

# Data Sharing Review

Richard Thomas and Dr Mark Walport

## Consultation paper on the use and sharing of personal information in the public and private sector

### List of questions for response

We would welcome responses to the following questions set out in this consultation paper. Please follow the question order as set out in the consultation paper, leaving a blank response box for any questions not answered.

Please email your completed form to [contact@datasharingreview.gsi.gov.uk](mailto:contact@datasharingreview.gsi.gov.uk)

Alternatively you can send a hard copy response to:

**Data Sharing Review Secretariat**  
**5.26 Steel House**  
**11 Tothill Street**  
**London**  
**SW1H 9LJ**

Thank you.

### Section 1: Background

Question 1.

Comments: The Council shares personal data with partner agencies for health and social care purposes, and shares personal data pursuant to a number of its other functions.

### Section 2: Scope of personal information sharing, including benefits, barriers and risks of data sharing and data protection

Question 2.

Comments: Reducing costs; providing more 'joined-up' services; improving services.

Question 3.

Comments: Maintaining security; ensuring a proportionate approach based on a properly articulated balance between the public benefits of data sharing and the risk of prejudice to individuals' rights and interests; ensuring proper governance arrangements.

Question 4.

Comments: The more secure and well documented these methods are, the better.

Question 5.

Comments:

Question 6.

Comments:

Question 7.

Comments: Generally, difficulties have arisen with health sector partners. This seems to be partly due to cultural factors, and partly due to the very sensitive nature of the data these partners hold.

There are difficulties currently with Audit Commission requests to share data for the purposes of 'data matching' pursuant to the National Fraud. There are legal concerns that the strict test of necessity in construing 'likely', and the interpretation of 'in any case' to mean in each particular case in relation to the exemption from the subject access rights in sec 29(1) DPA (see R (on the application of Alan Lord) v The Secretary of State for the Home Department [2003]), should also be read across to the exemption from non-disclosure in sec 29(3). If it is correct to do so, (and given also that a fair processing condition must also still be satisfied) the use of this exemption for data-matching exercises where crime will be detected in only a proportion of cases, and where there will no examination of individual circumstances, could be very difficult. Generally, data sharing for anti-crime purposes could also become more difficult.

Question 8.

Comments:

### **Section 3: The legal framework**

Question 9.

Comments: As a public authority under the Human Rights Act 1998, there is now something of a 'mis-match' between the rather technical and detailed requirements of the DPA, and the broader requirements of Article 8. In many respects the human rights principles seem more appropriate for public authorities, viz all 'processing' is prima facie an interference with the right to respect for private and family life unless it can be demonstrated that it is 'necessary' on one of the permitted grounds for interference, and is proportionate.

Question 10.

Comments: Whilst there has been much debate about what 'incompatible' means, and how far other purposes can reasonably be said to be compatible, this does seem unduly technical and semantic, although it is acknowledged that the second principle is derived from the requirements of Directive 95/46/EC, Articles 6 and 7. It does also seem difficult to reconcile this requirement with the conditions for fair and legitimate processing which permit processing which is necessary for a range of public purposes, and without the consent of the data subject. In any event, it does seem that the root issue (which the Article 8 requirements address more directly) should really be whether any processing of whatever

nature (irrespective of the purpose the data was expressed to be collected for) can be justified on one of the permitted grounds for interference, and is proportionate.

Question 11.

Comments: The reluctance of the Courts to find any general right of privacy at common law is perhaps leading to a predisposition also to restrict the scope of the DPA – in particular in *Durant v Financial Services Authority* [2003], and *Johnson v Medical Defence Union* [2007]., and the comment by Lord Phillips MR in *Campbell v MGN Ltd* [2002] that the DPA was ‘certainly a cumbersome and inelegant piece of legislation’.

Question 12.

Comments: Under para 6(2) Schedule 2 DPA, the Secretary of State could by order specify circumstances where 6(1) is taken to be satisfied. It is suggested that the Secretary of State could use this power to specify certain basic sharing of ‘non sensitive’ data between public sector partners, subject to certain safeguards such as privacy impact assessments by the partners and certain specified security requirements.

Question 13.

Comments: Public authorities are in the rather strange position that there are three separate sets of legal rules to be considered in relation to data-sharing, viz the DPA, the Article 8 rights, and the common law of confidentiality. Whilst there are indications that the courts will regard the confidentiality rules as being informed by the requirements of Article 8, the position remains that public authorities must examine all three sets of rules in detail to ensure that proposals for data sharing are lawful. This can lead to confusion and uncertainty, and may lead authorities to become ‘risk averse’ in this area of activity.

Question 14.

Comments: Greater security could be achieved by imposing specific security requirements, for example with regard to encryption, across all data sharing by public sector partners. However, problems of compatibility of technology etc would arise, and no doubt public authorities would require funding to achieve compliance.

Question 15.

Comments:

#### **Section 4: Consent and transparency**

Question 16.

Comments: A general requirement that the consent of the data subject should first be sought, except where it would be unreasonable to seek such consent, would perhaps be useful in relation to the processing of sensitive personal data. The Council’s data sharing protocol with health and social services partners is based on the principle that consent should be obtained wherever possible.

Question 17.

Comments: In relation to any large scale data sharing exercise, this could raise severe

practical problems in terms of delays, increased costs, identifying in records whether or not consent had been given, the proper duration of consents etc. Given lawful and legitimate processing is already permitted where necessary for a range of other public purposes without consent, a specific requirement for consent in all cases would actually restrict the basis for data sharing. Given this processing is also permitted under the Directive, such a restriction would also mean the UK had not properly transposed the Directive into English law.

Question 18.

Comments: As a condition of permitting greater data sharing under para 6(2), an Order could specify what steps public authorities should take in relation to making data sharing transparent. These could include privacy impact assessments via citizen panels or scrutiny inquiries, greater publicity in local media, the adoption of trust charters detailing the protections put in place, etc.

Question 19.

Comments: Where local authorities are concerned, adopting data sharing policies could be designated as a 'Council function', with no delegation being permitted to a committee or to officers, so that the full Council would be required to debate the benefits and risks of data sharing proposals. Some aspects of the Framework code of practice are helpful but do not provide sufficient guidance, for example in relation to how privacy impact assessments should be carried out and what threshold would make data sharing unjustifiable. For local authorities, formulating a general methodology for deciding when data sharing arrangements are justifiable and when not should not prove too difficult. All are democratic and accountable, decision-making is already governed by statutory rules, all local authorities have scrutiny arrangements, and most have arrangements for consulting with customers via citizens' panels and the like.

## **Section 5: Technology**

Question 20.

Comments: Clearly information technology has had a great impact, but equally this should not in itself be the driver for data sharing.

Question 21.

Comments: There would be benefits from such an approach, including certainty and consistency as well as greater security, but there could be significant and perhaps overriding cost considerations.

Question 22.

Comments:

## **Section 6: International comparisons**

Question 23.

Comments:

Question 24.

Comments:

Question 25.
--------------

Comments:
-----------

Question 26.
--------------

Comments:
-----------

**Section 7: Additional questions**

Question 27.
--------------

Comments:
-----------

Question 28.
--------------

Comments:
-----------