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

November 2018

For information about the Northern Ireland Audit Office please contact:

Northern Ireland Audit Office
106 University Street
BELFAST
BT7 1EU

Tel: 028 9025 1000
Email: info@niauditoffice.gov.uk
Website: www.niauditoffice.gov.uk

TABLE OF CONTENTS

		Page
Foreword by the Comptroller and Auditor General		5
1.	Introduction to the Code	6
1.1	Role of the Comptroller and Auditor General	6
1.2	Data Matching	6
1.3	The statutory framework	7
1.4	Structure of the Code	8
1.5	Review of the Code	8
1.6	Relationship to data protection legislation and other information sharing codes	9
1.7	Reproducing the Code	9
1.8	Queries on the Code	9
1.9	Complaints	9
2.	The Code of Data Matching Practice	11
2.1	Status, scope and purpose	11
2.2	What is data matching?	11
2.3	Who will be participating?	12
2.4	Governance arrangements	13
2.5	How the Comptroller and Auditor General chooses data to be matched	14
2.6	The data to be provided	14
2.7	Powers to obtain and provide the data	15
2.8	Fairness and transparency	15
2.9	Quality of the data	17
2.10	Security	17
2.11	Supply of data to the Comptroller and Auditor General	19
2.12	The matching of data by the Comptroller and Auditor General	19
2.13	Access to the results by participants	19
2.14	Following up the results	20
2.15	Disclosure of data used in data matching	21
2.16	Access by individuals to data included in data matching	22
2.17	Role of auditors	23
2.18	Retention of data	23
2.19	Reporting of data matching exercises	24
2.20	Review of data matching exercises	25
3.	Compliance with the Code and the Role of the Information Commissioner	26
3.1	Compliance with the Code	26
3.2	Role of the Information Commissioner	26

Appendices

Appendix 1: About the National Fraud Initiative 28
Appendix 2: Definitions of terms used in the Code 29

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 statutory provisions inserted in the Audit and Accountability (Northern Ireland) Order 2003 by the Serious Crime Act 2007, I have the power to undertake data matching exercises for the purpose of assisting in the prevention and detection of fraud. This has provided significant opportunity to tackle and reduce the scale of fraud against public sector bodies in Northern Ireland and beyond, and provided a strong deterrent against future fraudulent acts. Data matching is a powerful tool in combating fraud, as demonstrated by the National Fraud Initiative (NFI), which is the principle means by which I exercise my data matching powers. The NFI has helped participating bodies identify fraud and overpayments totalling in excess of £1 billion across the UK since 1996. In Northern Ireland, almost £35 million of outcomes have been achieved since 2008.

In exercising my 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 data protection legislation. 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 Data Sharing Code of Practice (May 2011) (which is currently being revised to reflect the General Data Protection Regulation) and Right to be Informed guidance.

The Code creates a balance between the important public policy objective of preventing and detecting fraud, and the need to pay due regard to the rights of those whose data are matched for this purpose. I believe it will provide a robust framework for the future development of my data matching activities.

KIERAN DONNELLY
Comptroller and Auditor General

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 public reporting 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 for Communities 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, the health service and other public bodies 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 an organisation, against other records held by the same or another organisation, to see how far they match. This allows potentially fraudulent applications, 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 receive a report of matches which identify inconsistencies in the data held which may be indicative of fraud and which they should follow-up and investigate where appropriate, to

[1] The National Fraud Initiative (NFI) is a data matching exercise which was established by the Audit Commission and has operated since 1996. Following closure of the Audit Commission, responsibility for the NFI transferred to the Cabinet Office from 1 April 2015. For more details see **Appendix 1**. Participation in the NFI is the main means by which the Comptroller and Auditor General exercises his data matching powers.

detect instances of fraud, over or underpayments and other errors and, where appropriate, take remedial action and/or update their records accordingly.

1.2.4 NFI data matching currently comprises two main strands which are: batch matching different sets of data; and point of application matching, for the purpose of prevention and detection of fraud. See Appendix 1 for further information.

1.3 The statutory framework

1.3.1 The Comptroller and Auditor General, supported by the Northern Ireland Audit Office, will conduct **data matching exercises** under statutory powers inserted in the Audit and Accountability (Northern Ireland) Order 2003[2].

1.3.2 Under the 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 legislation** apply, so data cannot be voluntarily provided if to do so would be a breach of **data protection legislation**. In addition, sharing of **patient data** on a voluntary basis is prohibited.

e) The Comptroller and Auditor General may disclose the results of **data matching exercises** where this assists in the prevention and detection of

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

fraud, including disclosure to bodies that have provided the data, and to auditors, as appropriate, as well as in pursuance of a duty under an enactment.

f) The Comptroller and Auditor General may disclose both data provided for data matching and the results of data matching to the Cabinet Office, the Auditor General for Wales, the Auditor General for Scotland, the Accounts Commission for Scotland and Audit Scotland, where necessary, 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. A person found guilty of the offence is liable on conviction on indictment to imprisonment for a term not exceeding two years, to a fine or to both, or on summary conviction to imprisonment for a term not exceeding six months, to a fine not exceeding the statutory maximum or to both.

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 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.

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 2**. 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 will 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 to data protection legislation and other information sharing codes

1.6.1 In addition to this Code, when participating in **data matching exercises**, bodies should have regard to any other relevant information-sharing codes and guidance, including any statutory guidance from the Information Commissioner, which is available on the Information Commissioner's website at https://ico.org.uk/

1.6.2 References to compliance with, or in accordance with, **data protection legislation** should be construed as compliance with current **data protection legislation** applicable in the UK, as defined in the Data Protection Act 2018, which includes the General Data Protection Regulation (EU) 2016/679 (GDPR).

1.6.3 The Comptroller and Auditor General will review this Code in light of changes in the law and consider at that point whether the Code requires further amendment and, if so, the appropriate time to do so.

1.7 Reproducing the Code

1.7.1 Bodies participating in **data matching exercises** may reproduce the text of this Code as necessary to alert all those involved to obligations they may have under **data protection legislation**, in particular in relation to fairness and transparency in processing **personal data**.

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.gov.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.

1.9.2 Complaints about the Comptroller and Auditor General's role in conducting **data matching exercises** can be made in writing to the Director of Corporate Services at the above address, or by email to complaints@niauditoffice.gov.uk .

1.9.3 Further details of the complaints procedure may be found on the Northern Ireland Audit Office website at https://www.niauditoffice.gov.uk/complaints-page

1.9.4 If having followed the Northern Ireland Audit Office's complaints procedure you remain dissatisfied, you can refer your complaints to the Northern Ireland Public Service Ombudsman. Information on how to complain, together with a copy

of the complaints form, is available here: https://nipso.org.uk/nipso/making-a-complaint/how-do-i-make-a-complaint-to-nipso/

1.9.5 If there is a concern about the way that the Comptroller and Auditor General's **data matching exercises** deal with **personal data**, you can report this to the Information Commissioner: https://ico.org.uk/concerns/

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. It applies 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 **data protection legislation**, 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. However, it is incumbent on all **participants** in **data matching exercises** to ensure that their own procedures are compliant with the law as amended from time to time.

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 legislation**.

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, including the identification of patterns and trends. The purpose of data matching is to identify inconsistencies that may indicate fraud. However, the Act makes it clear that the powers to data match cannot be used to identify patterns and trends in an individual's characteristics or behaviour which suggest nothing more than the individual's potential to commit fraud in the future.

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 legislation**.

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 (not including **patient data**) voluntarily for **data matching exercises** if the Comptroller and Auditor General decides that it is appropriate to use their data and where to do so would not breach the **data protection legislation** or the Regulation of Investigatory Powers Act 2000. This includes bodies or persons outside Northern Ireland. These are referred to as **voluntary participants** in this Code. Note: **mandatory participants** can also submit additional data on a voluntary basis, that is, where data has not been required by the Comptroller and Auditor General.

2.3.3 The Comptroller and Auditor General and public audit agencies in the UK (the Cabinet Office, 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 data protection requirements.

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 General 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 Cabinet Office. The Cabinet Office, 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 privacy 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 https://www.niauditoffice.gov.uk/national-fraud-initative or by contacting the NFI Co-ordinator (see 2.4.4 for contact details). Additional, more operational, guidance will be provided within the secure NFI website.

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) details on the timings of each of the stages of a **data matching exercise**, with a full timetable for the data matching from submission of data to completion of recorded outcomes where relevant; and

e) information on how to interpret matches.

Secure NFI Website

2.4.7 In relation to **data matching exercises** undertaken by the Cabinet Office on behalf of the Comptroller and Auditor General, **participants** will have access to a secure NFI website which is password-protected and encrypted, allowing **participants** to transmit data to the Cabinet Office and the Cabinet Office to make available the results of data matching in secure conditions. The site also provides **participants** with access to further guidance material and training videos, including reports on the quality of their data.

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 to suggest that fraud may be occurring and this fraud is likely to be detected as a result of matching those data sets. The evidence may be the identification of anomalies in data sets (which are then further investigated by **participants** to see if actual fraud has occurred). The evidence may come from previous successful **data matching exercises** which have identified (significant) anomalies, from pilot exercises, from **participants** themselves or from other reliable sources of information, such as auditors. The presence of evidence 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**.

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.

2.5.3 The Comptroller and Auditor General will review the results of each exercise in order to ensure that it is appropriate to continue to match that data and also to make any refinements to how he matches data for future exercises, in particular whether the matches continue to show a significant level of fraud.

2.6 The data to be provided

2.6.1 The data required from **participants** will be the data that is adequate, relevant and limited to what is necessary to undertake the matching exercise, to enable individuals to be identified accurately and to report results of sufficient quality to meet the purpose of preventing and detecting fraud. This will be set out in the form of a data specification for each dataset in the Comptroller and Auditor General's guidance for each exercise.

2.6.2 Any revisions to the data specifications will be published in the NFI Instructions available on the Northern Ireland Audit Office website at

https://www.niauditoffice.gov.uk/national-fraud-initative and notified to the **senior responsible officer** at each **participant** in good time. This is 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** for data matching must comply with **data protection legislation**; must not be prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000; and may not include **patient data**. Otherwise, provision of that data 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 **data protection legislation**. In practice, this means that the disclosure of data must be in accordance with the data protection principles, or a relevant exemption has been applied (see http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/enacted .

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.

2.7.6 The **processing of data** by the Comptroller and Auditor General in a **data matching exercise** is carried out with statutory authority and therefore does not require the consent of the individuals concerned.

2.8 Fairness and transparency

2.8.1 **Data protection legislation** requires that data must be processed lawfully, fairly, in a transparent manner and for specified and legitimate purposes. In addition, **data controllers** must inform individuals that their data will be processed. Participating organisations must therefore provide a written notice, known as a privacy notice, which contains the information required by **data protection legislation**. Guidance on the Right to be Informed is available on the Information Commissioner's website.

Privacy notices

2.8.2 The privacy notice should contain information required by **data protection legislation**, such as:

a) the identity of the **data controller**;
b) the purpose or purposes for which the data may be processed;
c) the legal basis which the **data controller** is relying on for processing;
d) the categories of **personal data** collected;
e) the recipient or category of recipients of **personal data**;
f) details of retention period or criteria for retention;
g) the source of the **personal data**;
h) the right to lodge a complaint with the Information Commissioner; and
i) any further information that is necessary to enable the processing to be fair.

More detail on privacy notices is available at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

2.8.3 **Participants** should, so far as is practicable and unless an exemption from the fair processing requirement applies, ensure that privacy notices are provided, or 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 and include details of the legal basis on which the **data controller** relies for the processing. Consistent with the Information Commissioner's guidance (link provided above), the notice should specify who the data will be shared with. The notice should also contain details of how individuals can find out more information about the processing in question and how to exercise their rights.

2.8.4 Communication with individuals whose data is to be matched should be clear, prominent and timely. Where data matching is being undertaken at the point of application, then the notification provided at this time would suffice. Where data matching is being undertaken after the point of application, then it is good practice for further privacy notices to be issued before each round of data matching. The Information Commissioner's guidance (detailed above) advises on when an organisation should actively communicate privacy information.

2.8.5 When providing data to the Comptroller and Auditor General or his **agent**, **participants** should submit a declaration confirming compliance with the privacy notice requirements. If the Comptroller and Auditor General becomes aware that privacy notice requirements have not been adhered to, he should agree the steps necessary for the **participant** to achieve compliance. The Comptroller and Auditor General may seek input from the Information Commissioner as part of this process.

Timing of privacy notices

2.8.6 **Participants** should provide privacy notices at the point of collecting **personal data** where practicable. It is for **participants** to ensure, in line with the law as it stands at the time and in line with current ICO guidance, that they provide the appropriate form of notice at the appropriate time to meet the requirements of fairness and transparency. **Participants** should in any event provide such notices before disclosure of the data to the Comptroller and Auditor General or his **agent**, unless it would involve a disproportionate effort or proves impossible.

2.9 Quality of the data

2.9.1 **Participants** should ensure that the data they provide to the Comptroller and Auditor General or his **agent** are of a good quality in terms of accuracy and completeness, in line with **data protection legislation** which requires **personal data** to be accurate and, where necessary, kept up to date.

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 should be taken to address any issues raised in data quality reports supplied by the Comptroller and Auditor General or his **agent** to the **participant** on the secure NFI website**.**

2.9.3 Linked to the requirement under **data protection legislation** for data to be accurate is the right to have inaccurate **personal data** rectified. Please refer to the Information Commissioner's guidance on rectification: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/. Guidance is also available in the General Data Protection Regulation (GDPR) and Data Protection Act (DPA) 2018.

2.10 Security

2.10.1 The Comptroller and Auditor General, any organisation 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 a responsible person or persons within the organisation ;

(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) the C&AG, staff at the Northern Ireland Audit Office and at any organisation acting as the C&AG's **agent** who have access to **personal data** will be subject to security clearance procedures. As a minimum, all staff will be subject to Baseline Personnel Security Standard checks before they work on the NFI;

(e) 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. A record of data protection training should be retained for accountability purposes. **Participants** should ensure their staff have adequate training and also refer staff to the training modules on the secure NFI website that provide guidance on how to use the NFI website and how to review matches; and

(f) 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, where necessary. The body responsible should consider what further steps it should take in the light of the Information Commissioner's guidance on security and/or management of security breaches, including following its internal procedures and notifying its Data Protection Officer.

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 and undertake necessary training in this respect. Such staff should be subject to strict access authorisation procedures. Breach of authorisation procedures should attract appropriate disciplinary sanctions.

2.10.4 The Cabinet Office will usually conduct **data matching exercises** on behalf of the Comptroller and Auditor General (see paragraph 2.3.4). The NFI system is subject to the Cabinet Office's information assurance and risk management process. The outcome of this is that the system is HMG accredited annually to store and process data. Further details on this process can be provided on request (see contact details at paragraph 1.8.1).

2.10.5 Any firm processing data (the data processor) as the Cabinet Office's **agents** will do so under a contract in writing that imposes requirements as to technical and organisational security standards, and under which the firm may only act on instructions from the Cabinet Office (the **data controller**). The Cabinet Office reserves the right to review the firm's compliance against these standards at any time. In addition, the Cabinet Office requires annual security testing, supplemented by additional tests as appropriate. The Comptroller and Auditor General will obtain assurance on compliance with these standards from time to time.

2.10.6 **Data protection legislation** includes requirements, in certain circumstances, to report **personal data** breaches to the Information Commissioner within 72 hours (see guidance on Information Commissioner's website). There is also a requirement to notify the data subject of data breaches in certain circumstances, dependent on the nature of the data and an assessment of the potential risk to data subjects (see Article 34 of the GDPR).

2.11 Supply of data to the Comptroller and Auditor General

2.11.1 **Participants** should only submit data to the Cabinet Office via the secure NFI website or use authorised **Application Programming Interfaces** (APIs) to automatically submit information to the NFI for matching. 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 Data matching must be lawful, fair and transparent. The Comptroller and Auditor General will ensure he matches data fairly and in line with his legislative powers, i.e. for the purpose of assisting in the prevention and detection of fraud.

2.12.2 The Comptroller and Auditor General, or his **agents** in **data matching exercises**, will apply data matching rules which seek to identify exact and fuzzy data matches which highlight an anomaly which may indicate fraud.

2.12.3 All data stored electronically by the Cabinet Office, acting as the Comptroller and Auditor General's **agent**, or any organisation or firm undertaking data matching on their behalf, will be held on a system that has been assured as part of the Cabinet Office's information assurance and risk management process.

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, against an agreed schedule. Back-ups will be subject to the same security 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** only via the secure NFI website or authorised APIs. 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, for

example, a named officer can be given access to one or more dataset types. 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 secured in line with the NFI Security Policy that is provided on the secure NFI website. 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).

2.13.4 Where the **participant** is sharing data under the point of application data sharing agreement, the **participant** and service provider are responsible for the security of all information viewed or extracted from the system and are responsible for ensuring appropriate security controls are implemented. The Comptroller and Auditor General's **agents** are only responsible for the security of the information up to the web-portal interface and are not responsible for the security of the **participant** and service provider end-point systems that view or extract the information on the portal.

2.13.5 The Comptroller and Auditor General and his **agents** shall ensure that procedures and system security controls are in place, relating to information disclosed for data matching, that reflect the provisions in this Code and **data protection legislation,** to:

- make accidental compromise of, damage to, or loss of the information unlikely during storage, handling, use, processing, transmission or transport;
- deter deliberate compromise, or opportunist attack; and
- dispose of or destroy **personal data** in a manner to make reconstruction unlikely.

2.13.6 The Comptroller and Auditor General's **agents** and **participants** shall ensure that the systems used to connect to the NFI web portal do not pose any security risk to the NFI system. Any data traffic that is identified or regarded as malicious by the Comptroller and Auditor General or his **agents** may result in the connection to the **participant** being severed immediately.

2.14 Following up the results

2.14.1 The detailed steps taken by a **participant** to investigate the results of data matching are outside 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 both interpretation of matches and co-operation between **participants**, prepared by the Cabinet Office and available on its secure NFI website.

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

2.14.4 **Participants** should notify the Comptroller and Auditor General or his **agents** of any amendments made to **personal data** to correct substantial errors, so that they can amend the NFI data and prevent further matches being generated due to the error.

2.15 Disclosure of data used in data matching

2.15.1 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.

2.15.2 There is legal authority for the Comptroller and Auditor General to disclose the data or results where that disclosure is for, or in connection with, the purpose for which it was obtained, i.e. for, or in relation to, the prevention and detection of fraud. This includes, for example, disclosure of the results to the **participant** to investigate any matches, and disclosure to auditors, as appropriate, to assess the **participant's** arrangements for the prevention and detection of fraud. However, if the data used for a **data matching exercise** includes **patient data**, it may only be disclosed so far as the purpose for which disclosure is made relates to a relevant NHS body.

2.15.3 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, to the auditors they appoint, or to a body or person acting on their behalf.

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

2.15.5 The legal basis for these rules is Article 4D of the Audit and Accountability (Northern Ireland) Order 2003 (see Appendix 3). Any disclosure by the Comptroller and Auditor General, a **participant** or any other person in breach of Article 4D is a criminal offence and the person may be liable on summary conviction to

imprisonment for a term not exceeding six months, a fine or both.

2.16 Access by individuals to data included in data matching

Rights under data protection legislation

2.16.1 Individuals whose **personal data** are included in a **data matching exercise** have the right under **data protection legislation** for confirmation that their data is being processed, access to their **personal data** and access to other supplementary information (which largely corresponds with the information that should be provided in a privacy notice). [There are also rights under the Freedom of Information Act 2000 – see below].

2.16.2 Requests for the **personal data** of the requester should be dealt with in accordance with the organisation's general arrangements for responding to such requests. The requests should be dealt with without undue delay and within one month, unless the requests are complex or numerous when it is possible to extend the time by a further two months. Further guidance is available from the Information Commissioner in this respect at https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-of-access/

2.16.3 Individuals' subject access rights may be limited as a consequence of exemptions from **data protection legislation**. 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**.

Accuracy of data

2.16.4 Individuals have rights under **data protection legislation** 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. There is also a right to have inaccurate data rectified (see paragraph 2.9.3).

2.16.5 Similarly, an individual can check the accuracy of data the Comptroller and Auditor General or his **agent** holds about them by making a written subject access request to the NFI Co-ordinator (see 1.8.1 for contact details).

Rights under Freedom of Information legislation

2.16.6 Rights under the Freedom of Information Act 2000 extend only to accessing official information held by a public authority. Requests for non-personal information under the Freedom of Information Act 2000 relating to **data matching exercises** may be subject to exemptions provided by the Freedom of Information Act, especially the law enforcement exemption (section 31). However, the law enforcement exemption would only relate to circumstances where disclosure would be likely to prejudice the prevention and detection of a crime or the apprehension or prosecution of an offender. Where a request is brought under the Freedom of Information Act, but is in fact a request for **personal data**,

then it should be dealt with under the right of access for **personal data** discussed above.

Inclusion of data

2.16.7 Individuals who want to know whether their data is to be included in a **data matching exercise** can check the most up to date guidance on the Northern Ireland Audit Office's website at https://www.niauditoffice.gov.uk/national-fraud-initative. The NFI Instructions will tell them what data sets and fields are collected and from which bodies, so they can determine from that information whether their **personal data** is likely to be included in the **data matching exercises** undertaken. Alternatively, this information can be found out by contacting the NFI Co-ordinator (see 1.8.1 for contact details).

Complaints

2.16.8 **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.

2.16.9 Complaints about the Comptroller and Auditor General's role in conducting **data matching exercises** will be dealt with under the Northern Ireland Audit Office's complaints procedure (see paragraph 1.9.2 for details).

2.17 Role of auditors

2.17.1 In the case of **mandatory participants**, the Comptroller and Auditor General or a local government auditor, as appropriate, will 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** must not be kept in a form which permits identification of data subjects for any longer than is necessary.

2.18.2 Access to the results of a **data matching exercise** on the secure NFI 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.** Details of data

retention and deletion are included in the NFI Privacy Notice on the Northern Ireland Audit Office's website at https://www.niauditoffice.gov.uk/national-fraud-initative.

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 the secure NFI website or shared via the NFI API, are destroyed securely and promptly, and rendered irrecoverable. Data retained will be subject to the requirements of **data protection legislation**.

2.18.4 Subject to what is said below, all original data transmitted to the Comptroller and Auditor General or his **agents**, including data derived or produced from that original data and data held by any firm undertaking data matching as the Comptroller and Auditor General's **agent**, will be securely destroyed and rendered irrecoverable within three months of the conclusion of the exercise.

2.18.5 In the event that any data is submitted on hard media then the data on the media will be securely destroyed and rendered irrecoverable by the Comptroller and Auditor General or his **agents** as soon as it has been uploaded onto the secure NFI environment. This will be within one month of submission by the **participant**.

2.18.6 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** in line with a defined retention schedule. 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 may be identified, unless the information is already in the public domain and it is fair and lawful to use it. The Comptroller and Auditor General may report on the progress of prosecutions resulting from data matching to the extent the information is already in the public domain and any such reporting is compliant with **data protection legislation**.

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 **data protection legislation**. If a matter is referred to the Information Commissioner, he or she would consider compliance with this Code by **participants** or the Comptroller and Auditor General in determining whether or not, in the view of the Information Commissioner, there has been any breach of **data protection legislation**, and where there has been such a breach, whether or not any enforcement action is required and the extent of such action. Guidance on the Information Commissioner's approach to data breaches and enforcement is available on the Information Commissioner's website.

3.2.2 Questions about data protection and information sharing should initially be raised with the **participant's** data protection officer. Questions about data protection law may also be addressed to the Northern Ireland Regional Office of the Information Commissioner at:

The Information Commissioner's Office, 3rd Floor, 14 Cromac Place, Ormeau Road, Belfast, BT7 2JB.

ICO Helpline: 0303 123 1113

Email: ni@ico.org.uk

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

3.2.3 The Information Commissioner may be invited to review the Comptroller and Auditor General's data matching processes from time to time, to assess compliance with **data protection legislation**. **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**. Further information can be found on https://ico.org.uk/for-organisations/resources-and-support/audits/ .

Appendix 1 – About the National Fraud Initiative (NFI)

1. The NFI brings together a wide range of organisations across the UK public and private sectors to tackle fraud. By using data matching/analytics to compare different datasets across these organisations, the NFI is able to identify potentially fraudulent claims and overpayments.

2. The data is cross matched and also compared to key data sets provided by other **participants**, including government departments. The NFI also works with public audit agencies in all parts of the UK and key data sets provided by government departments to prevent and detect fraud. For example, the matching may identify that a person is listed as working while also receiving benefits and not declaring any income. The relevant organisation should then investigate and, if appropriate, amend or stop benefit payments.

3. The organisations that participate in the NFI are responsible for following up and investigating the matches, and identifying frauds and overpayments.

4. The NFI is an important part of the Comptroller and Auditor General's work to develop and provide access to data sharing, data matching and analytical products to help those working to counter fraud across Government to identify and reduce loss. Since the NFI became the responsibility of the Cabinet Office in March 2015, it has sought to build on the valuable work done in this area by the Audit Commission.

5. The NFI is working to increase usage of data matching and has added a fraud prevention product (AppCheck) to the established two yearly NFI fraud detection national exercise. This preventative product helps organisations to stop fraud at the point of application, thereby reducing administration and future investigation costs.

Examples of the data matches the NFI undertakes

Data match	Possible fraud or error
Pension payments to records of deceased people.	Obtaining the pension payments of a dead person.
Housing benefit payments to payroll records.	Failing to declare an income while claiming housing benefit.
Payroll records to records of failed asylum seekers.	Obtaining employment while not entitled to work in the UK.
Blue badge records to records of deceased people.	A blue badge being used by someone who is not the badge holder.
Housing benefit payments to records of housing tenancy.	Claiming housing benefit despite having a housing tenancy elsewhere.
Payroll records to other payroll records.	An employee is working for one organisation while being on long-term sick leave at another.

Appendix 2 - Definitions of terms used in the Code

For the purposes of this Code, the following definitions apply:

Term	Definition
Agent(s)	A body or person conducting a data matching exercise on behalf of the Comptroller and Auditor General (C&AG). In relation to the National Fraud Initiative (NFI), the C&AG's principal agent is the Cabinet Office which administers the NFI exercise. The C&AG and Cabinet Office are joint data controllers for the purposes of the NFI and their relationship is governed by a Memorandum of Understanding. "Agent" may also refer to the firm with which the Cabinet Office contracts to undertake the processing of data.
Application Programming Interface (API)	In computer programming, an application programming interface (API) is a set of subroutine definitions, protocols and tools for building software and applications.
Audited Body	A body audited by the Comptroller and Auditor General or by a local government auditor.
Data controller	The natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data.
Data matching exercise	The comparison of sets of data to determine how far they match (including the identification of any patterns and trends). The purpose of data matching is to identify inconsistencies that may indicate fraud.
Data protection legislation	As defined in section 3(9) of the Data Protection Act 2018 (DPA), as well as the General Data Protection Regulation 2016/679 (GDPR) and relevant regulations.
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 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 and 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** 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; or (b) informing individuals about their physical or mental health or condition, the diagnosis of their condition or their care and treatment.
Personal Data	Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
Processing of data	Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
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.