



DATA PROTECTION ACT 1998

GUIDANCE NOTE 8 - DATA MATCHING

Prepared By: Christopher Lambeth
Corporate Information
Governance Officer
Date of Publication: 20th October 2006
Version: 1.3

Table of Contents

1. Version Control	3
2. Points of contact for this Guidance	3
3. Introduction	4
4. The National Fraud Initiative	4
5. Staff Records.....	4
6. Statutory Requirement	5
7. The Prevention / Detection of Fraud	5
8. The Data Protection Principles	5
8. Advice and Assistance	8

1. Version Control

Version	Date	Notes
1.0		Sent out to DP Contacts for comments
1.1	26 th July 2006	Updated following comments received
1.2	16 th October 2006	Updated with additional comments

2. Points of contact for this Guidance

Corporate Information Governance Team

Name	Malkiat Thiarai
Title	Corporate Governance & Information Manager
Telephone	0121 303 1909
Email	malkiat_thiarai@birmingham.gov.uk

Document Author

Name	Christopher Lambeth
Title	Corporate Information Governance Officer
Telephone	0121 303 4876
Email	christopher_lambeth@birmingham.gov.uk

3. Introduction

3.1 What is Data Matching?

Computerised comparison of two or more sets of records with the main objective of searching for records relating to the same individual. "Data Matching" is comparing separate sets of data, either collected by different Data Controllers, or by the same Data Controller in different contexts. The aim of the comparison is the identification of anomalies and inconsistencies either within one set of data, or between two or more different sets. The information will usually have been obtained from application forms. For example, the details contained within a database containing information relating to Housing Benefit or Council Tax Benefit might be compared with the Payroll database - anyone earning above a certain amount may not be entitled to claim such benefits.

Despite the need to protect the public purse, data matching must still be done within strict parameters. At the point when the two or more databases are compared, many innocent people's personal information will be processed for this purpose. Even when "matches" are found, guilt may not be presumed. Further investigations will need to be completed before fraud can be deemed to have been committed.

4. The National Fraud Initiative

4.1 The Initiative

The Audit Commission and the Association of Local Authority Treasurers agreed that such studies be carried out as part of the standard audit of local authority. There is no discretion given to Birmingham City Council as to whether to submit their accounts to audit. The Commission however gave the Information Commissioner an assurance that, it would insist that authorities consult staff and will have provided a notification to all data subjects **before submitting any data**.

5. Staff Records

5.1 Data Matching of Staff Records for Fraud Prevention

The Social Security Administration (Fraud) Act 1997 gives the basis for local authorities and government agencies to share information held in relation to benefits administration in order to identify overpayment or underpayment of benefit entitlement and for the purpose of verifying the accuracy of records.

If internal audit want to match staff payroll data for the purpose of preventing fraud, the Commissioner recommends firstly that staff and representative bodies are consulted and given time to make representations. Also in order to satisfy the fair obtaining aspect of the first data protection principle, a notification should be included on the payslip, relevant forms etc. along the lines suggested in the Audit Commission Code of Practice on Data Matching.

6. Statutory Requirement

6.1 Delegated Powers

The City Council is restricted to exercising only those powers, which have been specifically delegated to them by committee. Where information is given to District Audit or any other third party for data matching because of a statutory requirement Internal Audit must first ensure that it is a written requirement stating which statutory powers are being used. It is the responsibility of Internal Audit to ensure, before participating in data matching exercises, that the necessary statutory powers exist in order to do so.

7. The Prevention / Detection of Fraud

7.1 Data Matching for the Prevention / Detection of Fraud

When data is collected for one purpose i.e. student grants and the information is also to be used to data match for fraud prevention/detection, the form used for data collection has to contain the following wording;

“This authority is under a duty to protect the public funds it administers, and to this end may use the information you have provided on this form within this authority for the prevention and detection of fraud. It may also share this information with other bodies administering public funds solely for these purposes.”

(This will ensure compliance with the first data protection principle).

8. The Data Protection Principles

8.1 The Principles

The principles need to be applied in the area of data matching as follows: (only those, which apply, are referenced).

Principle 1 > Personal data shall be processed fairly and lawfully and, in particular, shall not be processed unless –

- a) at least one of the conditions in schedule 2 is met, and
- b) in the case of sensitive personal data, at least one of the conditions in schedule 3 is also met.

Fair obtaining - At the time of data collection individuals must be made aware of what the information is to be used for and who it may be disclosed to.

The following wording is acceptable to the Commissioner’s office to notify individuals of possible data matching. This is not a “get-out” clause and does not mean that any use of the data collected is regarded as it having been obtained fairly. If this wording is used it does NOT mean that the Commissioner’s office will not investigate complaints regarding data matching activities.

“We must protect the public funds we handle and so we may use the information you have provided on this form to prevent and detect fraud. We may also share this information, for the same purposes, with other organisations which handle public funds.”

Legal Services Department has agreed that as long as this wording is present on relevant forms data matching in circumstances already laid down can be undertaken.

Fair Processing - There is a risk of unfair processing of personal data if search criteria employed produce a significant number of mismatches. As a “rule of thumb” the system ought not to produce matches of names and addresses which a person would readily recognise as relating to different individuals.

Principle two > Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.
Notification must be complete in terms of the intended uses and disclosures of the data held. Data matching will be notified as “Crime prevention and prosecution of offenders”.

Principles Three to Five

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

Principle Four > Personal data shall be accurate and, where necessary, kept up to date.

Principle Five > Personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes
These three principles address the issue of data quality, to ensure compliance the following must be undertaken;

- To produce a list of data items that are to be included in the match - by implication BCC should not use data for matching beyond this list, and not hold other items which may be excessive or irrelevant;
- To specify the form in which data items must be submitted in order to make reliable matches - e.g. Forename, Initial, Surname, full address, and postcode (all of an individuals information may not be needed);
- To specify common data standards, such as codes for different types of benefit fraud;
- To specify that data to be matched has been collected or validated within a certain period, the same time periods should be used to avoid matches being misinterpreted;

To ensure compliance with the fifth Principle the following retention periods must be adhered to:

- Data where there is evidence of actual fraud - completion of case
- Data where there is active suspicion of attempted fraud - 6 months
- Data where there is no evidence of fraud - kept until the end of the data match exercise.

In terms of accuracy you should ensure high levels of quality of data.

Investigator reports must be cross-referenced to the original data match to reflect the true position, particularly where they exonerate data subjects.

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

After a matching exercise if a subject access request is received an individual has the right to see the information about them as a result of the matching exercise. There is an exemption which allows the City Council to refuse a subject access request where if it were given out it would prejudice the crime prevention / detection exemption within the Act. It is not appropriate to rely on this exemption except in such cases i.e. not when a match is found, but when investigations have shown that there may be a crime being committed. The test as to the applicability of the exemption is thus a case by case one.

** Any such request and subsequent refusal will need to be documented by the Corporate Information Governance Team.*

Principle Seven > Appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data.

Given the sensitivity of the data that are likely to be held and that the harm that might result from any unauthorised disclosures of data could be considerable, the following MUST be complied with;

- Disclosures of data MUST NOT be made before consulting the appropriate notification entry first. All such disclosures should be documented.
- Unauthorised personnel (anyone not involved in the investigation) must not be allowed to have access to the data.
- The data should only be used for fraud investigation purposes.
- A high level of security is essential, as data will be very sensitive.
- Any data passed for matching in an electronic form must be encrypted and sent via a recognised courier company

**Data Matching procedures are available
on request from Birmingham Audit**

8. Advice and Assistance

11.1 The Corporate Information Governance Team

The Corporate Information Governance Team provides advice and assistance on the Data Protection Act 1998 and the Freedom of Information Act 2000 as well as other associated legislation. The Corporate Team can be contacted on 0121 303 4876 or in writing at the following address:

Corporate Information Governance Team
Intelligent Client Function
1st Floor, Lancaster Circus
1 Lancaster Circus
Birmingham
B4 7AB

11.2 Directorate Data Protection Contact Officers

Birmingham City Council has a Data Protection Officer within each individual Directorate in order to provide assistance on data protection issues. If you have any concerns relating specifically to your Directorate please contact your contact officer in the first instance and they will be able to advise you accordingly.

A full list of DP Contact officers is available on In-line.

11.3 The Information Commissioner

The Information Commissioner is the governing body for Data Protection and Freedom of Information and is an independent officer who is appointed by the Queen and reports directly to parliament.

The Information Commissioners duties include:

- Maintaining a register of data controllers
- Distribution of information on legislation
- Promoting compliance with the data protection principles
- Considers complaints about breaches of the principles within the Act
- Prosecutes offenders who contravene the Act

The Commissioner is there to help everyone comply with the Act. If you would like further advice on the Act you can contact the Information Commissioner's office at the address below or you can search their web-site to locate useful information on legislation matters.

Information Commissioner's Office
Wycliffe House
Water Lane
Wilmslow
Cheshire
SK9 5AF

Tel: 01625 545 745