Cabinet Office

Code of Data Matching Practice

Laid before Parliament pursuant to schedule 9, paragraph 7 of the Local Audit and Accountability Act 2014

Consultation Draft issued: 21 September 2017

Contents

Foreword

I am pleased to present the Cabinet Office Code of Data Matching Practice, which will govern the exercise of the data matching powers provided to the Cabinet Office by the Local Audit and Accountability Act 2014.

The Act requires that the Code of Data Matching Practice is set out and followed by all organisations that participate in the Cabinet Office's data matching exercises.

The Code of Data Matching Practice has been developed with the benefit of input from a range of stakeholders who have responded to consultation. In drawing up this Code, the Cabinet Office has also taken account of the Information Commissioner's Data Sharing Code of Practice (May 2011) and Privacy notices, transparency and control Code of Practice (October 2016).

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. We believe it will provide a robust framework for the future development of the Cabinet Office's data matching activities.

Damian Green MP
First Secretary of State and Minister for the Cabinet Office

1. Introduction to the Code

1.1. Role of the Cabinet Office

1.1.1. The Cabinet Office is responsible within government for public sector efficiency and reform. Conducting data matching exercises to assist in the prevention and detection of fraud is one of the ways in which the Minister for the Cabinet Office fulfils this responsibility.

1.2. Background to the National Fraud Initiative

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

1.2.2. The National Fraud Initiative, known as the NFI, is a data matching exercise that has operated since 1996. The NFI assists public bodies and private sector organisations to prevent and detect fraud and error, and also help auditors to assess the arrangements that audited bodies have put in place to deal with fraud.

1.2.3. Data matching in the NFI involves comparing sets of data[1], such as the payroll or benefits records of a body or organisation, against other records held by the same or another body or 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 may require further investigation. In the NFI, 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 detect instances of fraud, over or under-payments and other errors and where appropriate take remedial action and/or update their records accordingly.

1.2.4. The 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. The four NFI products currently available are: National Exercise, ReCheck, FraudHub and AppCheck. See Appendix 1 for further information.

1.3. The statutory framework

1.3.1. From 2014 the Cabinet Office conduct data matching exercises under its statutory powers in the Local Audit and Accountability Act 2014. Previous exercises utilising the same powers were conducted as part of the Audit Commission Act 1998.

1.3.2. Under the Local Audit and Accountability Act 2014 legislation:

[1] A set of data consists of one or more records

- the Cabinet Office may carry out data matching exercises for the purpose of assisting in the prevention and detection of fraud;

- the Cabinet Office may require certain bodies (as set out in the Act) to provide data for data matching exercises;

- bodies may participate in its data matching exercises on a voluntary basis where the Cabinet Office considers it appropriate. Where they do so, the Act states that there is no breach of confidentiality and generally removes other restrictions in providing the data to the Cabinet Office. The requirements of the Data Protection Act 1998, however, continue to apply, so data cannot be voluntarily provided if to do so would be a breach of the Data Protection Act 1998. In addition sharing of patient data on a voluntary basis is prohibited.

- the Cabinet Office 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 auditors that it appoints as well as in pursuance of a duty under an enactment;

- the Cabinet Office may disclose both data provided for data matching and the results of data matching to the Auditor General for Wales, the Comptroller and Auditor General for Northern Ireland, the Auditor General for Scotland, the Accounts Commission for Scotland and Audit Scotland, for the purposes of preventing and detecting fraud;

- 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 summary conviction to a fine not exceeding level 5 on the standard scale;

- the Cabinet Office may charge a fee to a body participating in a data matching exercise and must set a scale of fees[2] for bodies required to participate;

- the Cabinet Office must prepare and publish a Code of Practice. All bodies conducting or participating in its data matching exercises, including the Cabinet Office itself, must have regard to the Code; and

- the Cabinet Office may report publicly on its data matching activities[3].

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.

[2] The Cabinet Office consult on the NFI work programme and scale of fees prior to each national exercise. The results of the consultation are published on GOV.UK

[3] On 4 November 2016 a report was published on GOV.UK that set out the results of the NFI in the period 1 April 2014 to 31 March 2016.

1.5. Review of the Code

1.5.1. The Cabinet Office will review this Code to ensure it remains fit for purpose. Should there be a significant change in the NFI's data matching exercises the Code will be updated to reflect these changes.

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 data or information sharing codes and guidance, including guidance from the Information Commissioner (Data Sharing Code of Practice (May 2011) and Privacy notices, transparency and control Code of Practice (October 2016).

1.6.2. At the time of writing this Code, the Data Protection Act 1998 is the relevant legislation governing the use of personal data. In May 2018 the EU General Data Protection Regulation ("GDPR") will come into effect. This Code has been written to reflect the law as it currently stands but recognises that from May 2018 the GDPR and the data protection bill (as enacted) will be the applicable legislation.

1.6.3. Where possible this Code also reflect forthcoming requirements under the GDPR and/or refers to guidance on this for participants.

1.6.4. References to compliance with, or in accordance with, the Data Protection Act 1998 should be construed post the change in the law in May 2018 as compliance with current data protection legislation applicable in the UK.

1.6.5. The Cabinet Office will review this Code in light of changes in the law to assess whether it remains fit for purpose.

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 the Data Protection Act 1998 or the GDPR or any subsequent legislation on use of personal data 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 Head of NFI, Cabinet Office, FEDG Team, 4th Floor, 1 Horse Guards Road, London SW1A 2HQ. Email: nfiqueries@cabinetoffice.gov.uk

1.9. Complaints

1.9.1. Complaints about bodies that are participating in the Cabinet Office's data matching exercises' should be addressed to the bodies themselves.

1.9.2. Complaints about the Cabinet Office's role in conducting data matching exercises will be dealt with under its complaints procedure.

1.9.3. Further details of the Cabinet Office's complaints procedure may be found at its website at https://www.gov.uk/government/organisations/cabinet-office/about/complaints-procedure.

1.9.4. If having followed the Cabinet Office's complaints procedure you remain dissatisfied, you can refer your Complaints to the Parliamentary and Health Service Ombudsman. Complaints to the Ombudsman must be referred by your MP to the Ombudsman. Information on how to complain, together with a copy of the complaints form is available here: http://www.ombudsman.org.uk/make-a-complaint/how-to-complain.

1.9.5. If there is a concern about the way that the NFI deals with personal data you can report this to the Information Commissioner: https://ico.org.uk/concerns/

2. The Code of Data Matching Practice

2.1. Status, scope and purpose

2.1.1. This Code has been drawn up by the Cabinet Office following a statutory consultation process, and has been laid before Parliament by the Secretary of State as required by Schedule 9, paragraph 7 of the Local Audit and Accountability Act 2014. It applies until such time as a replacement Code is laid before Parliament.

2.1.2. This Code applies to all data matching exercises conducted by or on behalf of the Cabinet Office under Schedule 9 of the Local Audit and Accountability Act 2014 for the purpose of assisting in the prevention and detection of fraud.

2.1.3. Any person or body conducting or participating in the Cabinet Office'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 Cabinet Office and its staff, auditors 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 requirements.

2.2. What is data matching?

2.2.1. The Local Audit and Accountability Act 2014 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 Act 1998.

2.3. Who will be participating?

2.3.1. Under the Local Audit and Accountability Act 2014, the Cabinet Office may require relevant authorities, best value authorities and NHS Foundation Trusts in England 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 Cabinet Office decides that it is appropriate to use their data and where to do so would not breach the Data Protection Act 1998 or the Regulation of Investigatory Powers Act 2000. This includes bodies or persons outside England and Wales. 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 Minister.

2.3.3. The Cabinet Office may undertake data matching exercises on behalf of its equivalent audit bodies (Auditor General for Wales, the Comptroller and Auditor General for Northern Ireland, the Auditor General for Scotland, the Accounts Commission for Scotland and Audit Scotland). These bodies may also share the data they obtain with each other to enable cross-border matching. Any such disclosures must comply with the data protection requirements.

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 Cabinet Office, 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 Head of NFI is responsible for data matching exercises at the Cabinet Office. (See 1.8.1 for contact details).

Cabinet Office Guidance

2.4.5. For each data matching exercise, the Cabinet Office 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 GOV.UK website at https://www.gov.uk/government/collections/national-fraud-initiative/ or by contacting the Head of NFI (see 1.8.1 for contact details). Additional, more operational, guidance will be provided within the secure NFI website.

2.4.6. The guidance will contain:

- a list of the responsibilities of the nominated officers at the participant;
- specifications for each set of data to be included in the data matching exercise;

- any further requirements and returns concerning the data to be provided;
- 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
- information on how to interpret matches.

Secure NFI website

2.4.7. The Cabinet Office has set up a secure, password-protected and encrypted website for its data matching exercises, known as the secure NFI website. This site allows 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.

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 Cabinet Office as recipients of personal data against the appropriate purpose(s) for the prevention and detection of fraud.

2.4.9. Information on notification is available from the Information Commissioner's Office. Notification templates are available from the Information Commissioner for local authorities, NHS and other public bodies. See https://ico.org.uk//for-organisations/register.

2.5. How the Cabinet Office chooses data to be matched

2.5.1. The Cabinet Office will only choose data sets to be matched where it 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). This 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 Cabinet Office decides whether it is appropriate to accept data from a **voluntary participant**, or to require data from a **mandatory participant**.

2.5.2. The Cabinet Office 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 should 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 Cabinet Office 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 it 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 minimum needed 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 data set in the Cabinet Office's guidance for each exercise.

2.6.2. Any revisions to the data specifications will generally be published on the GOV.UK website https://www.gov.uk/government/collections/national-fraud-initiative at least six months before any mandatory data is to be provided to the Cabinet Office, and will be notified to the senior responsible officer at each participant. 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 Cabinet Office.

2.7.2. The provision of data to the Cabinet Office for data matching by a voluntary participant must comply with the Data Protection Act 1998; must not be prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 and may not include patient data. Otherwise, the Local Audit and Accountability Act 2014 provides that provision of that data does not amount to a breach of confidentiality, and generally does not breach other legal restrictions (see paragraph 3 of schedule 9 of that Act).

2.7.3. Patient data[4] may not be shared voluntarily, and so may only be used in data matching if the Cabinet Office requires it from a mandatory participant.

2.7.4. As stated above 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 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.

[4] "Patient data" means data relating to an individual which are held for medical purposes (within the meaning of section 251 of the National Health Service Act 2006) and from which the individual can be identified.

2.8. Fairness and transparency

2.8.1. Being transparent and providing accessible information to individuals about how you use their personal data is a key element of the Data Protection Act 1998 and the GDPR. The most common way to provide this information is by a privacy notice (see further below).

2.8.2. The processing of data by the Cabinet Office in a data matching exercise is carried out with statutory authority. It does not therefore require the consent of the individuals concerned.

Privacy notices

2.8.3. The Data Protection Act 1998 requires participants to inform individuals that their data will be processed, unless an exemption applies. Specifically, the Data Protection Act provides, pursuant to the first data protection principle that for processing to be fair data controllers must inform individuals whose data is to be processed of:

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

2.8.4. The provision of this information is required to meet the requirements of fairness and transparency under the Data Protection Act 1998 and is often referred to as a privacy notice. It enables people to know that 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. The GDPR has further requirements about what information should be available to data subjects. There is information available on this on the Information Commissioner's website[5]: https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-notices-transparency-and-control/privacy-notices-under-the-eu-general-data-protection-regulation/

2.8.5. 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. The notice should state that the data will be provided to the Cabinet Office for this purpose. The notice should also contain details of how individuals can find out more information about the processing in question. For more information on privacy notices, participants should refer to the Information Commissioner's guidance: Privacy notices, transparency and control – a code of practice on communicating privacy information to individuals published 7 October 2016.

2.8.6. 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

[5] The GDPR has rules on giving privacy information to data subjects. These are more detailed and specific than the DPA and place an emphasis on making privacy notices understandable and accessible.

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 exercises.

2.8.7. When providing data to the Cabinet Office, participants should submit a declaration confirming compliance with the privacy notice requirements. If the Cabinet Office becomes aware that privacy notice requirements have not been adhered to, it should agree the steps necessary for the participant to achieve compliance.

Collection of new data

2.8.8. 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 Cabinet Office, unless it is impractical to do so.

Retrospective privacy notices

2.8.9. Where, for whatever reason, a privacy notice was not given at the time of the original collection of the data, participants should provide retrospective privacy notices at the earliest reasonable opportunity, and before disclosure to the Cabinet Office, unless it is impracticable to do so.

2.9. Quality of the data

2.9.1. Participants should ensure that the data they provide to the Cabinet Office are of a good quality in terms of accuracy and completeness in line with provisions in the Data Protection Act 1998 and the GDPR which require personal data to be accurate and where necessary kept up to date[6].

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 by the Cabinet Office to the participant on the secure NFI website.

2.10. Security

2.10.1. The Cabinet Office, any firm undertaking data matching as its 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;

[6] Both have provisions relating to rectifying inaccurate personal data.

(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 at the Cabinet Office and at any firm acting as its 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. Key staff will be subject to SC clearance which will commence when staff are appointed;

(e) all staff with access to data are given training that is sufficient to enable them to appreciate why and how they need to protect the data. 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. The body responsible should consider what further steps it should take in the light of any Information Commissioner's guidance on security and/or 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 and undertake necessary training in this respect[7]. 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's secure NFI website is password protected and encrypted to 256 bit SSL standards both for the transmission of data to the Cabinet Office and disclosure of the results of data matching to participants.

2.10.5. Any firm processing data as the Cabinet Office's agent will do so under a contract in writing that imposes requirements as to technical and organisational security standards so as to meet ISO 27001/02, and under which the firm may only act on instructions from the Cabinet Office. The Cabinet Office reserves the right to review the firm's compliance against these standards at any time. In addition the Cabinet Office will implement a rolling review programme.

2.10.6. Where the Cabinet Office undertakes data matching exercises on behalf of the Auditor General for Wales, the Comptroller and Auditor General for Northern Ireland, the Auditor General for Scotland, the Accounts Commission for Scotland or Audit Scotland, there should be a written contract in place which imposes the same requirements.

[7] Including when GDPR comes into force, training on the security requirements under that.

2.11. Supply of data to the Cabinet Office

2.11.1. Participants should only submit data to the Cabinet Office via the secure NFI website or using authorised APIs (Application Programming Interface) to automatically submit information to the NFI for matching.

2.12. The matching of data by the Cabinet Office

2.12.1. The Cabinet Office will ensure it matches data fairly and for the purpose of assisting in the prevention and detection of fraud.

2.12.2. The Cabinet Office will apply data matching rules which seek to identify exact and fuzzy data matches which indicate an anomaly which may indicate fraud.

2.12.3. All data stored electronically by the Cabinet Office or any firm undertaking data matching as its agent will be held on a secure encrypted, password protected computer system maintained in a secure environment.

2.12.4. All data provided for the purpose of data matching exercises will be backed up by the Cabinet Office or its agents at appropriate intervals, against an agreed schedule. Backups will be subject to the same security and access controls as the data.

2.13. Access to the results by the bodies concerned

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 the secure NFI website should be password protected on a secure encrypted, 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).

2.13.4. 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 Cabinet Office is only responsible for the security of the information up to the web-portal interface and is 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 Cabinet Office and service provider shall ensure that procedures and system security controls are in place relating to information disclosed for data matching that reflect the provisions in the Code and data protection legislation:

- make accidental compromise of, damage to, or loss of the information unlikely during processing, storage, handling, use, 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 service provider and participant 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 Cabinet Office and their service providers 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 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 Cabinet Office, 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.

2.14.4. Participants should notify the Cabinet Office of any amendments to personal data to correct substantial errors so that we 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 Cabinet Office for the purposes of data matching exercises and the results of the data matching.

2.15.2. There is legal authority for the Cabinet Office 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 the **auditor** 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 Cabinet Office may disclose data to:

1) a **relevant audit authority** (such as the Auditor General for Wales; the Comptroller and Auditor General for Northern Ireland; the Auditor General for Scotland; the Accounts

Commission for Scotland; Audit Scotland; a person designated as a local government auditor under Article 4 of the Local Government (Northern Ireland) Order 2005 (SI 2005/1968 (N.I.18));

2) the related parties in relation to a relevant audit authority are a:

   a) body or person acting on the authority's behalf;

   b) body whose accounts are required to be audited by the authority or by a person appointed by the authority; and

   c) person appointed by the authority to audit those accounts.

2.15.4. A body in receipt of results from the Cabinet Office 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 schedule 9, paragraph 4 of the Local Audit and Accountability Act 2014. Should the Cabinet Office, a **participant** or any other person disclose information to which this paragraph applies, except so far as that disclosure is authorised by sub-paragraph (2) or (7) of the 2014 Act, they will be guilty of an offence and liable on summary conviction to a fine not exceeding level 5 on the standard scale.

2.16. Access by individuals to data included in data matching

2.16.1. Individuals whose **personal data** are included in a data matching exercise have the right under section 7 of the Data Protection Act 1998 to be told what information an organisation holds about them; whether any personal data is being processed; a description of that data and the reason for processing it and whether that data will be given to any other organisation or people. Individuals also have a right to be given a copy of the information comprising the data and to be given details of the source of the data (where available). Individuals can also request information held by public authorities under the Freedom of Information Act 2000. However, where the information requested is **personal data** of the requester that request should be treated as subject access request. Requests for information or personal data should be dealt with in accordance with the organisation's general arrangements for responding to these requests. There are similar rights under the GDPR but there will be differences.

2.16.2. Individuals' subject access rights may be limited as a consequence of exemptions from the 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.

2.16.3. Individuals have rights under the Data Protection Act 1998 (and will have similar rights under GDPR) 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. Similarly, an individual can check the accuracy of data the Cabinet Office hold about them by making a written subject access request to the Head of the NFI. (See 1.8.1 for contact details).

2.16.5. Information requests under the Freedom of Information Act 2000 may be subject to exemptions on disclosure. Of particular relevance to the data matching of the NFI (i.e. for the purposes of the prevention and detection of fraud) is 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. Another possible exemption from disclosure under the Freedom of Information Act is the personal information exemption at section 40. Whether or not information is exempt from disclosure should be determined 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 most up to date information on the GOV.UK website. This will tell them what data sets and fields we collect and from which bodies so that they may be able to determine from that information whether their personal data is likely to be included in the data matching exercises the NFI undertakes (data requirements, data specifications and the list of mandatory bodies). Alternatively, this information can be found out by contacting the Head of NFI (see 1.8.1 for contact details).

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 Cabinet Office is best placed to deal with it, the complaint should be passed on promptly to the Cabinet Office.

2.16.8. Complaints about the Cabinet Office's role in conducting data matching exercises will be dealt with under the Cabinet Office's complaints procedure (see 1.9 for details).

2.17. Role of auditors

2.17.1. Where a participant is an audited body to which Public Sector Audit Appointments Limited[8] appoints an **auditor**, the **auditor** will be concerned to assess the arrangements that the **audited body** has in place to:

- prevent and detect fraud generally; and
- follow up and investigate matches and act upon instances of fraud and error.

2.17.2. Where a **participant** does not have an **auditor** appointed by the Public Sector Audit Appointments Limited, 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.

[8] Public Sector Audit Appointments Limited (PSAA) was incorporated by the Local Government Association (LGA) in August 2014. PSAA is a company limited by guarantee without any share capital and is a subsidiary of the Improvement and Development Agency (IDeA) which is wholly owned by the LGA.

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 Cabinet Office will notify the end date of this period to participants. A Data Deletion Schedule setting out the criteria for retaining and deleting data and matches will be published by the Cabinet Office on GOV.UK.

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. 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 promptly and rendered irrecoverable. Data retained will be subject to the requirements of the applicable Data Protection legislation.

2.18.4. Subject to what is said below, all original data transmitted to the Cabinet Office, including data derived or produced from that original data, including data held by any firm undertaking data matching as the Cabinet Office's agent, will be 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 destroyed and rendered irrecoverable by the Cabinet Office 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 Cabinet Office 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 Cabinet Office will prepare and publish a report on its data matching exercises from time to time on GOV.UK. This will bring its data matching activities and a summary of the results achieved to the attention of the public.

2.19.2. The Cabinet Office'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. The Cabinet Office may report on the prosecutions resulting from data matching to the extent the information is in the public domain already and any such reporting is compliant with data protection legislation.

2.20. Review of data matching exercises

2.20.1. The Cabinet Office will review the results of each exercise in order to refine how it chooses the data for future exercises and the techniques it uses

2.20.2. As part of its review of each exercise, the Cabinet Office should 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 Cabinet Office becomes aware that a **participant** has not complied with the requirements of the Code, the Cabinet Office should 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 Cabinet Office's compliance, to the Cabinet Office), before contacting the Information Commissioner.

3.1.3. If you wish to make a complaint about activities these should be addressed to the organisation responsible. If your complaint is concerning a **participant** then address it directly to a **participant**. If it is about the Cabinet Office's role see section 1.9 above for the complaints procedure.

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 Cabinet Office 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 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 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: 0303 123 1113 / 01625 545 745
Email: casework@ico.org.uk

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

3.2.3. The Information Commissioner has the power (under section 51(7) of the Data Protection Act 1998) to assess any processing of personal data for the following of good practice and shall inform the data controller of the results of such action. The Cabinet Office has invited the Information Commissioner to exercise that power and assess its processes and would encourage participants to do the same. 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 Cabinet Office'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.
Council tax records to electoral register.	A council tax payer gets council tax single person discount but the person is living with other countable adults, and so does not qualify for a discount.
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
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.
Auditor	A person appointed by Public Sector Audit Appointments Limited (PSAA) (under regulation 3 of the Local Audit (Appointing Person) Regulations 2015) as an auditor in relation to the accounts of an audited body.
Audited body	A local government or NHS body to which PSAA appoints the auditor. This includes all principal local government bodies such as police authorities, local probation boards and fire and rescue authorities as well as local councils. These bodies are listed in Schedule 2 to the Local Audit and Accountability Act 2014.
Best value authority	An authority described in section 1(1) of the Local Government Act 1999.
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. The Cabinet Office consider a data matching exercise to range from one application submission through to the full national exercise batch matching.
Key contact	The officer nominated by a participant's senior responsible officer to act as point of contact with the Cabinet Office for the purposes of data matching exercises.
Mandatory participant	A relevant authority, English best value authority or NHS Foundation Trust that is required by the Cabinet Office to provide data for a data matching exercise.
Participant	An organisation that provides data to the Cabinet Office 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 that are held for medical purposes (within the meaning of section 251 of the National Health Service Act 2006) and from which the individual can be identified. This includes both clinical data (for example, the medical records) and demographic data (for example, the name and address) of patients.

Term	Definition
Personal Data	Data relating to a living individual who can be identified from that data or from that data and other information which is in the possession of, or is likely to come into the possession of, the data controller and includes any expression of opinion about the individual and any indication of the intentions of the data controller or any other person in respect of the individual.
Relevant authorities	As defined in Schedule 2 of the Local Audit and Accountability Act 2014.
Relevant audit authority	As defined in Schedule 9, section 4, sub section (4) of the Local Audit and Accountability Act 2014.
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 Cabinet Office accepts data on a voluntary basis for the purpose of data matching.