2 This Code applies to all data matching exercises conducted by or on behalf of the Comptroller and Auditor General under Articles 4A to 4G of the Audit and Accountability (Northern Ireland) Order 2003 for the purpose of assisting in the prevention and detection of fraud.

2.1.3 Any person or body conducting or participating in the Comptroller and Auditor General's data matching exercises must, by law, have regard to the provisions of this Code.

2.1.4 The purpose of this Code is to help ensure that the Comptroller and Auditor General, the Northern Ireland Audit Office, and all persons and bodies involved in data matching exercises comply with the law, especially the provisions of the Data Protection Act 1998 and to promote good practice in data matching. It includes guidance on the notification process for letting individuals know why their data is matched and by whom, the standards that apply and where to find further information.

2.1.5 This Code does not apply to the detailed steps taken by a **participant** to investigate matches from a data matching exercise. It is for **participants** to investigate matches in accordance with their usual practices for investigation of fraud and error.

2.1.6 The Information Commissioner regards the provisions of the Code as demonstrating a commitment to good practice standards that will help organisations to comply with data protection principles.

2.2 What is data matching?

2.2.1 The Audit and Accountability (Northern Ireland) Order 2003 defines data matching as the comparison of sets of data to determine how far they match. The purpose of data matching is to identify inconsistencies that may indicate fraud.

2.2.2 Where a match is found it indicates that there may be an inconsistency that requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out by the **participant**.

2.2.3 The data compared is usually personal data. Personal data may only be obtained and processed in accordance with the Data Protection Act 1998.

2.3 Who will be participating?

2.3.1 Under the Audit and Accountability (Northern Ireland) Order 2003, the Comptroller and Auditor General may require:

- any body whose accounts are required to be audited by the Comptroller and Auditor General, other than any body whose accounts are required to be audited by virtue of section 55 of the Northern Ireland Act 1998 which includes North/South Implementation Bodies audited jointly by the Comptroller and Auditor General and the Irish Comptroller and Auditor General; and
- any body whose accounts are required to be audited by a local government auditor

to provide data for data matching exercises. Bodies required to participate in this way are referred to in this Code as **mandatory participants**.

2.3.2 Any other body or person may provide data voluntarily for data matching exercises if the Comptroller and Auditor General decides that it is appropriate to use their data. This includes bodies or persons outside Northern Ireland. These are referred to as **voluntary participants** in this Code.

2.3.3 The Comptroller and Auditor General and public audit agencies in the UK (**the Audit Commission**, the Auditor General for Wales, the Auditor General for Scotland, the Accounts Commission for Scotland and Audit Scotland) may share the data they obtain with each other to enable cross-border matching. Any such disclosures must comply with the Data Protection Act 1998.

2.3.4 The Comptroller and Auditor General may conduct data matching exercises himself, or arrange for them to be done on his behalf (a body/person conducting an exercise on behalf of the Comptroller and Auditor is referred to as his 'agent(s)' in this Code). In practice, the Comptroller and Auditor General's data matching will usually be undertaken by the **Audit Commission**. The **Audit Commission**, and any firm with which it is contracted, will undertake the key aspects of the exercise on behalf of the Comptroller and Auditor General, including the collection and processing of data.

2.4 Governance arrangements

Nominated officers

2.4.1 The Director of Finance or equivalent senior named officer of each **participant** should act as **senior responsible officer** for the purposes of data matching exercises.

2.4.2 The **senior responsible officer** should nominate officers responsible for data handling, for follow up investigations and to act as a **key contact** with the Comptroller and Auditor General or his agent, and should ensure they are suitably qualified and trained for their role.

2.4.3 **Participants'** data protection officers should be involved in the arrangements for data handling, training and providing fair processing notices at an early stage.

2.4.4 The NFI Co-ordinator is the principal point of contact at the Northern Ireland Audit Office for the Comptroller and Auditor General's data matching exercises (nficoordinator@niauditoffice.gov.uk).

Guidance

2.4.5 For each data matching exercise, the Comptroller and Auditor General will make available guidance to all **participants**. This will set out the detailed responsibilities and requirements for participation. The most up-to-date guidance can be found on the Northern Ireland Audit Office's website at www.niauditoffice.gov.uk.

2.4.6 The guidance will contain:

a) a list of the responsibilities of the nominated officers at the **participant**;

b) specifications for each set of data to be included in the data matching exercise;

c) any further requirements and returns concerning the data to be provided;

d) a timetable for processing;

e) a data protection compliance return; and

f) information on how to interpret matches, and on co-operation between **participants**.

Secure NFI Website

2.4.7 In relation to data matching exercises undertaken by the **Audit Commission** on behalf of the Comptroller and Auditor General, **participants** will have access to other guidance material and training modules, including reports on the quality of their data, on the secure NFI website. This site is password-protected and encrypted and allows **participants** to transmit data to the **Audit Commission**, and the **Audit Commission** to make available the results of data matching in secure conditions.

Notification by data controllers of processing purposes

2.4.8 The Information Commissioner maintains a public register of data controllers that process data covered by the Data Protection Act 1998. Data controllers determine the purpose and manner in which personal data will be processed. Each register entry includes the name and address of the data controller, the purposes for which data are processed, and specified information in relation to each purpose. Those data controllers that are required to notify, but fail to do so, are committing a criminal offence. It is the responsibility of all **participants** (both **mandatory** and **voluntary**) to ensure their notification to the Information Commissioner covers the Comptroller and Auditor General and his agents as recipients against the appropriate purpose(s) for the prevention and detection of fraud.

2.4.9 A Notification Handbook, which sets how to complete the required Notification Form, is available from the Information Commissioner's Office. Notification templates are available from the Information Commissioner for central government bodies, local authorities and health service bodies.

2.5 How the Comptroller and Auditor General chooses data to be matched

2.5.1 The Comptroller and Auditor General will only choose data sets to be matched where he has reasonable evidence that fraud is likely to be found as a result of matching those data sets. This will be a key consideration when the Comptroller and Auditor General decides whether it is appropriate to accept data from a **voluntary participant**, or to require data from a **mandatory participant**. Evidence may come from previous data matching exercises, from pilot exercises, from **participants** themselves or from other reliable sources of information.

2.5.2 The Comptroller and Auditor General will undertake new areas of data matching on a pilot basis to test their effectiveness in preventing or detecting fraud. Only where pilots achieve matches that demonstrate a significant level of potential fraud will they be extended nationally. A small number of serious incidents of fraud or a larger number of less

serious ones may both be treated as significant. The terms of this Code apply in full to pilot exercises. Pilot data must be provided in accordance with the provisions of the Data Protection Act 1998.

2.5.3 The Comptroller and Auditor General will review the results of each exercise in order to refine how it chooses the data for future exercises.

2.6 The data to be provided

2.6.1 The data required from **participants** will be the minimum needed to undertake the matching exercise, to enable individuals to be identified accurately and to report results of sufficient quality. This will be set out in the form of a data specification for each data set in the guidance for each exercise.

2.6.2 Any revisions to the data specifications will be published on the Northern Ireland Audit Office website at www.niauditoffice.gov.uk and notified to the **senior responsible officer** at each **participant** in good time to ensure that **participants** have early notification of any changes so they can prepare adequately.

2.7 Powers to obtain and provide the data

2.7.1 All **mandatory participants** must provide data for data matching exercises as required by the Comptroller and Auditor General. Failure to provide data without reasonable excuse is a criminal offence under Article 4B of the Audit and Accountability (Northern Ireland) Order 2003.

2.7.2 The provision of data to the Comptroller and Auditor General by a **voluntary participant** does not amount to a breach of confidentiality and generally does not breach other legal restrictions. This is provided for in Article 4C of the Audit and Accountability (Northern Ireland) Order 2003.

2.7.3 **Patient data** may not be shared voluntarily, and so may only be used in data matching if the Comptroller and Auditor General requires it from a **mandatory participant**.

2.7.4 Whether **participants** provide data on a mandatory or voluntary basis, they are still required to provide the data in accordance with the provisions of the Data Protection Act 1998. In practice, this means that the disclosure of data must be in accordance with the data protection principles unless a relevant exemption within the Data Protection Act 1998 has been applied.

2.7.5 In most cases, data matching will take place in accordance with the data protection principles with no need to rely on exemptions. The

main exemptions in relation to obtaining and providing data are sections 34 and 35 of the Data Protection Act 1998. They would need to be considered in the circumstances of each data matching exercise. Relevant extracts from the Data Protection Act 1998, including the data protection principles, are set out in Appendix 2.

2.8 Fairness and transparency

2.8.1 The processing of data by the Comptroller and Auditor General in a data matching exercise is carried out with statutory authority. It does not require the consent of the individuals concerned under the Data Protection Act 1998. The relevant provisions of the Data Protection Act are included in Appendix 2.

Fair processing notices

2.8.2 The Data Protection Act 1998 normally requires **participants** to inform individuals that their data will be processed. Unless an exemption applies, for data processing to be fair, the first data protection principle requires data controllers to inform individuals whose data is to be processed of:

a) the identity of the data controller;
b) the purpose or purposes for which the data may be processed; and
c) any further information that is necessary to enable the processing to be fair.

2.8.3 The provision of this information is known as a fair processing notice. It enables people to know their data is being used in order to prevent or detect fraud and to take appropriate steps if they consider the use is unjustified or unlawful in their particular case.

2.8.4 **Participants** should, so far as is practicable, ensure that fair processing notices are actively provided, or at least made readily available to the individuals about whom they are sharing information. The notice should clearly set out an explanation that their data may be disclosed for the purpose of preventing and detecting fraud. The notice should state that the data will be provided to the Comptroller and Auditor General for this purpose. The notice should also contain details of how individuals can find out more information about the processing in question.

2.8.5 Communication with individuals whose data is to be matched should be clear, prominent and timely. It is good practice for reminder notices to be issued before each round of data matching exercises.

2.8.6 When providing data to the Comptroller and Auditor General or his agent, **participants** should submit a declaration confirming compliance with the fair processing notification requirements. If the

Comptroller and Auditor General becomes aware that fair processing requirements have not been adhered to, he should agree the steps necessary for the **participant** to achieve compliance.

Layered notices

2.8.7 The Information Commissioner recommends a layered approach to fair processing notices. Usually there are three layers: summary notice, condensed text and full text. Taken together, the three layers comprise the fair processing notice.

2.8.8 The *summary notice* should provide the minimum necessary content and should be provided to the individuals whose data is to be matched. Where practicable, it should point to where more detailed information can be found, for example, by providing web-links to the second and third layers, or contact details for a named person such as the **key contact** or data protection officer. **Participants** should make clear where individuals can obtain further information about how, why and by whom their data is being processed.

2.8.9 In the case of benefits, licences and applications for services, for example, the summary notice should usually be included on the application form used to collect the data in the first place.

2.8.10 In other cases, such as occupational pensioners, where **participants** usually communicate formally at least once a year, using, for example, a newsletter, summary notices should be included in these communications, which should be sent to named individuals in advance of each data matching exercise where practicable. This will avoid the cost of a separate mailing.

2.8.11 **Participants** should notify their employees both at the time of the original application for their post and before each exercise, for example, by including a summary notice in their payslip.

2.8.12 The *condensed text* should give a summary of the Comptroller and Auditor General's data matching exercises, and should be available on the **participant's** website as well as in hard copy on request. This layer should provide a link to the more detailed full text.

2.8.13 The *full text* should be available on the Northern Ireland Audit Office's website and should include an explanation of the legal basis for the Comptroller and Auditor General's data matching exercises and a more detailed description of how the initiative works.

2.8.14 While **participants** should decide the content and means of issue of fair processing notices for themselves, good practice examples of a three-layered approach are included at Appendix 3. Such notices may have the effect of deterring fraud as well as informing applicants

about the use of data in data matching.

2.8.15 The benefit of the layered approach are to give appropriate levels of fair processing information to different audiences, depending on their information needs. Individuals who wish to have a relatively short explanation can access this in a summary notice, while more comprehensive information can be made available for others.

Collection of new data

2.8.16 **Participants** should provide summary fair processing notices at the point of collecting personal data where practicable. **Participants** should in any event provide such notices before disclosure of the data to the Comptroller and Auditor General or his agent, unless it is impractical to do so.

Retrospective fair collection notices

2.8.17 Sometimes it will not be practicable to provide a summary fair processing notice at the time of the original collection of the data. In such cases, **participants** should provide retrospective summary fair processing notices at the earliest reasonable opportunity, and before disclosure to the Comptroller and Auditor General or his agent, unless it is impracticable to do so.

Deceased persons

2.8.18 Some of the data used for data matching exercises relates to deceased persons. Although information relating to a deceased individual cannot be regarded as personal data of the deceased person under the Data Protection Act 1998, common law rules of confidentiality may restrict disclosure in certain circumstances. In order not to cause unnecessary distress or harm, particular care and sensitivity should be taken in dealing with data concerning deceased persons throughout the exercise, but particularly in the case of investigation of matches.

2.9 Quality of the data

2.9.1 **Participants** should ensure that the data they provide to the Comptroller and Auditor General and his agents are of a good quality in terms of accuracy and completeness. Processing of inaccurate data could mean that the **participant** is in breach of data protection.

2.9.2 Before providing data for matching, **participants** should ensure that the data are as accurate and up to date as possible. Errors identified from previous data matching exercises should be rectified, and action taken to address any issues raised in data quality reports supplied to the **participant** from those exercises.

2.10 Security

2.10.1 The Comptroller and Auditor General, any body or firm undertaking data matching as his agent and all **participants** must put in place security arrangements for handling and storing data in data matching exercises.

2.10.2 These arrangements should ensure that:

a) specific responsibilities for security of data have been allocated to one or more managers;

b) security measures take appropriate account of the physical environment in which data are held, including the security of premises and storage facilities;

c) there are physical and logical controls to restrict access to data held electronically, so that only those named individuals who need to access the data for the purpose of data matching exercises can do so;

d) all staff with access to data are given training that is sufficient to enable staff to appreciate why and how they need to protect the data; and

e) if a breach of security occurs, or is suspected, authorised users are given new passwords or are required to change their passwords as soon as possible. The body responsible should consider what further steps it should take in the light of the Information Commissioner's guidance on management of security breaches.

2.10.3 All persons handling data as part of the data matching exercise should be made aware of their data protection, confidentiality and security obligations. Such staff should be subject to strict access authorisation procedures. Breach of authorisation procedures should attract appropriate disciplinary sanctions.

2.10.4 The **Audit Commission** will usually conduct data matching exercises on behalf of the Comptroller and Auditor General (see paragraph 2.3.4). Its secure NFI website is password-protected and encrypted to 128 bit SSL standards both for the transmission of data to the Commission and disclosure of the results of data matching to **participants**.

2.10.5 Any body or firm processing data as the Comptroller and Auditor General's agents will do so under a written agreement or contract that imposes requirements as to technical and organisational security standards so as to meet ISO 27001/02. The Comptroller and Auditor General will obtain assurance on compliance with these

standards from time to time.

2.11 Supply of data to the Comptroller and Auditor General

2.11.1 **Participants** must make all reasonable efforts to ensure the security of data in transmission to the Comptroller and Auditor General or his agents. They should only submit data to the **Audit Commission** via the secure NFI website. For other exercises, the submission of data should be by secure means (such as secure electronic transmission or delivery in person) as approved in writing by the Comptroller and Auditor General or his agent.

2.12 The matching of data by the Comptroller and Auditor General

2.12.1 The Comptroller and Auditor General will ensure he matches data fairly and for the purpose of assisting in the prevention and detection of fraud.

2.12.2 The techniques used by the Comptroller and Auditor General or his agents in data matching exercises must be those that are indicative of potential fraud only. They should be refined in the light of practical experience, having identified any lessons from reviewing the results of previous exercises.

2.12.3 All data stored electronically by the Comptroller and Auditor General or any body or firm undertaking data matching as his agent will be held on a secure, password-protected computer system maintained in a secure environment. All staff of the Comptroller and Auditor General and his agents who have access to personal data included in a data matching exercise will be subject to security clearance procedures.

2.12.4 All data provided for the purpose of data matching exercises will be backed up by the Comptroller and Auditor General or his agents at appropriate intervals, as reasonably necessary. Back-ups will be subject to the same security, destruction and access controls as the original data.

2.13 Access to the results by participants

2.13.1 All results from data matching exercises will be disclosed to **participants** via secure web-access or by other secure means. The results comprise the computer data file of reported matches and other relevant information arising from processing the data.

2.13.2 The **senior responsible officer** should ensure that the results of a data matching exercise are disclosed only to named officers for each type of result. The secure NFI website is designed for that

purpose.

2.13.3 All results from data matching exercises held by the **participant** other than on a secure website should be password protected on a secure, password-protected computer system. Any printed results should be kept in locked storage in a secure environment and should only be accessible to named individuals (as referred to in 2.10.2 c).

2.14 Following up the results

2.14.1 The detailed steps taken by a **participant** to investigate the results of data matching are beyond the scope of the Code. However, it is important to recognise that matches are not necessarily evidence of fraud. **Participants** should review the results to eliminate coincidental matches, and will want to concentrate on potentially fraudulent cases. In the process, they will need to identify and correct those cases where errors have occurred.

2.14.2 No decision should be made as a result of a data match until the circumstances have been considered by an investigator at the **participant**. Investigating Officers will find it helpful to refer to the guidance on how to interpret matches and cooperation between bodies prepared by the **Audit Commission**, which are available on its secure NFI website.

2.14.3 **Participants** should consider whether any corrections to personal data found to contain errors as a result of data matching are substantial enough to warrant notification to the persons concerned.

2.15 Disclosure of data used in data matching

2.15.1 The Comptroller and Auditor General may carry out data matching exercises for the purpose of assisting in the prevention and detection of fraud, as part of an audit or otherwise. He is supported by the Northern Ireland Audit Office, and may obtain the services of others (consultants and firms) in fulfilling his responsibilities.

2.15.2 Data obtained for the purpose of a data matching exercise may not be disclosed unless there is legal authority for so doing. This applies to both data obtained by the Comptroller and Auditor General for the purposes of data matching exercises and the results of the data matching.

2.15.3 There is legal authority for the Comptroller and Auditor General to disclose the data or results when this will assist in the prevention and detection of fraud. This includes, for example, disclosure of the results to the **participant** to investigate any matches, and disclosure to a local government auditor, as appropriate, to assess the **participant's**

arrangements for the prevention and detection of fraud. However, **patient data** may only be shared for a purpose relating to a relevant NHS body.

2.15.4 The Comptroller and Auditor General may also disclose data to public audit agencies in England, Wales and Scotland, to the bodies whose accounts they audit or arrange to be audited, and to the auditors they appoint.

2.15.5 A body in receipt of results from the Comptroller and Auditor General may only disclose them further if it is to assist in the prevention and detection of fraud, to investigate and prosecute an offence, or for the purpose of a disclosure otherwise required by statute.

2.15.6 The legal basis for these rules is Article 4D of the Audit and Accountability (Northern Ireland) Order 2003 (see Appendix 2). Any disclosure by the Comptroller and Auditor General, a **participant** or any other person in breach of Article 4D is a criminal offence.

2.16 Access by individuals to data included in data matching

2.16.1 Individuals whose data are included in a data matching exercise may have rights of access to information under the Data Protection Act 1998 or the Freedom of Information Act 2000. These should be dealt with in accordance with the organisation's general arrangements for responding to requests for information.

2.16.2 Individuals' usual rights of access to data held about them may be limited as a consequence of section 29 of the Data Protection Act 1998 where disclosure would be likely to prejudice, for example, the prevention or detection of a crime or the apprehension or prosecution of an offender. This determination should be made on a case by case basis by the organisation in receipt of the request for information. This means that individuals may, in some cases, be refused full access to information about them that has been processed in data matching exercises.

2.16.3 Individuals have rights under the Data Protection Act 1998 if data held about them is inaccurate. They should be able to check the accuracy of the data held on them by contacting the **participant** holding the data.

2.16.4 Individuals should not expect to be told about data or data matches concerning any other person unless that person has given consent, as this is likely to amount to a breach of data protection principles.

2.16.5 Information requests under the Freedom of Information Act 2000 may be subject to the law enforcement exemption under section

31, for example where its disclosure would be likely to prejudice the prevention and detection of a crime or the apprehension or prosecution of an offender, or the personal information exemption under section 40. These determinations should be made on a case by case basis by the organisation in receipt of the request for information.

2.16.6 Individuals who want to know whether their data is to be included in a data matching exercise can check the data specifications for each exercise in the Comptroller and Auditor General's guidance. The most up to date guidance can be found on the Northern Ireland Audit Office's website at www.niauditoffice.gov.uk.

2.16.7 **Participants** should have arrangements in place for dealing with complaints from individuals about their role in a data matching exercise. If a **participant** receives a complaint and the Comptroller and Auditor General is best placed to deal with it, the complaint should be passed on promptly to the Comptroller and Auditor General.

2.17 Role of auditors

2.17.1 In the case of **mandatory participants** (central and local government bodies), the Comptroller and Auditor General or a local government auditor, as appropriate, will be concerned to assess the arrangements that the **audited body** has in place to:

a) prevent and detect fraud generally; and

b) follow up and investigate matches and act upon instances of fraud and error.

2.17.2 Where a **participant** does not come under 2.17.1 it is a matter for the **participant** and its auditor to determine the role of the auditor in data matching and what disclosure to the auditor is appropriate.

2.18 Retention of data

2.18.1 Personal data should not be kept for longer than is necessary.

2.18.2 Access to the results of a data matching exercise on a secure website will not be possible after a minimum reasonable period necessary for **participants** to follow up matches. The Comptroller and Auditor General or his agents will notify the end date of this period to **participants.**

2.18.3 **Participants** and their auditors may decide to retain some data after this period. They may, for example, be needed as working papers for the purposes of audit, or for the purpose of continuing investigation or prosecution. **Participants** should consider what to retain in their individual circumstances in light of any particular obligations imposed

on them. **Mandatory participants** should discuss with the Comptroller and Auditor General or a local government auditor, as appropriate, what should be retained for the purposes of audit. All **participants** should ensure that data no longer required, including any data taken from a secure website, are destroyed promptly and rendered irrecoverable. Data retained will be subject to the requirements of the Data Protection Act 1998.

2.18.4 All original data submitted to the Comptroller and Auditor General or his agent in whatever form will be destroyed and rendered irrecoverable by the Comptroller and Auditor General or his agent within six months of submission by the **participant**. Subject to what is said below, all data that are derived or produced from that original data, including data held by any body or firm undertaking data matching as the Comptroller and Auditor General's agent, will be destroyed and rendered irrecoverable within three months of the conclusion of the exercise.

2.18.5 A single set of reference codes for previous matches, together with any comments made by **participants**' investigators, will be retained securely off-line by the Comptroller and Auditor General or his agent for as long as they are relevant. This is solely for the purpose of preventing unnecessary reinvestigation of previous matches in any subsequent data matching exercise.

2.19 Reporting of data matching exercises

2.19.1 The Comptroller and Auditor General will prepare and publish a report on his data matching exercises from time to time. This will bring his data matching activities and a summary of the results achieved to the attention of the public.

2.19.2 The Comptroller and Auditor General's report will not include any information obtained for the purposes of data matching from which a person or body may be identified unless the information is already in the public domain. The Comptroller and Auditor General may report on the progress of prosecutions resulting from data matching as these will be in the public domain.

2.20 Review of data matching exercises

2.20.1 The Comptroller and Auditor General will review the results of each exercise in order to refine how he chooses the data for future exercises and the techniques he uses.

2.20.2 As part of his review of each exercise, the Comptroller and Auditor General will consider any complaints or representations made by **participants** or by people whose data has been processed during the exercise.

3. COMPLIANCE WITH THE CODE AND THE ROLE OF THE INFORMATION COMMISSIONER

3.1 Compliance with the Code

3.1.1 Where the Comptroller and Auditor General becomes aware that a **participant** has not complied with the requirements of the Code, the Comptroller and Auditor General will notify the body concerned and seek to ensure that it puts in place adequate measures to meet the Code's requirements.

3.1.2 Questions and concerns about non-compliance with the Code should be addressed to the organisation responsible in the first instance (that is to the **participant** or, if it concerns the Comptroller and Auditor General's compliance, to the Comptroller and Auditor General) before contacting the Information Commissioner.

3.2 Role of the Information Commissioner

3.2.1 The Information Commissioner regulates compliance with the Data Protection Act 1998. If a matter is referred to the Information Commissioner, they would consider compliance with this Code by participants or the Comptroller and Auditor General in determining the nature of any enforcement action. Guidance on the Information Commissioner's approach to enforcement and their Data Protection Strategy is available on their website. Questions about the law and information sharing generally may be addressed to the Information Commissioner, who 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

Email: mail@ico.gsi.gov.uk
Website: www.ico.gov.uk (use on-line enquiries form for questions regarding the legislation for which the Information Commissioner is responsible)

3.2.2 The Information Commissioner has been invited (under section 51(7) of the Data Protection Act 1998) to review the Comptroller and Auditor General's data matching processing from time to time to assess compliance with the Data Protection Act 1998.

3.2.3 **Participants** are encouraged to invite the Information Commissioner's Office to review their procedures. The purpose of this review would be to assess **participants'** compliance with data protection principles when processing personal data for the purposes of data matching exercises.

APPENDIX 1

DEFINITIONS OF TERMS USED IN THE CODE

For the purposes of this Code the following definitions apply:

Term	Definition
Audit Commission	Audit Commission for Local Authorities and the National Health Service in England.
Audited Body	A body audited by the Comptroller and Auditor General or by a local government auditor.
Key Contact	The officer nominated by a participant's senior responsible officer to act as point of contact with the Comptroller and Auditor General and his agents, such as the Audit Commission, for the purposes of data matching exercises.
Mandatory Participant	A body whose accounts are required to be audited by: • the Comptroller and Auditor General, except for bodies audited by the Comptroller and Auditor General by virtue of section 55 of the Northern Ireland Act 1998; or • a local government auditor which is required by the Comptroller and Auditor General to provide data for a data matching exercise.
Participant	An organisation that provides data to the Comptroller and Auditor General, or his agents (such as the Audit Commission), for the purposes of a data matching exercise, which may be on either a mandatory or voluntary basis.
Patient Data	Data relating to an individual which are held for any of the following purposes and from which the individual can be identified - (a) preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health and social care services; (b) informing individuals about their physical or mental health or condition, the diagnosis of their condition or their care and treatment.
Senior Responsible Officer	The Director of Finance or other senior named officer of the participant responsible for ensuring compliance with this Code.

Voluntary Participant	An organisation from which the Comptroller and Auditor General considers it appropriate to accept data on a voluntary basis for the purpose of data matching

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 – the data protection principles and fair processing requirements
- Section 27 of the Data Protection Act 1998
- Section 29 of the Data Protection Act 1998
- Section 34 of the Data Protection Act 1998
- Section 35 of the Data Protection Act 1998
- Section 31 of the Freedom of Information Act 2000
- Section 40 of the Freedom of Information Act 2000
- Article 4A of the Audit and Accountability (Northern Ireland) Order 2003
- Article 4B of the Audit and Accountability (Northern Ireland) Order 2003
- Article 4C of the Audit and Accountability (Northern Ireland) Order 2003
- Article 4D of the Audit and Accountability (Northern Ireland) Order 2003 – extracts relating to the criminal offence associated with disclosing data matching results

1. Data protection principles and fair processing requirements in the Data Protection Act 1998

Schedule 1, Part I – The Principles

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.

2. 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.

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

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

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

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

7. 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.

8. [*text omitted from this extract*]

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

[*text omitted from this extract*]

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
[*text omitted from this extract*]

5

The processing is necessary—

(a) for the administration of justice,

(aa) *[text omitted from this extract]*

(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 – 5
[*text omitted from this extract*]

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) *[text omitted from this extract]*

(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 subparagraph (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 27 of the Data Protection Act 1998

Subject information and non-disclosures provisions

(1) [*text omitted from this extract*]

(2) In this Part "the subject information provisions" means-

(a) the first data protection principle to the extent to which it requires compliance with paragraph 2 of Part II of Schedule 1, and
(b) section 7.

(3) In this Part "the non-disclosure provisions" means the provisions specified in subsection (4) to the extent to which they are inconsistent with the disclosure in question.

(4) The provisions referred to in subsection (3) are-

(a) the first data protection principle, except to the extent to which it requires compliance with the conditions in Schedules 2 and 3,
(b) the second, third, fourth and fifth data protection principles, and
(c) sections 10 and 14(1) to (3).

(5) Except as provided by this Part, the subject information provisions shall have effect notwithstanding any enactment or rule of law prohibiting or restricting the disclosure, or authorising the withholding, of information.

3. Relevant parts of section 29 of the Data Protection Act 1998

Section 29 Crime and taxation

(1) Personal data processed for any of the following purposes-

a) the prevention or 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*]

4. Section 34 of the Data Protection Act 1998

Section 34 Information available to the public by or under enactment

Personal data are exempt from-

(a) the subject information provisions,
(b) the fourth data protection principle and section 14(1) to (3), and
(c) the non-disclosure provisions,

if the data consist of information which the data controller is obliged by or under any enactment, other than an enactment contained in the Freedom of Information Act 2000, to make available to the public, whether by publishing it, by making it available for inspection, or otherwise and whether gratuitously or on payment of a fee.

5. Relevant parts of section 35 of the Data Protection Act 1998

Section 35 Disclosures required by law or made in connection with legal proceedings etc.

(1) Personal data are exempt from the non-disclosure provisions where the disclosure is required by or under any enactment, by any rule of law or by the order of a court.

(2) [*text omitted from this extract*]

6. Relevant parts of sections 31 and 40 of the Freedom of Information Act 2000

Section 31 Law enforcement

(1) Information which is not exempt information by virtue of section 30 is exempt information if its disclosure under this Act would, or would be likely to, prejudice-

(a) the prevention or detection of crime,

(b) the apprehension or prosecution of offenders,

(c) - (i) [*text omitted from this extract*]

(2) [*text omitted from this extract*]

(3) The duty to confirm or deny does not arise if, or to the extent that, compliance with section 1(1)(a) would, or would be likely to, prejudice any of the matters mentioned in subsection (1).

Section 40 Personal information

(1) Any information to which a request for information relates is exempt information if it constitutes personal data of which the applicant is the data subject.

(2) Any information to which a request for information relates is also exempt information if--

(a) it constitutes personal data which do not fall within subsection (1), and

(b) either the first or the second condition below is satisfied.

(3) The first condition is--

(a) in a case where the information falls within any of paragraphs (a) to (d) of the definition of "data" in section 1(1) of the Data Protection Act 1998, that the disclosure of the information to a member of the public otherwise than under this Act would contravene--

(i) any of the data protection principles, or

(ii) section 10 of that Act (right to prevent processing likely to cause damage or distress), and

(b) in any other case, that the disclosure of the information to a member of the public otherwise than under this Act would contravene any of the data protection principles if the exemptions in section 33A(1) of the Data Protection Act 1998 (which relate to manual data held by public authorities) were disregarded.

(4) The second condition is that by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(c) of that Act (data subject's right of access to personal data).

(5) The duty to confirm or deny--

(a) does not arise in relation to information which is (or if it were held by the public authority would be) exempt information by virtue of subsection (1), and

(b) does not arise in relation to other information if or to the extent that either-

(i) the giving to a member of the public of the confirmation or denial that would have to be given to comply with section 1(1)(a) would (apart from this Act) contravene any of the data protection principles or section 10 of the Data Protection Act 1998 or would do so if the exemptions in section 33A(1) of that Act were disregarded, or

(ii) by virtue of any provision of Part IV of the Data Protection Act 1998 the information is exempt from section 7(1)(a) of that Act (data subject's right to be informed whether personal data being processed).

(6) [*text omitted from this extract*]

(7) In this section--

"the data protection principles" means the principles set out in Part I of Schedule 1 to the Data Protection Act 1998, as read subject to Part II of that Schedule and section 27(1) of that Act;

"data subject" has the same meaning as in section 1(1) of that Act;

"personal data" has the same meaning as in section 1(1) of that Act.

7. Extracts from Articles 4A-D of the Audit and Accountability (Northern Ireland) Order 2003

4A Power to conduct data matching exercises

(1) The Comptroller and Auditor General may conduct data matching exercises or arrange for them to be conducted on his behalf.

(2) A data matching exercise is an exercise involving the comparison of sets of data to determine how far they match (including the identification of any patterns and trends).

(3) The power in paragraph (1) is exercisable for the purpose of assisting in the prevention and detection of fraud.

(4) That assistance may, but need not, form part of an audit.

(5) A data matching exercise may not be used to identify patterns and trends in an individual's characteristics or behaviour which suggest nothing more than his potential to commit fraud in the future.

(6) [*text omitted from this extract*]

4B Mandatory provision of data

(1) The Comptroller and Auditor General may require-
(a) any body mentioned in paragraph (2); and
(b) any officer or member of such body,
to provide the Comptroller and Auditor General or a person acting on his behalf with such data (and in such form) as the Comptroller and Auditor General or that person may reasonably require for the purpose of conducting data matching exercises.

(2) The bodies are –
(a) any body (including a holder of a statutory office) whose accounts are required to be audited by the Comptroller and Auditor General, other than a body whose accounts are required to be so audited by virtue of section 55 of the Northern Ireland Act 1998 (c. 47);
(b) any body whose accounts are required to be audited by a local government auditor.

(3) A person who without reasonable excuse fails to comply with a requirement of the Comptroller and Auditor General under paragraph 1(b) is guilty of an offence and liable on summary conviction –
(a) to a fine not exceeding level 3 on the standard scale; and
(b) to an additional fine not exceeding £20 for each day on which the offence continues after conviction for that offence.

(4) [*text omitted from this* extract]

4C Voluntary provision of data

(1) If the Comptroller and Auditor General thinks it appropriate to conduct a data matching exercise using data held by or on behalf of a body or person not subject to Article 4B, the data may be disclosed to the Comptroller and Auditor General or a person acting on his behalf.

(2) A disclosure under paragraph (1) does not breach –

(a) any obligation of confidence owed by a person making the disclosure; or

(b) any other restriction on the disclosure of information (however imposed).

(3) But nothing in this Article authorises a disclosure which –

(a) contravenes the Data Protection Act (c.29); or

(b) is prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 (c. 23).

(4) Data may not be disclosed under paragraph (1) if the data comprise or include patient data.

(5) "Patient data" means data relating to an individual which are held for any of the following purposes and from which the individual can be identified –

(a) preventative medicine, medical diagnosis, medical research, the provision of care and treatment and the management of health and social care services;

(b) informing individuals about their physical or mental health or condition, the diagnosis of their condition or their care and treatment.

(6) This Article does not limit the circumstances in which data may be disclosed apart from this Article.

(7) Data matching exercises may include data provided by a body or person outside Northern Ireland.

4D Disclosure of results of data matching etc

(1) This Article applies to the following information—
(a) information relating to a particular body or person obtained by or on behalf of the Comptroller and Auditor General for the purpose of conducting a data matching exercise,
(b) the results of any such exercise.

(2) Information to which this Article applies may be disclosed by or on behalf of the Comptroller and Auditor General if the disclosure is—

(a) for or in connection with a purpose for which the data matching exercise is conducted,
(b) to a body mentioned in paragraph (3) (or a related party) for or in connection with a function of that body corresponding or similar to the audit functions of the Comptroller and Auditor General or a local government auditor under any statutory provision or the data matching functions of the Comptroller and Auditor General under Article A4; or
(c) in pursuance of a duty imposed by or under a statutory provision.

(3) The bodies are—
(a) the Audit Commission for Local Authorities and the National Health Service in England;
(b) the Auditor General for Wales;
(c) the Auditor General for Scotland;
(d) the Accounts Commission for Scotland;
(e) Audit Scotland.

(4)-(6) [*text omitted from this extract*]

(7) Information disclosed under paragraph (2) may not be further disclosed except—
(a) for or in connection with the purpose for which it was disclosed under sub-paragraph (a) or the function for which it was disclosed under sub-paragraph (b) of that paragraph;
(b) for the investigation or prosecution of an offence (so far as the disclosure does not fall within sub-paragraph (a)); or
(c) in pursuance of a duty imposed by or under a statutory provision.

(8) Except as authorised by paragraphs (2) and (7), **a person who discloses information to which this section applies is guilty of an offence** and liable—
(a) on conviction on indictment, to imprisonment for a term not exceeding two years, to a fine or to both, or
(b) on summary conviction, to imprisonment for a term not exceeding 6 months, to a fine not exceeding the statutory maximum or to both.

(9)-(10) [*text omitted from this extract*]

APPENDIX 3

EXAMPLES OF GOOD PRACTICE LAYERED FAIR PROCESSING NOTICES FOR PUBLIC BODIES

The Information Commissioner recommends that a layered approach is adopted when issuing fair processing notices. The purpose of each layer and the benefits of the approach are described in paragraph 2.8.

Participants in the Comptroller and Auditor General's data matching exercises 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 example, for benefits, housing tenancies, employment, market traders and taxi drivers)

{Name of Participant} 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 with other bodies responsible for auditing or administering public funds for these purposes.

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

Level 1 – Summary Text – Example for Payslips (for employees)

Please note that key payroll data may be provided to bodies responsible for auditing and administering public funds for the purposes of preventing and detecting fraud. For more details, see {web-link to Level 2 notice on Participant's website} or contact {name and contact details}.

<u>Level 1 – Summary Text – Example for Letters</u> (for example, to pensioners, employees and tenants, where communication by newsletter, payslip and so on is not practicable)

This example has been drafted for pensioners; the words in [square brackets] should be amended accordingly for employees, tenants etc.

Dear {name [of pensioner]}

THIS LETTER IS FOR INFORMATION ONLY – YOU ARE NOT REQUIRED TO TAKE ANY ACTION

We are participating in an exercise to promote the proper spending of public money.

We are required to protect the public funds we administer. We may share information provided to us with other bodies responsible for auditing or administering public funds in order to prevent and detect fraud.

The Comptroller and Auditor General currently requires us to participate in his anti-fraud initiative. For this initiative, we are providing details of [pensioners] so that they can be compared to information provided by other public bodies. This will ensure, for example, that [no pensions are being paid to persons who are deceased or no longer entitled, and that occupational pension income is being declared when housing benefit is applied for].

Sometimes wrong payments are made because of a genuine error. Previous exercises have uncovered instances of [pensioners] receiving too little [pension], resulting in the payments to [pensioners] being increased. These exercises, therefore, help promote the best use of public funds.

You do not need to respond to this letter. You may be contacted again in the future if the exercise suggests you are not receiving the correct amount of [pension]. Further information is available on our website at {Participant's web-link}. However, if you do have any questions, you should contact {name and contact details}, who can also provide hardcopies of information available on our website.

Level 2 – Condensed Text – to be published on Participant's website

The {name of Participant} is required to protect the public funds it administers. It may share information provided to it with other bodies responsible for auditing or administering public funds, in order to prevent and detect fraud.

The [Comptroller and Auditor General/Local Government Auditor – Delete as appropriate] audits the accounts of this {insert type of body}. The Comptroller and Auditor General is [also] responsible for carrying out data matching exercises under his powers in Articles 4A to 4G of the Audit and Accountability (Northern Ireland) Order 2003.

Data matching involves comparing computer records held by one body against other computer records held by the same or another body to see how far they match. This is usually personal information. Computerised data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it indicates that there may be an inconsistency that requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

The Comptroller and Auditor General currently requires us to participate in a data matching exercise to assist in the prevention and detection of fraud. We are required to provide particular sets of data to the Comptroller and Auditor General for matching. Details are set out on the Northern Ireland Audit Office website, www.niauditoffice.gov.uk.

The use of data by the Comptroller and Auditor General in a data matching exercise is carried out with statutory authority. It does not require the consent of the individuals concerned under the Data Protection Act 1998.

Data matching by the Comptroller and Auditor General is subject to a Code of Practice. This may be found at www.niauditoffice.gov.uk.

For further information on the Comptroller and Auditor General's legal powers and the reasons why he matches particular information, see {web-link to Level 3 notice on Northern Ireland Audit Office website}. For further information on data matching at this {insert type of body} contact {name and contact details}.

Level 3 – Full Text – to be published on the Northern Ireland Audit Office website

Comptroller and Auditor General's data matching exercises

Introduction

The Comptroller and Auditor General conducts data matching exercises to assist in the prevention and detection of fraud.

Data matching involves comparing sets of data, such as the payroll or benefits records of a body, against other records held by the same or another body to see how far they match. The data is usually personal information. The data matching allows potentially fraudulent claims and payments to be identified. Where a match is found it indicates that there may be an inconsistency that requires further investigation. No assumption can be made as to whether there is fraud, error or other explanation until an investigation is carried out.

The processing of data by the Comptroller and Auditor General in a data matching exercise is carried out with statutory authority under his powers in Articles 4A to 4G of the Audit and Accountability (Northern Ireland) Order 2003. It does not require the consent of the individuals concerned under the Data Protection Act 1998.

All bodies participating in the Comptroller and Auditor General's data matching exercises receive a report of matches that they should investigate, so as to detect instances of fraud, over or underpayments and other errors, to take remedial action and update their records accordingly.

Legal basis

The Comptroller and Auditor General will conduct data matching exercises under his new statutory powers in the Audit and Accountability (Northern Ireland) Order 2003. Under the new powers:

a) the Comptroller and Auditor General may carry out data matching exercises for the purpose of assisting in the prevention and detection of fraud, as part of an audit or otherwise;

b) the Comptroller and Auditor General may require certain bodies to provide data for data matching exercises. Currently these are all the bodies whose accounts are required to be audited by the Comptroller and Auditor General, with the exception of those audited by virtue of section 55 of the Northern Ireland Act 1998 (which includes North/South Implementation Bodies), or by a local government auditor;

c) other bodies and persons may participate in his data matching exercises on a voluntary basis where the Comptroller and Auditor General considers it appropriate. Where they do so, the statute states that there is no breach of confidentiality and generally removes other restrictions in providing the

data to the Comptroller and Auditor General;

d) the requirements of the Data Protection Act 1998 continue to apply;

e) the Comptroller and Auditor General may disclose the results of data matching exercises where this assists in the prevention and detection of fraud, including disclosure to bodies that have provided the data, and to local government auditors, as appropriate;

f) the Comptroller and Auditor General may disclose both data provided for data matching and the results of data matching to the Audit Commission, the Auditor General for Wales, the Auditor General for Scotland, the Accounts Commission for Scotland and Audit Scotland, for the purposes of preventing and detecting fraud;

g) wrongful disclosure of data obtained for the purposes of data matching by any person is a criminal offence;

h) the Comptroller and Auditor General may charge a fee to any body participating in a data matching exercise, subject to obtaining the consent of the Department of Finance and Personnel in the case of a body whose functions are discharged on behalf of the Crown;

i) the Comptroller and Auditor General must prepare and publish a Code of Practice. All bodies conducting or participating in his data matching exercises, including the Comptroller and Auditor General himself, must have regard to the Code; and

j) the Comptroller and Auditor General may report publicly on its data matching activities.

Bodies required to provide or which volunteer data for matching

Currently, the Comptroller and Auditor General requires the following bodies to provide data:

[*List to be updated by the Comptroller and Auditor General from time to time*]

In addition, the following bodies provide data to the Comptroller and Auditor General for matching on a voluntary basis:

[*List to be updated by the Comptroller and Auditor General from time to time*]

The data that is matched and the reasons for matching it

For information describing which data sets are matched by the Comptroller and Auditor General please refer to the guidance available on this website.

Code of Data Matching Practice

Data matching by the Comptroller and Auditor General is subject to a Code of Practice (see www.niauditoffice.gov.uk).

Further Information

Information about the Comptroller and Auditor General's data matching exercises may be found at www.niauditoffice.gov.uk. Alternatively please contact the Northern Ireland Audit Office NFI Co-ordinator, Northern Ireland Audit Office, 106 University Street, Belfast, BT7 1EU; email nficoordinator@niauditoffice.gov.uk.