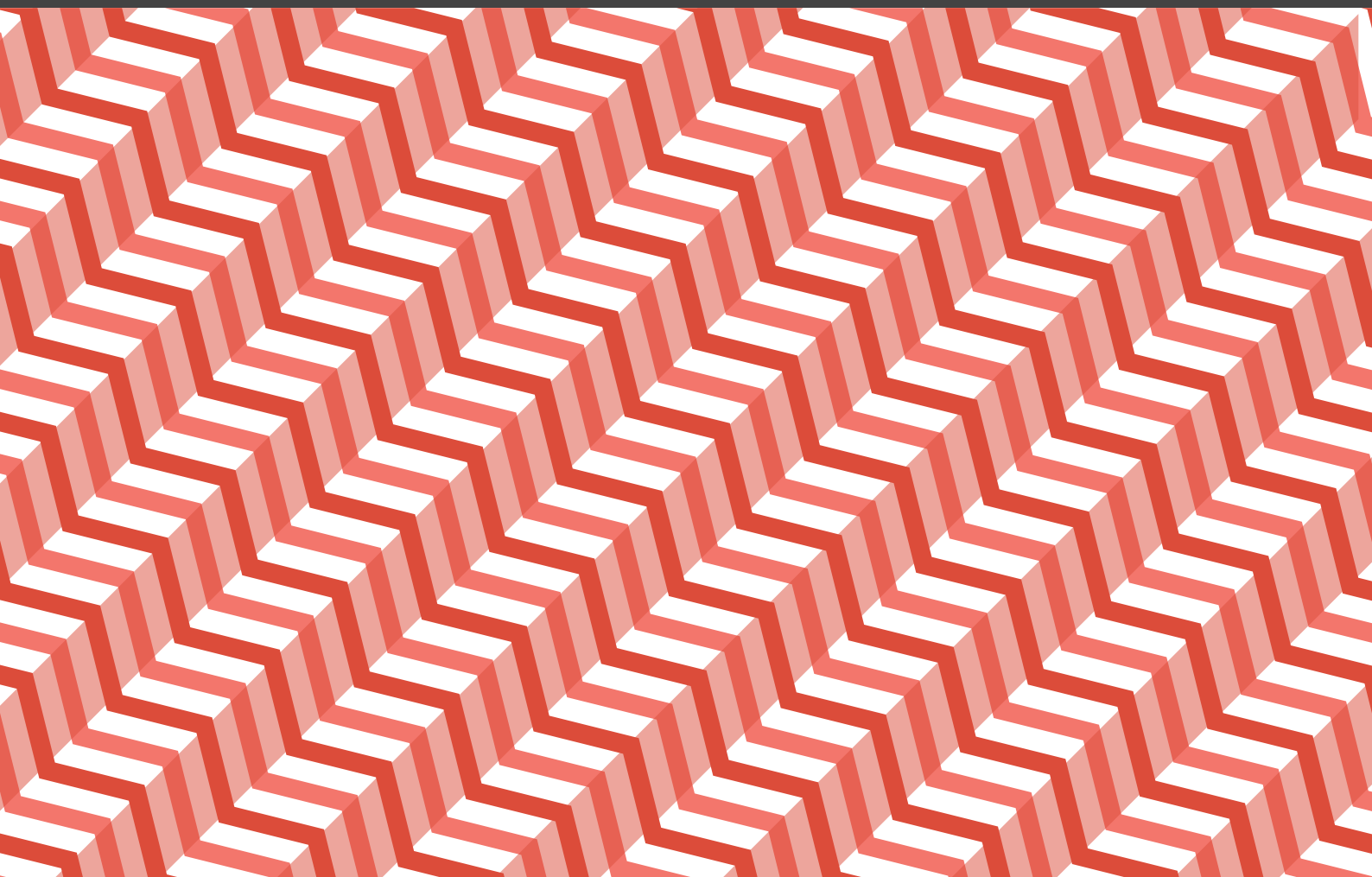
November 2018

Archwilydd Cyffredinol Cymru
Auditor General for Wales

Code of Data Matching Practice



I have prepared this Code of Data Matching Practice, following a statutory consultation process, for presentation to the National Assembly under the Public Audit (Wales) Act 2004.

Adrian Crompton
Auditor General for Wales
Wales Audit Office
24 Cathedral Road
Cardiff
CF11 9LJ

The Auditor General is independent of the National Assembly and government. He examines and certifies the accounts of the Welsh Government and its sponsored and related public bodies, including NHS bodies. He also has the power to report to the National Assembly on the economy, efficiency and effectiveness with which those organisations have used, and may improve the use of, their resources in discharging their functions.

The Auditor General also audits local government bodies in Wales, conducts local government value for money studies and inspects for compliance with the requirements of the Local Government (Wales) Measure 2009.

The Auditor General undertakes his work using staff and other resources provided by the Wales Audit Office, which is a statutory board established for that purpose and to monitor and advise the Auditor General.

© Auditor General for Wales 2018

You may re-use this publication (not including logos) free of charge in any format or medium. If you re-use it, your re-use must be accurate and must not be in a misleading context. The material must be acknowledged as Auditor General for Wales copyright and you must give the title of this publication. Where we have identified any third party copyright material you will need to obtain permission from the copyright holders concerned before re-use.

For further information, or if you require any of our publications in an alternative format and/or language, please contact us by telephone on 029 2032 0500, or email info@audit.wales. We welcome telephone calls in Welsh and English. You can also write to us in either Welsh or English and we will respond in the language you have used. Corresponding in Welsh will not lead to a delay.

Mae'r ddogfen hon hefyd ar gael yn Gymraeg.

Contents

Foreword by the Auditor General for Wales

I am pleased to present this Code of Data Matching Practice to the National Assembly for Wales under the Public Audit (Wales) Act 2004.

The Public Audit (Wales) Act 2004 gives me powers to carry out data matching exercises. The statute requires that I prepare this Code, following consultation, and that all participating bodies follow the Code in data matching exercises carried out under this legislation.

In 2017 my predecessor, Huw Vaughan Thomas, asked the Finance Committee of the National Assembly to consider seeking changes to update the legislation; for example, so that it includes further purposes, such as the prevention and detection of crime other than fraud. Such updating is needed to enable the scope of work in Wales to keep pace with that of other UK audit agencies. If such updating is forthcoming, I shall, of course, review the Code to ensure that it appropriately takes account of them.

The data matching powers provided to me, and the exercise of those powers with other UK auditors, provide a powerful means of preventing and detecting fraud. I reported some £5.4 million of savings in the most recent exercise for Wales 2016-18 (**National Fraud Initiative in Wales Report 1 April 2016 to 31 March 2018***,* October 2018).

This Code promotes compliance with the law and good practice among all participating bodies in data matching exercises using my powers, while balancing the need for this work to be done carefully to prevent unnecessary intrusion into people's affairs. I have developed it taking account of responses to the statutory consultation, the Information Commissioner's Data Sharing Code of Practice (May 2011), the Information Commissioners Code of Practice on Privacy Notices, Transparency and Control (October 2016) and the Article 29 Data Protection Working Party Guidelines on Transparency under Regulation 2016/679 (the General Data Protection Regulation (GDPR)).

The Code will help to ensure that people's information is protected and processed appropriately during data matching exercises. It also helps let individuals know why their data are matched, the standards and protections that apply and where to find further information.

Adrian Crompton
Auditor General for Wales

Part 1 – Introduction to this Code

Role of the Auditor General for Wales

1 The Auditor General is the external auditor of most of the Welsh public sector. He examines and certifies the accounts of the Welsh Government and its sponsored and related public bodies, the Assembly Commission and National Health Service bodies in Wales, as well as county and county borough councils, police and crime commissioners, chief constables, fire and rescue authorities, national parks and community councils. He has statutory power to report to the National Assembly for Wales on the economy, efficiency and effectiveness with which those organisations have used, and may improve the use of, their resources in discharging their functions.

2 Where the Auditor General is the external auditor of a participating body[1], he will be concerned to assess the arrangements that a body has in place to prevent and detect fraud, to follow up and investigate matches and act upon instances of fraud and error.

Background to Data Matching

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

4 Data matching exercises, such as the National Fraud Initiative (NFI) that the Auditor General does in co-operation with the Cabinet Office and UK audit bodies, help audited bodies to prevent and detect fraud and error, so securing better value from public money. The exercises also help the Auditor General to assess the arrangements that audited bodies have put in place to deal with fraud, which can help the bodies to achieve further improvements.

1 Terms in bold are defined in Appendix 2

5 Data matching involves comparing sets of data, such as the payroll or benefits records of one body against other records held by the same or another body to see how far they match. This allows potentially fraudulent claims and payments to be identified. Where a match is found, it may indicate that there is an inconsistency which requires further investigation; it is not necessarily evidence of fraud. Where no match is found, the data matching powers will have no material effect on those concerned. In the NFI, participating bodies receive a report of matches that identify inconsistencies in the data held and may be indicative of fraud. Participating bodies should follow up and investigate such matches, to detect instances of fraud, over and under payments and other errors, and where appropriate take remedial action and/or update their records accordingly.

6 The NFI data matching currently comprises two main strands: batch matching of sets of data and point of application matching (undertaken at the time a person applies for a benefit or service). See Appendix 1 for information about the point of application services available at the time of writing.

The Statutory Framework

7 The Auditor General conducts data matching exercises under his statutory powers in the Public Audit (Wales) Act 2004 (the 2004 Act). Under the legislation:

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

b the Auditor General may require local government and NHS bodies in Wales to provide data for data matching exercises.

c other bodies may participate in the Auditor General's data matching exercises on a voluntary basis where the Auditor General considers it appropriate. Where they do, the 2004 Act states that there is no breach of confidentiality and generally removes other restrictions in providing the data to the Auditor General for Wales.

d The requirements of data protection legislation apply, so data cannot be provided voluntarily if to do so would be a breach of data protection legislation.

e the Auditor General may disclose the results of data matching exercises to bodies that have provided the data as well as in pursuance of a duty under an enactment.

f the Auditor General may publish a summary report.

g the Auditor General may disclose both data provided for data matching and the results of data matching to the Cabinet Office, 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.

h 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.

i the Auditor General may charge a fee to any body participating in a data matching exercise and must set a scale of fees for bodies required to participate.

j the Auditor General must prepare a Code of Data Matching Practice following consultation with bodies required to participate (local government and NHS), the Information Commissioner and other bodies that the Auditor General thinks fit. The Auditor General must also lay a copy of the Code and any alterations made to it before the National Assembly and publish the Code. All bodies conducting or participating in his data matching exercises must have regard to the Code, including the Auditor General himself.

Structure of the Code

8 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.

9 Certain terms used in the Code are defined in Appendix 2. These terms appear in bold text for ease of identification.

Review of the Code

10 The Auditor General intends to review and update the Code periodically when there are changes in the law and to reflect comments and experience drawn from each data matching exercise.

Relationship to Data Protection Legislation

11 In addition to this Code, when taking part in data matching exercises, Participating Bodies should have regard to relevant data or information sharing codes and guidance, including any statutory guidance from the Information Commissioner, such as the Data Sharing Code of Practice prepared under section 121 of the Data Protection Act 2018, which is to be available on the Information Commissioner's Office website.

12 References to compliance with data protection legislation should be construed as compliance with current data protection legislation applicable in the UK.

Reproducing the Code

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

Queries on the Code

14 Any questions about this code or a data matching exercise should be addressed to the Wales Audit Office's NFI Co-ordinator, Wales Audit Office, 24 Cathedral Road, Cardiff, CF11 9LJ; Email: nfi@audit.wales.

15 Information about the Auditor General's data matching exercises is available on the Wales Audit Office's website.

Complaints

16 Complaints about bodies participating in the Auditor General's data matching exercises should be addressed to those bodies.

17 Complaints about how the Auditor General's functions are undertaken, including in respect how Wales Audit Office staff or others carry out work on his behalf, will be dealt with under the Wales Audit Office complaints procedure. Such complaints can be made by phone, email or letter to the Complaints Manager, Wales Audit Office, 24 Cathedral Road, Cardiff CF11 9LJ, 029 2032 0500 or complaints@audit.wales. Further details about the complaints procedure are available on the Wales Audit Office's website.

18 If you have a concern about the way that the Auditor General deals with personal data you can raise it with the Wales Audit Office Data Protection Officer by emailing infoofficer@audit.wales or by writing to the Complaints Manager, Wales Audit Office, 24 Cathedral Road, Cardiff CF11 9LJ, or phoning 029 2032 0500. You may also raise such concerns with the Information Commissioner (details are on the Information Commissioner's website).

Part 2 – Data Matching Practice

Status, scope and purpose

19 This Code has been prepared by the Auditor General following a statutory consultation process, and has been laid before the National Assembly under section 64G(4) of the Public Audit (Wales) Act 2004. It applies until a replacement Code is laid before the National Assembly.

20 This Code applies to all data matching exercises conducted by or on behalf of the Auditor General under s64A of the Public Audit (Wales) Act 2004 for the purposes of assisting in the prevention or detection of fraud.

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

22 The purpose of this Code is to explain data matching and give guidance to the Auditor General and his staff, or others carrying out work on his behalf, and all bodies involved in data matching exercises to comply with the law, especially the provisions of data protection legislation. It is also intended to promote good practice in data matching and to let individuals know why their data is matched and by whom, the standards which apply and where to find further information. However, it is incumbent on all participating bodies to ensure that their own procedures when participating are compliant with the law as amended from time to time.

23 This Code does not, however, strictly apply to the detailed steps taken by a participating body to investigate matches from a data matching exercise. It is for participating bodies to investigate matches in accordance with their usual practices for investigation of fraud and error.

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

What is data matching?

25 The Public Audit (Wales) Act 2004 defines data matching as the comparison of sets of data to determine how far they match (including the identification of any patterns or trends). The purpose of data matching is to identify inconsistencies that may suggest fraud. The Act makes it clear that 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.

26 Where a match is found, it suggests there may be an inconsistency that requires further investigation. No assumption can be made about whether there is fraud, error or other explanation until an investigation is carried out by the participating body.

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

Who participates?

28 Under the Public Audit (Wales) Act 2004, the Auditor General may require all local government bodies and NHS bodies in Wales to provide personal data relating to their employees, members and the people they serve for data matching exercises. Bodies required to participate in this way are referred to in this Code as mandatory bodies. Mandatory bodies must provide data for data matching exercises as required by the Auditor General under section 64B of the 2004 Act. Failure to provide data as required without reasonable excuse is a criminal offence.

29 Any other body or person may provide data voluntarily for data matching exercises if the Auditor General decides that it is appropriate to use their data. These are referred to as voluntary participating bodies in this Code. Where a voluntary participating body provides data to the Auditor General for data matching, the law (section 64C of the 2004 Act) provides that this does not amount to a breach of confidentiality, and generally does not breach other legal restrictions. However, patient data may not be shared voluntarily, and may only be used in data matching if the Auditor General requires it from a mandatory body.

30 The Auditor General may conduct data matching exercises himself or arrange for them to be done for him. In practice, most of the Auditor General's data matching will be done in the form of joint exercises with other UK audit agencies, such as the National Fraud Initiative. In this, the Cabinet Office has undertaken all the key aspects of the exercise for the Auditor General[2] and other UK auditors, including the collection and processing of data.

2 Under section 21 of the Public Audit (Wales) Act 2013, the Wales Audit Office must provide such services as the Auditor General requires for the Auditor General's functions. The Wales Audit Office also has power under section 19 of the 2013 Act to make arrangements to co-operate with other public bodies to facilitate the exercise of the Auditor General's and other bodies' functions.

Governance arrangements

31 The Auditor General requires each participating body's Director of Finance or equivalent to be the responsible officer and to nominate a senior member of staff to be the key contact for each data matching exercise. The responsible officer should also nominate staff to be responsible for data handling and investigating of matches. The responsible officer should ensure that nominated staff are suitably qualified and trained for their role.

32 The key contact should liaise with the Data Protection Officer for the participating body. The Data Protection Officer should be involved in the arrangements for data handling, training and providing privacy notices at the appropriate time.

33 The NFI Co-ordinator is the principal point of contact at the Wales Audit Office for all the Auditor General's data matching exercises (nfi@audit.wales). Full contact details are in paragraph 14.

34 For each data matching exercise, the Auditor General (or his agent) will make guidance available to all participating bodies. This will set out the detailed responsibilities and requirements for participation. The most up-to-date guidance is on the Wales Audit Office's website.

35 The guidance will contain:

a a list of the responsibilities of the nominated officers at the participating body;

b specifications for each set of data (listing the minimum data to be provided by the participating body to enable data matching and to ensure results of sufficient quality);

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

d a timetable for processing;

e a data protection compliance return; and

f information on how to interpret matches, and on co-operation between participating bodies.

How the Auditor General chooses data for matching

36 The Auditor General will choose sets of data for matching where there is reasonable evidence that fraud may be occurring and this fraud is likely to be detected as a result of matching those data sets. This will be the key consideration when the Auditor General decides whether it is appropriate to accept data from a voluntary participating body, or to require data from a mandatory body. Evidence may come from previous data matching exercises, from pilot exercises, from participating bodies or from other reliable sources of information, such as the Auditor General's staff or others carrying out work on his behalf.

37 The Auditor General will undertake new areas of data matching on a pilot basis to test their effectiveness in preventing or detecting fraud. The Auditor General will review the results of pilot exercises and will only extend exercises where pilots achieve matches that demonstrate a significant level of potential fraud. A significant level may be indicated by a few serious incidents of fraud or a larger number of smaller ones. The terms of this Code apply in full to pilot exercises. Pilot data must be provided in accordance with the provisions of data protection legislation.

38 The Auditor General will review the results of each full data matching exercise in order to ensure that it is appropriate to continue to match that data and also to refine how he chooses data for future exercises. In particular, the Auditor General will consider whether such matches continue to show a significant level of fraud.

The data provided for matching

39 The data required from participating bodies will be the minimum needed to undertake the matching exercise, to enable individuals to be identified accurately and to report results of sufficient quality. This will be set out in the form of a data specification for each data set in the Auditor General's guidance for each exercise.

40 Any revisions to the data specifications will generally be published at least six months before the data sets are to be provided on the Wales Audit Office website. The Auditor General's NFI Co-ordinator will draw the attention of participating bodies' key contacts to such revisions by email. This is to ensure that participating bodies have early notification of any changes, so they can prepare adequately.

Powers to obtain and provide the data

41 Under section 64B of the 2004 Act, all mandatory bodies must provide data for data matching exercises as required by the Auditor General.

42 The provision of data to the Auditor General for data matching by a voluntary participating body must comply with data protection legislation, must not be prohibited by Part 1 of the Regulation of Investigatory Powers Act 2000 and may not include patient data. Otherwise the Public Audit (Wales) Act 2004 (s64C) provides that provision of the data does not amount to a breach of confidentiality, and generally does not breach other restrictions.

43 Patient data may not be shared voluntarily and so may only be used in data matching if the Auditor General requires it from a mandatory body.

44 All participating bodies are required to provide the data in accordance with the provisions of data protection legislation. In practice, this will mean that the disclosure of data is either in accordance with the data protection principles, or a relevant exemption under the Data Protection Act 2018 has been applied.

45 In most cases, data matching will be done in accordance with the data protection principles without the need to rely on exemptions.

Fairness and transparency

46 Data protection legislation requires that data must be processed lawfully, fairly, in a transparent manner and for specified and legitimate purposes. In addition, data controllers must inform individuals that their data will be processed. Participating 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/.

47 The privacy notices should contain information required by data protection legislation such as:

- the identity of the data controller,
- the purpose or purposes for which the data may be processed,
- the legal basis which the data controller is relying on for processing,
- the categories of personal data collected,
- the recipient or categories of recipients of personal data,
- details of retention period or criteria on retention,
- the source of the personal data,
- the right to lodge a complaint with the Information Commissioner's Office, and
- any further information that is necessary to enable the processing to be fair.

48 Participating bodies should, so far as practicable and unless an exemption from the fair processing requirement applies, ensure that notices are provided, or made readily available, to the individuals about whom they are sharing information. The privacy notice should clearly set out an explanation that their data may be disclosed for the purpose of preventing and detecting fraud and include details of the legal basis on which the data controller relies for the processing. The notice should state that the information will be provided to the Auditor General for this purpose and it should specify who the data will be shared with. The privacy notice should also contain details of how individuals can find out more information about the processing and how to exercise their rights.

49 Communication with individuals whose data are to be matched should be clear, prominent and timely. Where data matching is being undertaken at the point of application (e.g. at the time that an individual applies for a benefit), then a privacy notice provided at this time is sufficient. Where data matching is being undertaken after the point of application 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 provide privacy information,

50 When providing data to the Auditor General, or to the Cabinet Office as the Auditor General's agent, the participating body should submit a data protection compliance return confirming compliance with privacy notice notification requirements. The Auditor General will check that the requirements have been adhered to and, where necessary, will set out the steps necessary for the participating body to achieve compliance. He may also seek input from the Information Commissioner as part of this process.

51 Participating bodies should provide privacy notices at the point of collecting personal data where practicable. It is for participating bodies to ensure privacy notices are in line with the law, as it stands at the time, and in line with current Information Commissioner Office guidance that they provide the appropriate form of notice at the appropriate time to meet the requirements of fairness and transparency. Participating bodies should in any event provide such notices before disclosure to the Auditor General or his agent, unless it is impracticable to do so.

52 Some of the data used for data matching exercises relates to deceased persons. Although information relating to a deceased individual is not regarded as personal data of the deceased person under data protection legislation, common law rules of confidentiality may restrict disclosure, and such data is also likely to be personal information of a living, identifiable individual. To avoid unnecessary distress or harm, particular care and sensitivity should be taken in dealing with data concerning deceased persons throughout the exercise and in the investigation of matches.

Quality of the data

53 Participating bodies should ensure that the data they provide to the Auditor General and his agents are of good quality in terms of accuracy and completeness, in line with data protection legislation, which requires personal data to be accurate and where necessary kept up to date.

54 Before providing personal data for matching, participating bodies should ensure that these are as accurate and up to date as possible. Errors identified from previous data matching exercises should be rectified, and action taken to address issues raised in data quality reports supplied from those exercises.

55 Linked to the requirement under 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: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-rectification/

Data security

56 The Auditor General, any firm or body undertaking data matching as his agent and all participating bodies must put in place security arrangements for handling and storing data in data matching exercises.

57 These arrangements should ensure that:

a specific responsibility for security of data has been allocated to a responsible person or persons within each 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 electronic data so that only those who need to access the data for the purpose of a data matching exercise can do so,

d all Wales Audit Office staff and any firm acting as an agent of the Auditor General who have access to personal data will be subject to security clearance procedures. As a minimum all such individuals will be subject to Baseline Security Standard Checks before they work on data matching,

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. Participating bodies should ensure that their staff have adequate training, that records of this training are maintained and refer staff to the training resources on the secure NFI website that provide guidance on how to use the NFI website and how to review matches,

f there are robust mechanisms in place for recording access, use and transfer of data,

g if a breach of security occurs, or is suspected, where necessary authorised users should be given new passwords or required to change their passwords as soon as possible. The responsible body should also follow the Information Commissioner's guidance on the management of security breaches. Participating bodies' key contacts and the Wales Audit Office NFI Co-ordinator (nfi@audit.wales) should inform one another immediately in the event of a suspected or confirmed security breach and ensure that the Data Protection Officers of the Wales Audit Office and/ or the participating bodies affected are also so informed.

58 All persons handling data as part of the data matching exercise should be made aware of their data protection, confidentiality and security obligations under data protection legislation, the 2004 Act and this Code, and should be given appropriate training. Such staff should be subject to strict access authorisation procedures, with breaches engaging the applicable disciplinary process.

59 Where the Auditor General or his agents establish websites for the transmission of data or the results of data matching, these will be password protected and encrypted to 256 bit SSL standards. This applies to the current NFI website.

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

61 Where the Cabinet Office or another body undertakes data matching on behalf of the Auditor General there must be a written contract or other binding legal agreement in place which incorporates data processor provisions required by data protection legislation and which imposes security standards as outlined in this Code.

Supply of data to the Auditor General

62 Participating bodies should only submit data to the Auditor General for data matching through the secure NFI website (or another secure website authorised by the Auditor General) or using authorised Application Programming Interfaces (APIs) to automatically submit information for matching.

The matching of data by the Auditor General

63 The Auditor General will ensure that data matching is done fairly and for the purpose of assisting in the prevention and detection of fraud.

64 The Auditor General will apply data matching rules to identify exact and fuzzy data matches which indicate an anomaly which may indicate fraud.

65 All data transmitted and stored electronically by the Auditor General or his agents will be held on a secure, encrypted password-protected computer system maintained in a secure environment.

66 All data provided for data matching exercises will be backed up by the Auditor General or his agents at appropriate intervals. Back-ups will be subject to the same security and access controls as the original data.

Access to the results by the bodies concerned

67 All results from data matching exercises, such as matches and other relevant information arising from processing, will be disclosed to participating bodies only via the secure NFI website (or another secure data matching website) or authorised APIs.

68 The responsible officer should ensure that the results of a data matching exercise are disclosed only to named staff for each type of result. In the case of the NFI, the secure NFI website is designed for that purpose.

69 All results from data matching exercises held by the participating body should be password protected on a secure, password-protected computer system. Any printed results should be kept in locked storage in a secure environment and should only be accessible to named authorised individuals.

70 Where participating bodies are sharing data under a point of application data sharing agreement, participating bodies together with any service providers working for them are responsible for the security of all information viewed or extracted from the system and are responsible for ensuring appropriate security controls are implemented. (In respect of the NFI, 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 participating body and service provider end-point systems that view or extract the information on the portal.)

71 Service providers and participating bodies shall ensure that any systems used to connect to the NFI web portal (or other data matching 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 its NFI service providers may result in the participating body's connection to the NFI being severed immediately.)

72 The Auditor General and any agent carrying out data matching work on his behalf, including the Cabinet Office and its NFI service provider in respect of the NFI, shall ensure that procedures and system security controls are in place relating to information disclosed for data matching that reflect the provisions of this Code and data protection legislation, to:

- 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;
- dispose of or destroy personal data in a manner to make reconstruction unlikely.

Following up the results

73 The detailed steps taken by a participating body to investigate the results of data matching are outside the scope of the Code. Matches are not necessarily evidence of fraud, and participating bodies should review the results to eliminate coincidental matches and concentrate on potentially fraudulent cases. In the process, they will need to identify and correct cases where errors have occurred.

74 No decision should be made as a result of a data match until the circumstances have been considered by an investigator at the participating body. Guidance on interpreting matches and co-operation between participating bodies is available on the secure NFI website.

75 Participating bodies 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.

76 Participating bodies should notify the Auditor General of any amendments to personal data to correct substantial errors so that he can amend the submitted data and prevent further matches being generated due to the error.

Disclosure of data used in data matching

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

78 There is legal authority to disclose the data or results where the disclosure is for or in connection with the purpose for which it was obtained, ie, for or in relation to the prevention and detection of fraud. This includes, for example, disclosure of the results to the participating body to investigate any matches and disclosure to an auditor to enable them to assess the participating body's arrangements for the prevention and detection of fraud. However, patient data may only be shared for a purpose relating to a relevant NHS body.

79 The Auditor General may also disclose data to equivalent audit bodies in England, Northern Ireland and Scotland, to the bodies whose accounts they audit or arrange to be audited, and to the auditors they appoint. A body in receipt of results from the Auditor General or his agent may only disclose them further if it is to assist in the prevention and detection of fraud, to investigate and prosecute an offence, for the purpose of disclosure to an auditor or otherwise as required by statute.

80 Any disclosure by the Auditor General, a participating body or any other person in breach of these restrictions is a criminal offence. The relevant statutory provisions are sections 64D and 64E of the Public Audit (Wales) Act 2004.

Access to data

81 Individuals whose personal data are included in a data matching exercise have the right under data protection legislation to obtain confirmation that their personal data are being processed and to be given a copy of the information comprising their personal data. Individuals and other persons also have rights to access other (non-personal) information under the Freedom of Information Act 2000. Requests for personal data should be dealt with in accordance with the organisation's general arrangements for responding to these requests.

82 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.

83 Individuals who want to know whether their data are to be included in a data matching exercise can check the data specifications for each exercise on the Wales Audit Office's website or by contacting the Wales Audit Office's NFI Co-ordinator (see paragraph 14 for contact details). This will tell them what data sets and fields we collect and from which bodies so that they may determine whether their personal data are likely to be included in an exercise. They should be able to check the accuracy of the data held on them by approaching the participating body holding the data.

84 Participating bodies should have procedures in place for dealing with requests from individuals for access to their data, and for complaints about the inclusion of their data in a data matching exercise. They should also have arrangements in place for updating and correcting data. If a participating body receives a complaint during a data matching exercise that concerns the statutory basis of the exercise, or the Auditor General is otherwise best placed to deal it, the body should pass on the request promptly. Complaints about the Auditor General's role in conducting data matching exercises should be sent to the Wales Audit Office Complaints Manager (see paragraph 17) so that they can be dealt with under the Wales Audit Office complaints procedure.

85 Requests for other (non-personal) information under the Freedom of Information Act 2000 relating to data matching exercises may be subject to the exemptions provided by the Freedom of Information Act, especially the law enforcement exemption (section 31). However, the law enforcement exemption would only relate to circumstances where disclosure would be likely to prejudice the prevention or detection of crime. This determination would be made on a case by case basis. The Auditor General will, however, make information that is not covered by exemptions readily available through, for example, his published summary reports on data matching exercises.

Retention of data

86 Personal data should not be kept in a form which permits the identification of the data subjects for longer than is necessary.

87 Access to the results of a data matching exercise on the secure NFI website (or any other data matching website established by or for the Auditor General) will not be possible after a minimum reasonable period necessary for participating bodies to follow up matches. For the NFI, the Cabinet Office will notify the end date of this period to participating bodies and the Auditor General will publish a Data Deletion Schedule setting out the criteria for retaining and deleting data and matches on the Wales Audit Office's website. Similarly, data deletion schedules will be set by the Auditor General in respect of any other data matching exercises that the Auditor General may undertake.

88 Participating bodies and the Auditor General may decide to retain some data after the retention periods specified by the Cabinet Office in respect of data held on the NFI secure website, for example, as working papers for the purposes of audit, or for the purpose of continuing investigation or prosecution. Participating bodies should consider what should be retained in their individual circumstances. Participating bodies should ensure that data no longer required, including any data taken from the secure NFI website or shared via APIs, are destroyed promptly and rendered irrecoverable. Data retained will be subject to the requirements of data protection legislation.

89 The Auditor General or the Auditor General's agents will destroy all original data sets provided to him by participating bodies within six months of their submission. Particular data may need to be retained so as to provide evidence for prosecutions or for the qualification of accounts. The Auditor General will destroy all data derived or produced from the original data sets promptly and, with the exception of prosecution, money laundering reporting or qualification evidence, within three months of the conclusion of the exercise.

90 A single set of reference codes for matches, together with any comments made by participating body investigators, will also be retained securely offline by the Auditor General or his agents for as long as they are relevant. This is solely for the purpose of preventing unnecessary reinvestigation of matches in any subsequent data matching exercise. Data retained will be subject to the requirements of data protection legislation.

Reporting data matching exercises

91 The Auditor General may publish reports on his data matching exercises. These will summarise the work and the results achieved. They will not, however, include any personal information obtained for the purposes of data matching from which a person or body may be identified unless the information is already in the public domain. In any event, the Auditor General will not publish any personal information unless it is necessary for the proper exercise of his reporting functions and is in accordance with data protection legislation. The Auditor General may report on the progress of prosecutions resulting from data matching to the extent that the information is in the public domain and any such reporting is compliant with data protection legislation.

Review of data matching exercises

92 The Auditor General will keep data matching procedures under review, such as in relation to whether the quality of datasets is acceptable and participating bodies are meeting security standards.

93 The Auditor General will review the results of each exercise in order to refine the choice of data and the techniques used in future exercises. As part of his reviews, the Auditor General will consider any complaints or representations from participating bodies or people whose data have been processed in the exercises.

Part 3 – Compliance with the Code and the Role of the Information Commissioner

Compliance with the Code

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

95 Questions regarding the Code and concerns regarding non-compliance should be addressed to the Data Protection Officer of the participating body or the Auditor General in the first instance, before contacting the Information Commissioner.

The Role of the Information Commissioner

96 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 participating bodies and the Auditor General in determining whether or not, in the view of the Information Commissioner, there has been a breach of data protection legislation. Where there has been a breach, the Information Commissioner will determine whether or not enforcement action is required and the nature and extent of any enforcement action. Information about the Information Commissioner's approach to data breaches and enforcement is available on the Information Commissioner's website.

97 Questions regarding data protection legislation and information sharing 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 or 01625 545 745

Email: casework@ico.org.uk

Website: https://ico.org.uk/ (use online enquiries form for questions regarding the legislation for which the Information Commissioner is responsible)

98 The Information Commissioner may be invited to review the Auditor General's data matching processing from time to time, to assess compliance with data protection legislation. Participating bodies are encouraged to invite the Information Commissioner's Office to review their procedures. The purpose of this review would be to assess participating bodies' compliance with data protection principles when processing personal data for the purposes of data matching exercises.

Appendix 1 – about the NFI and its activities

The National Fraud Initiative

The NFI is part of the Cabinet Office's work to develop and provide access to data sharing, data matching and analytical activities to help to counter fraud across government by identifying and reducing losses.

By bringing together a wide range of public and private organisations across the UK the NFI tackles fraud by using data matching to compare different datasets to identify potentially fraudulent claims and overpayments.

The NFI also works with public audit agencies in all parts of the UK to analyse key data sets provided by government departments to prevent and detect fraud. The organisations that take part in the NFI are responsible for following up and investigating the matches, and identifying frauds and overpayments

NFI Activities

The National Exercise is the established two yearly fraud detection exercise, and information regarding the types of matches undertaken are available in the data specification on the Wales Audit Office's website.

As part of its work to increase the use of data matching, the NFI has added a fraud prevention activity called AppCheck. This activity helps to stop fraud at the point of application, so reducing administration and future investigation costs.

The NFI also offers ReCheck which enables participating bodies to re-perform existing data matches when it suits them to help identify fraud earlier.

The NFI operates through a secure web portal Fraud Hub where participating bodies upload data and have access to resources designed to support participation in the NFI.

Transport Layer Security (TLS) is an encryption protocol used to protect data that is sent between computers. When two computers send data, they agree to encrypt the information in such a way they both understand. Depending on the rules in place, either of them may refuse to connect if they cannot find a suitable encryption method.

In August 2018, the NFI changed the level of TLS encryption to enable a more secure transfer when uploading data to the web portal.

Appendix 2 – Definitions

The following definitions have been used in this Code.

Term	Definition
Application programming interfaces (APIs)	Software that accesses and interacts with other systems and databases to undertake data matching.
Code	Code of Data Matching Practice 2018
Data controller	The natural or legal person, pubic authority, agency or other body which, alone or jointly with others, determines the purpose and means of processing personal data.
Data matching	The comparison of sets of data, such as the payroll or benefits records of one body against other records held by the same or another body, to determine how far they match to allow inconsistencies that may be fraudulent claims and payments to be identified.
Data protection legislation	As defined in section 39 of the Data Protection Act 2018 (DPA) and includes the DPA as well as the General Data Protection Regulation 2016/679 (GDPR) and relevant regulations.
Key contact	The officer nominated by a participating body's senior responsible officer to act as point of contact with the Auditor General and the Auditor General's agents (such as the Cabinet Office) for the purposes of data matching exercises.
Mandatory body	A body that is required by the Auditor General pursuant to section 64B of the Public Audit (Wales) Act 2004 to provide data for a data matching exercise.
Participating body	Either a mandatory or voluntary participating body which provides data to the Auditor General or his agents for the purposes of a data matching exercise.

Term	Definition
Patient data	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 (includes clinical data, such as medical records, and demographic data, such as the addresses of patients).
Personal data	Data relating to a natural (living) person from which that person can be identified directly or indirectly.
Point of application matching	Cross-checking information provided by applicants for benefits, goods or services against other datasets at the time the application is made.
Responsible officer	The Director of Finance or other senior named member of staff of the participating body responsible for ensuring compliance with this Code.
Voluntary participating body	A body from which the Auditor General considers it appropriate to accept data on a voluntary basis for the purpose of data matching.

Wales Audit Office

24 Cathedral Road

Cardiff CF11 9LJ

Tel: 029 2032 0500

Fax: 029 2032 0600

Textphone: 029 2032 0660

We welcome telephone calls in Welsh and English.

E-mail: info@audit.wales

Website: www.audit.wales

Swyddfa Archwilio Cymru

24 Heol y Gadeirlan

Caerdydd CF11 9LJ

Ffôn: 029 2032 0500

Ffacs: 029 2032 0600

Ffôn Testun: 029 2032 0660

Rydym yn croesawu galwadau ffôn yn Gymraeg a Saesneg.

E-bost: post@archwilio.cymru

Gwefan: www.archwilio.cymru