

# 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: As the Lead Data Protection Officer for a local authority I advise on both one off disclosures of personal data and on the drafting and review of Purpose Specific Information Sharing Protocols for the Borough's Local Strategic Partnership.

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

Question 2.

Comments:

a) Benefits to individuals

More efficient and effective service delivery for those individuals who need assistance from a number of organisations.

Not having to give the same information to different organisations over and over again for connected purposes.

## B) Benefits to society

Financial savings brought about through the sharing of information and the reduction in duplication of administrative work

Identifying potential fraudsters through data matching different sources of information (e.g. matching benefits data against Council Tax records and other data sets to identify the last known address for an individual)

Protection of vulnerable individuals through delivery of more joined up services to ensure that they receive all necessary support. For example, housing individuals with mental health issues can involve a number of organisations (The Local Authority, the local mental health trust as well as voluntary organisations) each providing support to individuals.

Crime and anti social behaviour reduction through statutory agencies working together to better identify crime and anti social behaviour. The sharing of such information could enable more enforcement action to be taken against perpetrators.

### Question 3.

#### Comments:

#### a) Risks to individuals

Information could be taken only on "face value" and organisations could make assumptions on information received which are not true, with resultant actions having a negative effect on individuals.

An individual's information is lost due to inadequate protection when the information is transferred or once it is in the possession of the recipient organisation.

Personal information shared between organisations for a particular purpose is misused by receiving organisations and used for further unconnected purposes.

#### b) risk to society

There is not sufficient debate to inform the public of potential data sharing initiatives (for example "Contact Point").

Data sharing is not done in a responsible and proportionate manner. Public Sector organisations become overly intrusive into individuals lives and we slip into a big brother society through the back door, where an individual's right to a private life is not respected.

### Question 4.

#### Comments: -

Question 5.

Comments:

The majority of Local Authority organisations have implemented Centralised customer relationship management databases, with a view that the setting up of such a system will enable them to gain a holistic view of their customers. Whilst the creation of such system does not mean that a local authority is holding more personal information than it did previously. The actual purposes for which the information held on the CRM will be used are often considered after the system has been implemented, rather than at the outset. This could lead to information being used for inappropriate or unintended purposes.

From my experience public sector organisations are generally not very good at retaining information in line with the requirements of the 5<sup>th</sup> Data Protection Principle. Often case management systems which support data sharing are implemented with little or no consideration of the need to review and weed out personal data no longer required. The continued retention of irrelevant personal information increases the likelihood that excessive or unnecessary information is shared.

Question 6.

Comments:

From my experience I believe that private sector organisations buy and sell databases of personal information in an irresponsible fashion without proper notification or agreement from individuals. If the powers of the Information Commissioner remain the same, then private sector organisations will continue to see their profits as more important than compliance and responsible data handling.

Question 7.

Comments:

There is a tension between local authorities and health bodies, moving forward the government expects these organisations to work together in a more integrated way. However, local authorities and health bodies work to different standards and conflicting priorities. There are also significant cultural and trust barriers both within the Local Authorities (internal departments can operate as silos) and between Local Authorities and Health Bodies.

Question 8.

Comments:

When for example banks collect your information in their fair processing notice they tell you that they will share your information with other companies within their group of companies, often these companies are based abroad. I do not believe that these financial organisations should be able to do this without providing further fair processing information (i.e. naming the companies and the specific purposes for which they would like to use an individual's data) and also requiring an individual to "opt in" before data is shared. Whilst the 8<sup>th</sup> Data Protection Principle creates some protection for the data shared abroad, the more widely the information is spread across a group of companies, the less control an individual retains in relation to their own data and the greater potential for it to be misused or held insecurely.

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

Question 9.

Comments:

Strengths of the Data Protection Act

The subject Access rights provided by the Act are fairly comprehensive.

The 1<sup>st</sup> Principle and 7<sup>th</sup> Principles are the strongest principles within the Act and the majority of queries that I receive from staff require the application of these two principles. In particular, there is a growing recognition amongst staff that there is a requirement to be open and transparent with individuals in relation to how we use their personal data when we collect it.

Weakness of the Data Protection Act:

There are a lack of powers available to the Information Commissioner.

There is no statutory requirement for organisations to carry out regular compliance audits. Organisations should (with appropriate guidance) be required to undertake annual compliance audits and report findings to the Information Commissioner's Office, with follow up action from the Commissioner if necessary.

The Information Commissioner also needs to be given greater powers of audit, as personal data needs to be valued as much as other assets that an organisation has.

Also as an incentive to senior managers within local public sector bodies compliance audit results should form part of the new Common Area Assessments.

Question 10.

Comments: Generally, I believe that public authorities do adhere to the second data protection principle. For example within my local authority there are a number of distinct business areas (e.g. Council Tax, Housing Benefits, Parking) and there is a recognition (amongst the guardians of the different datasets) that information obtained within one of these business areas can not then be used for any further unrelated purpose. As a Data Protection Practitioner I am of the view that the second principle is of limited value, as interpretation and advice on what is an "incompatible" purpose is thin on the ground and those examples that are often cited within guidance are of limited value. The first principle is normally of greatest value when considering data sharing issues.

Question 11.

Comments:

Institutional barriers to the effective implementation of the Data Protection Act still exist. There is a continuous need to educate staff so that they focus on the important data protection issues when processing personal information. For

example when staff raise Data Protection queries with me they often have not fully examined the purpose for which they want to use the personal information, or even considered issues such as proportionality or necessity in relation to the disclosure of personal information.

The fact that the Act is called the "Data Protection Act" can also cause confusion where staff are uneducated on the subject, as they focus on the word "protection" and think that the Act only requires us to hold personal information securely and nothing more.

As stated above, I believe that organisations should value information held as much as their other assets (e.g. people and money). However, this is not the case when we consider the resources organisations typically put into information compliance. Normally an organisation will have one or possibly two officers responsible for ensuring Data Protection/Freedom of Information compliance. Compare this to the amount of resources normally given to manage an organisations human resources or accounting function and there is a clear imbalance.

Question 12.

Comments: See answer to 9 above.

Question 13.

Comments: The definition of relevant filing system contained within the Data Protection Act is poorly worded and has been interpreted in an extremely narrow fashion by the courts (e.g. in the Durrant case). The effect of this is that manual personal information held in an unstructured manner may not be afforded the same protection as computerised or structured manual personal data. However, it is foreseeable that the irresponsible use/disclosure of such unstructured information could be just as damaging to data subject.

Question 14.

Comments: -

Question 15.

Comments: -

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

Question 16.

Comments:

I believe that the legislation and guidance is generally clear on when consent is and is not required and the form that the consent should take (for example the obtaining of explicit consent for the sharing of sensitive personal data).

Consent of the data subject is going to be the basis for the majority of data sharing which is needed to support joint service provision between organisations. The benefit of obtaining the clients consent is that they clearly understand and agree to the sharing of their information, which in turn could mean that they do

not have to supply their information twice to two different organisations who are providing them with the service (e.g. between a Mental Health Trust and a Local Authority's social care function)

**Question 17.**

**Comments:** Reliance on consent for sharing personal information is the preferred option. However, there can be practical issues where individuals withdraw consent previously given. The implication of this is that organisations in receipt of information would need to be notified of the withdrawal of consent and in the absence of being able to satisfy other condition(s) for processing, cease processing the personal data.

**Question 18.**

**Comments:**

Organisations should be required to produce and publish purpose specific data sharing protocols where they are sharing information to aid transparency. Also as part of the notification process the Information Commissioner's Office could seek more specific information on the data sharing activities undertaken by organisations. This would enable the Commissioner's Office (with increased powers) to have a greater understanding of how organisations actually work and assist them when undertaking assessments, compliance checks/audits.

As well as producing protocols and leaflets for public consumption organisations should be required to actively record recipients of personal information (including the reasons for disclosure) and provide these to individuals where they make a subject access request.

**Question 19.**

**Comments:**

The data sharing code of practice has been useful as a checklist for data sharing considerations. I have compared the code's contents against our Local Strategic Partnership 2 tier framework and the code reaffirms the framework we have. However, the code should have been produced much sooner, as data sharing is not something that has just sprung up as a recent issue.

The privacy impact assessment handbook looks like a useful tool for larger data sharing projects (I have not actually actively used the PIA handbook in projects yet). However, most public sectors organisations have already produced and published their own Information sharing protocols, which contain the framework and standards that they will work under when sharing personal data.

**Section 5: Technology**

**Question 20.**

**Comments:**

Technological advances in my view have had minimal impact at present on information sharing at a local authority level. Whilst information could be more easily shared between organisations through tools such as email, not all local authorities use secure email to send personal data.

There are views within Local Authorities that Information Sharing Hubs (sharing of case management systems with controlled access levels) could be set up to assist organisations in data sharing activities. However, this approach is flawed from a compliance point of view as technology alone is not able to make appropriate decisions on the proportionality of a disclosure of personal data in a particular case.

Question 21.

Comments: I agree with the example suggested that personal data held on portable devices must be encrypted to a specified standard. I would also suggest that the same encryption standard should also apply to personal data shared between organisations by email. Clear links should be created between any legislative standard and ISO 27001.

Question 22.

Comments: More advice and guidance needs to be provide to Data Protection Practitioners highlighting available PET's. This in turn will assist in creating demand for privacy innovations from IT suppliers when organisations are undertaking procurement exercises.

## **Section 6: International comparisons**

Question 23.

Comments: -

Question 24.

Comments: -

Question 25.

Comments: -

Question 26.

Comments: -

## **Section 7: Additional questions**

Question 27.

Comments: The review has not looked at the issue of retention of shared personal information. If we are going to be more sharing of personal data in future organisations will need to do more to actively review and weed out personal data that is no longer required.

One major issue relating to the sharing of personal data is that the different terminology used by organisations can have a significant impact on how the personal data is interpreted by receiving organisations.

Question 28.

Comments: Sometimes, Just because an organisation already holds personal information, they feel that they can use that information for further purposes that they

believe are in individuals "best interests". The perception should be changed so that the personal data that organisations hold is seen as "belonging to the individual". There is still a lack of knowledge about how the Data Protection Act applies to situations, staff are too often focused on how personal information is held (e.g. manual or computerised) rather than looking at the purpose behind the information sharing.