Data Matching and the Law


“Data matching” – the comparison of separate sets of data in order to identify unwarranted differences and duplications – can be a powerful business tool. Auditors have long been users of data matching, at least on a small scale. They regularly compare data from different sources within the same organisation to test controls in financial systems and to test individual transactions. For example, they may compare payroll records with personnel records in order to establish whether weak controls are leading to incorrect payments.

A more recent innovation in the United Kingdom is the large-scale comparison of data sets from different organisations, such as the Audit Commission’s “National Fraud Initiative”. The Initiative matches data from local authorities and the Benefits Agency (the central government department responsible for social security benefits) in order to test the effectiveness of local authorities’ controls and arrangements for preventing and detecting fraud. Although it was not its primary purpose, the 1998 National Fraud Initiative identified an estimated £42 million of fraud in housing benefit, council tax benefit, pensions, student awards and payroll.

The increase in the range and volume of electronic records created by the drive towards e-government increases the scope, at least in technical terms, for the use of data matching. Increased connections between government databases will facilitate data matching on a continual basis, so reducing the need for special exercises.

In the United Kingdom, legal limits to the scope of data matching are now probably more prominent than the practical constraints. But the legal constraints on data matching are by no means abundantly clear. There are two basic legal considerations:

- in the case of matching data held by different bodies, the authority to share data; and in all cases,
- the protection of privacy.

There is uncertainty in both considerations

The authority to disclose information may derive from a statutory basis for either demanding or disclosing, or both. The Audit Commission\(^1\) considers that section 6 of the Audit Commission Act (1998) allows it to access data from the bodies it audits and from other persons for audit purposes. In such a situation, there is a duty to disclose, though there is also a duty to ensure that the disclosure really is within the power of the party requiring disclosure. If there is a duty to disclose, the Data Protection Act (1998) requirements that disclosure be lawful and necessary for the exercise of statutory functions are met.

But just as there is legislation that enables the sharing of data, there is legislation that prevents it. For example, the Finance Act (1989), prevents the Inland Revenue disclosing tax-payers’ information to all but very small number of parties. Imprisonment

---

1. Audit Commission (http://www.audit-commission.gov.uk/)
2. Data Protection Commissioner (http://www.dataprotection.gov.uk/)
of individual officers breaking taxpayer confidentiality ensures a cautious approach.

As to the protection of personal privacy, it is well known that the Data Protection Act and the Human Rights Act both give individuals rights to privacy. The Data Protection Commissioner\(^2\) has taken considerable interest in data matching, particularly where this involves information being shared among bodies, or where the data subject (the person whose data is held) may not have understood that their information would be used in this way. To help ensure that data matching complies with the principles of the Data Protection Act, the Commissioner issued a Guide to Developing Data Protection Codes of Practice on Data Matching. This covers issues such as registration of all parties to the exercise and notifying data subjects that their data may be used for the objective of the exercise. But overall, data matching has been guided more by legal opinion, which tends to vary, rather than case law.

The commencement of the Human Rights Act in October 2000 introduces a further element of uncertainty. The extent to which data matching complies with its provisions regarding personal rights to privacy is not clear. Although the Act includes exceptions to these provisions with respect to the prevention and detection of fraud, there are questions relating to the safeguards that must be in place when these exceptions are exercised.

Given the legal uncertainties, it is not surprising that there is a lack of authoritative guidance for those considering data matching. The Data Protection Commissioner is working on such guidance, in consultation with the Local Government Association, the Department of the Environment, Transport and the Regions, and the Department of Social Security. This should be available within 12 months.

The combination of increasing scope for data matching and uncertainty over the legal implications of using the technique were key reasons for the publication of our consultation paper, Data Matching and the Role of Public Sector Auditors\(^3\). The working group included representatives of the Office of the Data Protection Commissioner, the Inland Revenue, Treasury, the National Audit Office, the Audit Commission and local government. The Public Audit Forum is a body that builds on co-operation between the national audit agencies to provide a focus for developmental thinking on public audit.

As the title suggests, the paper is oriented towards public sector audit. But it is also relevant to public sector managers in general, not least by examining the respective roles of management and auditors with regard to data matching. It makes clear that the primary responsibility for the prevention and detection of fraud rests with management and not with their auditors. Managers would be wrong to assume that their auditors will use data matching to detect fraud for them. They may do that, but it is likely to be incidental to their testing of the organisation's controls.

The paper addresses the powers to transfer data, where data is matched between organisations, and the question of compliance with privacy legislation (the Data Protection Act 1998 and the Human Rights Act 1998). It also explores the cost-effectiveness of data matching, especially as there may be legal implications if data matching cannot be shown to achieve its aims. It concludes that the auditor's decision to use data matching should be made on a case by case basis. But it also sees a need for specific guidance to auditors on the use of data matching, building on the Data Protection Commissioner's work.  

---

**Principles of Data Protection**

Data covered by the Data Protection Act comprises facts and opinions about living, identifiable individuals. Anyone processing personal data must comply with the eight enforceable principles of good practice contained in the Act. They say that data must be:

- fairly and lawfully processed;
- processed for limited purposes;
- adequate, relevant and not excessive;
- accurate;
- not kept longer than necessary;
- processed in accordance with the data subject's rights;
- secure; and
- not transferred to countries without adequate protection.

---

3 This report is available on the Public Audit Forum web site (http://www.public-audit-forum.gov.uk/publicat.htm)