Cabinet Office

Draft Code of Data Matching Practice

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

Contents

Foreword

This document is 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 2014 Act).

The 2014 Act requires that the Code of Data Matching Practice is prepared by Government 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.

The purpose of this Code is to explain the data matching work the NFI does and to give guidance to Cabinet Office and its staff, auditors and all persons and bodies involved in data matching exercises on the law, especially the provisions of data protection legislation, and to promote good practice in data matching.

It reflects the introduction of new data matching powers set out in the 2014 Act which came into force in [date tbc]. The powers which were added were those set out in paragraph 8(2) of Schedule 9 of the 2014 Act:

(a) to assist in the prevention and detection of crime (other than fraud);

(b) to assist in the apprehension and prosecution of offenders;

(c) to assist in the prevention and detection of errors and inaccuracies; and

(d) to assist in the recovery of debt owing to public bodies.

The Code of Data Matching Practice has taken into account the data protection legislation.

The Code of Data Matching Practice reflects both the important public policy objectives which underpin Schedule 9 (1) (4)[1] and 9 (8) (2)[2] of the 2014 Act with the rights of those whose data are matched. We believe it will provide a robust framework for the future development of the Cabinet Office's data matching activities using the new data matching powers laid on (date tbc).

Julia Lopez MP Parliamentary Secretary

[1] The power in sub-paragraph (1) is exercisable for the purpose of assisting in the prevention and detection of fraud.

[2] The purposes which have been added are:

(a) to assist in the prevention and detection of crime (other than fraud),
(b) to assist in the apprehension and prosecution of offenders,
(c) to assist in the prevention and detection of errors and inaccuracies, and
(d) to assist in the recovery of debt owing to public bodies.

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, prevention and detection of crime (other than fraud), the apprehension and prosecution of offenders, prevention and detection of errors and inaccuracies, recovery of debt owing to public bodies are ways in which the Minister for the Cabinet Office fulfils this responsibility.

1.2. Background to the National Fraud Initiative

1.2.1. The National Fraud Initiative, known as the NFI, is a **data matching exercise** that has operated since 1996.

1.2.2. Until 2021 [date tbc] the Minister for the Cabinet Office had the power to conduct data matching exercises for one purpose: to assist in the prevention and detection of fraud. In 2021[date tbc] the powers for data matching were expanded. This means the NFI can assist public bodies and private sector organisations by conducting data matching for the following purposes;

(a) to assist in the prevention and detection of fraud;

(b) to assist in the prevention and detection of crime (other than fraud);

(c) to assist in the apprehension and prosecution of offenders;

(d) to assist in the prevention and detection of errors and inaccuracies; and

(e) to assist in the recovery of debt owing to public bodies.

1.2.3. Data matching in the NFI involves comparing sets of data[3], such as the payroll or benefits records of a body or organisation, against other records. These might be details about a person that owes debt to a government department, public records where there are possible errors or details of an offender held by the same or another body or organisation to see how far they match.

1.2.4. This allows organisations to identify matches where there might be fraud, possible crime (other than fraud), and details about an offender, details to help reduce error or debt. The match will highlight where data is validated or not validated against particular records and used in line with one of the five data matching powers specified in the 2014 Act. The results of a match will be used by the organisation to decide whether no action is required, or whether further investigation is needed. Data matching may also identify new information which would again be subject to further investigation.

1.2.5. The NFI data matching currently comprises two main strands which are **batch matching** different sets of data and **point of application data set matching**. The four NFI products currently available are: National Exercise, ReCheck, FraudHub and AppCheck. See Appendix 1 for further information.

[3] A set of data consists of one or more records.

1.3. The statutory framework

1.3.1. From 2014 the Cabinet Office has conducted data matching exercises pursuant to its statutory powers in the 2014 Act. Previously, exercises utilising similar powers were conducted by the Audit Commission pursuant to the Audit Commission Act 1998.

1.3.2. Under the 2014 Act:

- the Cabinet Office may carry out data matching exercises for the following purposes;
    a) to assist in the prevention and detection of fraud;
    b) to assist in the prevention and detection of crime (other than fraud);
    c) to assist in the apprehension and prosecution of offenders;
    d) to assist in the prevention and detection of errors and inaccuracies; and
    e) to assist in the recovery of debt owing to public bodies.
- the Cabinet Office may require certain bodies (as set out in the 2014 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 2014 Act states that there is no breach of confidentiality and generally removes other restrictions in providing the data to the Cabinet Office;
- the requirements are subject to the **data protection legislation**, so data cannot be voluntarily provided by an organisation if to do so would be a breach of data protection legislation. Additionally, data cannot be provided if the disclosure is prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016. Furthermore, sharing of **patient data** on a voluntary basis is prohibited;
- the Cabinet Office may disclose the results of data matching exercises where this meets the specified purposes (i.e. it is for or in connection with a purpose for which the data matching exercise is conducted), 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;
- wrongful disclosure of data obtained by or on behalf of a relevant minister 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[4] for bodies required to participate;

[4] 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

- the Cabinet Office must prepare and publish a Code of Practice (this Code), and keep it under review. 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[5].

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.

1.4.3. This Code is designed to be used alongside the Information Commissioner's data sharing code of practice ("the ICO data sharing code")[6], as altered or replaced from time to time, and should be read alongside it.

1.5. Review of the Code

1.5.1. The Cabinet Office will continue to keep this Code under review to ensure it remains fit for purpose. Should there be any further significant change to the NFI's data matching exercises the Code will be updated again to reflect those changes.

1.6. Relationship to the data protection legislation and other information sharing codes

1.6.1. When participating in data matching exercises, in addition to having regard to this Code, bodies should adhere to data protection legislation and any other relevant data or 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 section 3 (9) of the Data Protection Act 2018.

1.6.3. The Cabinet Office will continue to keep this Code under review 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 the data protection legislation, in particular in relation to fairness and transparency in processing **personal data**.

[5] In July 2020 a report was published on GOV.UK that set out the results of the NFI in the period 1 April 2018 to 31 March 2020.

[6] https://ico.org.uk/media/about-the-ico/consultations/2615361/data-sharing-code-for-public-consultation.pdf

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, First Floor, 10 South Colonnade, Canary Wharf, E14 4PU. Email: nfiqueries@cabinetoffice.gov.uk

1.8.2. The contact details for the Cabinet Office Data Protection Officer (DPO) are:

DPO, Cabinet Office, 70 Whitehall, London, SW1A 2AS

Email: dpo@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 our Data Protection Officer (dpo@cabinetoffice.gov.uk). You can also report a concern via 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 2014 Act. 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 2014 Act for the following purposes;

(a) to assist in the prevention and detection of fraud;

(b) to assist in the prevention and detection of crime (other than fraud);

(c) to assist in the apprehension and prosecution of offenders;

(d) to assist in the prevention and detection of errors and inaccuracies; and

(e) to assist in the recovery of debt owing to public bodies.

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 explain the data matching work the NFI does and to give guidance to Cabinet Office and its staff, auditors and all persons and bodies involved in data matching exercises on 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** of the NFI to ensure their own procedures when participating 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/follow up matches from a data matching exercise. It is for participants to investigate/follow up matches in accordance with their usual practices.

2.2. What is data matching?

2.2.1. The 2014 Act defines a data matching exercise as an exercise involving the comparison of sets of data to determine how far they match (including the identification of patterns and trends). Data matching can be used in order to identify inconsistencies or previously unknown information that may indicate fraud, prevent and detect crime, assist in the apprehension and prosecution of offenders, identify error and inaccuracies, or help recover debt owed to public bodies.

2.2.1. The 2014 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 or circumstance that requires further investigation. No assumptions can be made from the match. Further investigation will be put in place by participant organisations.

2.2.3. The data compared are usually personal data. Personal data may only be obtained and processed in accordance with the data protection legislation.

2.3. Fairness Principles for data sharing under the debt power

2.3.1. Fairness is a key consideration in respect of the operation of the debt data sharing power. Where matching relates to the reduction of debt owed to public bodies, participant organisations will have their own fairness policies and practice in how they manage debt. Participants should be conscious of the impact debt collection practices have on vulnerable customers and customers in hardship. Organisations should seek to align with the principles of fairness for government debt collection set out in the Government Functional Standard for Debt[7].

2.4. Who will be participating?

2.4.1. Under the 2014 Act 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**.

2.4.2. 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 data protection legislation or the Investigatory Powers Act 2016. 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.

2.4.3. 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) where they have matching data matching powers. 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 legislation.

2.5. Governance arrangements

Nominated officers

2.5.1. 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.

2.5.2. 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 that they are suitably qualified and trained for their role.

2.5.3. Participants' data protection officers should be consulted on the arrangements for data handling, training and providing privacy notices at an early stage.

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

---

7 https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/886367/GovS-014-Debt-Functional-Standard.pdf

Cabinet Office Guidance

2.5.5. For each data matching exercise, the Cabinet Office will make available appropriate guidance to participants. This will set out the 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. Bespoke guidance will be made available for the other NFI data matching products and pilots ie ReCheck, FraudHub and AppCheck.

2.5.6. 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

2.5.7. The Cabinet Office has a secure, password-protected and encrypted website for its data matching exercises. This site allows participants to upload 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, including reports on the quality of their data.

2.6. How the Cabinet Office chooses data to be matched

2.6.1. The Cabinet Office will only choose data sets to be matched where it has reasonable evidence to suggest data can help identify instances where the match meets one of the five purposes set out in the Schedule 9 of the 2014 Act.

2.6.2. The evidence may be the identification of anomalies in data sets (which are then further investigated by participants). 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.

2.6.3. The Cabinet Office will undertake new areas of data matching on a pilot basis to test their effectiveness for data matching. Only where pilots achieve matches that demonstrate a significant level of success in one of the data matching areas should they be extended nationally. For fraud, a small number of serious incidents of fraud or a larger number of less serious ones may both be treated as significant. This principle will apply to the other data matching powers: success will be a significant level of crimes other than fraud, significantly aiding the apprehension of offenders, showing a significant level of error or inaccuracies or significantly helping reduce debt owed to public bodies.

2.6.4. The terms of this Code apply in full to pilot exercises. Pilot data must be provided in accordance with the provisions of current data protection legislation.

2.6.5. 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 effectively target fraud, crimes other than fraud, aid the apprehension of offenders, show a significant level of error or inaccuracies or help reduce debt owed to public bodies.

2.7. The data to be provided

2.7.1. 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 purposes of the powers outlined in the 2014 Act. 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.

2.7.2. 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.

2.8. Powers to obtain and provide the data

2.8.1. All mandatory participants must provide data for data matching exercises as required by the Cabinet Office and compliance with data protection legislation.

2.8.2. The provision of data to the Cabinet Office for data matching by a voluntary participant must comply with the data protection legislation; must not be prohibited by any of Parts 1 to 7 or Chapter 1 of Part 9 of the Investigatory Powers Act 2016, and may not include patient data. Otherwise, the 2014 Act 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 the 2014 Act).

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

2.8.4. 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 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.

2.8.5. The processing of data by the Cabinet Office in a data matching exercise is lawful and carried out with statutory authority. It does not require the consent of the individuals concerned. The legal basis for processing the personal data is that processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the data controller (Article 6 (1) (e) UK GDPR). Our Privacy notice provides details of our processing and can be found on GOV.UK.

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

2.9. Fairness and transparency

2.9.1. The data protection legislation includes requirements for data to 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 bodies must therefore provide a written notice, known as a privacy notice, which contains the information required by data protection legislation. Guidance is available from the Information Commissioner's Office website at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

2.9.2. The privacy notice should contain information required by data protection legislation such as:

- the identity and contact details of the data controller and their Data Protection Officer;
- the purpose or purposes for which the data may be processed;
- the legal basis which the controller is relying on for processing;
- the categories of personal data collected;
- the recipient or category of recipients of personal data;
- details of retention period or criteria on retention;
- the source of the personal data;
- whether the data is to be offshored and how that is being done lawfully;
- the rights of the data subject;
- the right to lodge a complaint with the Information Commissioner; and
- any further information that is necessary to enable the processing to be fair.

2.9.3. 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 five purposes 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. Such information can contain a link to the Cabinet Office's NFI Privacy Notice to provide further context.

2.9.4. 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 exercises. The Information Commissioner's guidance mentioned above advises on when an organisation should actively communicate privacy information.

2.9.5. The processing of personal data by competent authorities for law enforcement purposes is outside the UK GDPR's scope (e.g. the Police investigating a crime).

Instead, this type of processing is subject to the rules in Part 3 of the DPA 2018. Where data is matched for the purposes of detecting and preventing crime and the apprehension and prosecution of offender's participants can also refer to the ICO Guide to Law Enforcement Processing for further information.

2.9.6. 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. The Cabinet Office may seek input from the Information Commissioner as part of this process.

2.10. Data Privacy Impact Assessment

2.10.1. Each controller must consider whether a data matching exercise will trigger the legal duty to first conduct a Data Privacy Impact Assessment (DPIA).

2.11. Quality of the data

2.11.1. 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 the data protection legislation, which requires personal data to be accurate and, where necessary, kept up to date.

2.11.2. 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.

2.11.3. Linked to the requirement under the data protection legislation for data to be accurate is the right under data protection legislation to have inaccurate personal data rectified. Please refer to the Information Commissioner's guidance on rectification: ico.org.uk

2.12. Security

2.12.1. 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.

2.12.2. 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) all staff at the Cabinet Office and at any company 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

(BPSS) checks before they work on the NFI. Key staff will be subject to Security Check (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.

2.12.3. 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.

2.12.4. The NFI system goes through the Cabinet Office's information assurance and risk management process. The outcome of this is that the system is HM Government accredited to store and process data. Further details on this process can be provided on request (contact details can be found in 1.8.1).

2.12.5. Any company 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, 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 requires annual security testing, supplemented by additional tests as appropriate.

2.12.6. 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.

2.12.7. The data protection legislation includes requirements, in certain circumstances, to report personal data breaches to the Information Commissioner within 72 hours, where feasible. 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). For further guidance on security please refer to guidance, as updated from time to time, on the Information Commissioner's website.

2.13. Supply of data to the Cabinet Office

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

2.14. The matching of data by the Cabinet Office

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

crime (other than fraud), to assist in the apprehension and prosecution of offenders, to assist in the prevention and detection of errors and inaccuracies; or to assist in the recovery of debt owing to public bodies.

2.14.2. 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, crime, information on a suspected offender, error and inaccuracies or help recover debt owed to a public body.

2.14.3. All data stored electronically by the Cabinet Office or any firm undertaking data matching as its agent will be held on a secure system that has been assured as part of the Cabinet Office's information assurance and risk management process.

2.14.4. 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. Back-ups will be subject to the same security and access controls as the data.

2.15. Access to the results by the bodies concerned

2.15.1. 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.

2.15.2. 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.

2.15.3. All results from data matching exercises held by the participant other than on the secure NFI 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).

2.15.4. 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 endpoint systems that view or extract the information on the portal.

2.15.5. 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 this 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.

2.15.6. 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.

2.16. Following up the results

2.16.1. The detailed steps taken by a participant to investigate the results of data matching are outside the scope of this Code. However, it is important to recognise that matches are not necessarily evidence of fraud, an indicator of crime, the identification of an offender, error or inaccuracy, or identification of a person owing debt to a public body. The match will provide intelligence for organisations to act on appropriately. Participants should review the results to validate the information as far as possible before taking action. They will also have to exercise caution in validating information in a match before taking action. In the process, they will need to identify and correct those cases where errors have occurred.

2.16.2. 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.

2.16.3. 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 in line with the requirements of the data protection legislation and any guidance issued by the Information Commission in this respect.

2.16.4. 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.

2.17. Disclosure of data used in data matching

2.17.1. 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.

2.17.2. 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. This includes, for example, disclosure of the data and results to the participant to investigate any matches, and disclosure to the auditor. 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.

2.17.3. Additionally, the Cabinet Office may disclose the data and results of data matching 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)) or a related party where they have the relevant powers;

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.

2.17.4. A body in receipt of results from the Cabinet Office may only disclose them further if the requirements in Schedule 9 Paragraph 4(7) of the 2014 Act are met.

2.17.5. The legal basis for these rules is Schedule 9, paragraph 4 of the 2014 Act. 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 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.

2.18. Access by individuals to data included in data matching

2.18.1. Individuals whose **personal data** are included in a data matching exercise have rights under the 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 to other information under the Freedom of Information Act 2000.

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

2.18.3. 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.

2.18.4. Individuals have rights under the 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.

2.18.5. Similarly, an individual can check the accuracy of data the Cabinet Office holds about them by making a written subject access request to the Head of the NFI. (See 1.8.1 for contact details).

2.18.6. Requests for other (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 2000, 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 2000, 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.

2.18.7. Individuals who want to know whether their data is to be included in a data matching exercise, can check the most up to date 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[8], data specifications[9] and the list of mandatory bodies[10]). Alternatively, this information can be found out by contacting the Head of NFI (see 1.8.1 for contact details).

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

2.18.9. 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).

2.19. Role of auditors

2.19.1. Where a participant is an **audited body** to which Public Sector Audit Appointments Limited[11] 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.

2.19.2. 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.

2.20. Retention of data

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

2.20.2. 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 is published by the Cabinet Office on GOV.UK (please note this may be updated on GOV.UK).

2.20.3. **Participants** and their **auditors** may decide to retain some data after this period. Data 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

[8] https://www.gov.uk/guidance/national-fraud-initiative-public-sector-data-requirements
[9] https://www.gov.uk/guidance/national-fraud-initiative-public-sector-data-specifications
[10] https://www.gov.uk/government/publications/fair-processing-national-fraud-initiative/fair-processing-level-3-full-text
[11] 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.

destroyed promptly and rendered irrecoverable. Data retained will be subject to the requirements of data protection legislation.

2.20.4. 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.

2.20.5. 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**.

2.20.6. 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 re-investigation of previous matches in any subsequent data matching exercise.

2.21. Reporting of data matching exercises

2.21.1. 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.

2.21.2. 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 and such reporting is compliant with data protection legislation. 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.

2.22. Review of data matching exercises

2.22.1. 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

2.22.2. 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. The ICO has published a Data Sharing Code of Practice. This Code can be read alongside the Information Commissioner's data sharing code of practice.

3.2.2. 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.

3.2.3. 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).

3.2.4. The Information Commissioner may be invited to review the Cabinet Office'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 at 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 help tackle fraud, fight crime, prosecute and apprehend offenders, reduce error and inaccuracies, and recover debt owed to public organisations. By using data matching/analytics to compare different datasets across these organisations, the NFI is able to identify anomalies or previously unknown information to aid local investigations into fraud, crime (other than fraud), error and debt.

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. For example;

    a) the matching may identify that a person is listed as working while also receiving benefits and not declaring any income and fraud may have occurred;

    b) in a criminal investigation or search for an offender the data may highlight previously unknown information about a suspect eg employment or benefits claims;

    c) a match may highlight an inaccuracy or error in public records which would impact on the quality of service received by the recipient; and

    d) in cases where public debt is owed to a public organisation the match may help locate a person who owes debt or provide information on their ability to pay that debt in line with the promotion of fairness in debt management across the public sector.

3. The relevant organisation should then investigate and, if appropriate, amend or stop benefit payments.

4. The organisations that participate in the NFI are responsible for following up and investigating the matches.

5. 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. 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.

6. The NFI is working to increase usage of data matching and has added a point of application 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. The NFI are likely to develop products to align with the new powers introduced in 2021.

Examples of the data matches the NFI can undertake under its Fraud powers

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.

Examples of the data matches the NFI can undertake with the powers introduced in 2021

Data match	Link to the NFI powers introduced in 2021
Government records to government records	To remove duplicates in government records.
Government records to DWP deceased records	Help government departments to remove records of deceased persons where applicable
Name and date of birth details to NFI data pots	Help investigating authorities trace/locate people as part of their criminal investigations.
Name and date of birth details to NFI data pots	Help trace/locate individuals who owe debt to a public organisation and or trace information about other debts owed which can be used to aid the recovery of that debt (in adherence with the Fairness in Debt Management Principles).
Entitlements to benefits to NFI data pots.	Help local authorities ensure that all those entitled to benefits such as concessionary travel concessions have access to them.

Appendix 2 – Definitions of terms used in the Code

For the purposes of this Code the following definitions apply:

Term	Definition
Anomaly	May refer to inconsistency or previously unknown information.
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	All relevant authorities listed in schedule 2 of the 2014 Act must, under Part 3 of the 2014 Act comply with the requirement to appoint a local auditor. Section 7 of the 2014 Act requires a relevant authority to appoint a local auditor to audit its accounts for a financial year not later than 31 December in the preceding financial year. Public Sector Audit Appointments Limited (PSAA) is required under the Local Audit (Appointing Person) Regulations 2015) to appoint an auditor to all opted-in authorities.
Audited body	A local government or NHS body to which an auditor has been appointed (by PSAA or by a local appointment). 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 2014 Act.
Best value authority	An authority described in section 1(1) of the Local Government Act 1999.
Data controllers	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. The Cabinet Office considers a data matching exercise to range from one application submission through to the full national exercise batch matching.
Data protection legislation	As defined in the Data Protection Act 2018 (DPA) and includes the DPA as well as the UK General Data Protection Regulation (UK GDPR) and other relevant regulations.

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.
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 to the 2014 Act.
Relevant audit authority	As defined in Schedule 9 paragraph 4(4) to the 2014 Act.
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.