

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

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: I work for a local authority. We have demands to share data with the caring services such as health authorities and charities as well as pressure to share information with private companies working in partnership with us

We hold data on social care, education, planning and environmental areas

Data is collected at source from members of the public and entered (sometimes more than once) into the council systems.

We are a local authority (County Council) and hold and share data in all our areas

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

Question 2.

Comments: For individuals there is convenience and the realisation that they will be looked after with minimum of data input.

For society, trends can be more easily monitored and assistance can be targeted more easily at vulnerable groups

Question 3.

Comments: Manual data runs the risk of being mislaid, electronic data runs the risk of the security being diluted. As an example data treated as extremely sensitive in one organisation could be treated with less reverence in another. Every organisation has its own unique culture and the expectation that data will be treated the same in each one is optimistic in the extreme.

HMRC loss of data DVLA loss of data.

Question 4.

Comments: The greatest risk lies in providing security for sensitive data. Many public authorities like our selves hold very sensitive (in the DPA sense) data. Traditionally we have been reasonably good at protecting that data internally, however as it travels electronically around the country, security may become diluted. Many people class financial data as sensitive, certainly the private sector would. There is a need for education of the users of the data into the significance of sensitive information

Question 5.

Comments: The mass of data transferred via the education system to central government is a worry. Unique pupil numbers and associated identifiers from Health ensure that the next generations will be the most monitored in history. As ever this is fine while we are ruled by a relatively benign regime but could be problematical if not dangerous for some individuals.

Question 6.

Comments: Store loyalty cards hold too much data on individuals particularly as they have expanded from predominantly store based to spread into other areas such as leisure and motor s as an example. People will be treated as groups rather than individuals with the risk that sectors of society less mobile (e.g the sick and the old) will be left behind as the private sector seek to make profits.

Question 7.

Comments: The sharing of housing Benefit data with Social care. The sharing of social care data with Connexions, sharing of criminal activity between police forces, less restrictive sharing from GPs who find it difficult to share with social care

Question 8.

Comments: Local government organisations and the audit commission where the audit commission compare financial data from the organisations against fraudulent social benefit claims. It seems iniquitous to target one section of society.

Section 3: The legal framework

Question 9.

Comments: The main strength of the Act are the 8 principles. This is an easy way to present the Act to those who do not understand as it is based as I always say on common sense. Its big weakness in my view is its Title Data Protection. It gives an impression of retaining data at all costs which has led to many misinterpretations such as in the Soham murders and other tabloid fodder. The Act facilitates the processing of data in a structured framework which I believe to be fair and it should be marketed as such.

Question 10.

Comments: Increasingly in local authorities, 'pushing the boundaries' to gain efficiencies mainly of a financial nature to erode the boundaries of legitimacy. As a data protection officer I am often under pressure to condone the use of data obtained for one purpose to be used in another. At times the processing is already underway where it is felt that the DP Officer might be seen as awkward!

Question 11.

Comments: My biggest bugbear is in trying to persuade people that data protection is not solely about protecting the data. Protection is only one although an important part of the Act. The Act encourages good practice, is compatible with regimes such as ITIL and Prince2 and overall provide a coherent guide to processing personal information.

Question 12.

Comments: The Information Commissioner has to have more power to intervene where misuse of data is suspected in much the same way as tax authorities now have.
A quality mark such as 'Investors in people' or 'ISO9001' should be encouraged to promote data protection.
Sanctions should have real teeth. It is a disgrace that the fines issued for breaches are so small, they should be made more severe.

Question 13.

Comments: The relationship between the human rights Act, Freedom of Information and data protection should be explained and promoted to the public to make them aware of the 'information' framework that is in place to protect , facilitate and promote their data in a positive way.

Question 14.

Comments: There are currently too many identity authentication systems in place at the moment. I speak from an authority that uses 4 different systems. A central ID card would be useful but I personally would feel more comfortable with the concept if the data that could be held centrally was transparent and limited. My fear is that once a central repository is established the temptation to collect everything will prove too tempting to governments.

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments: Consent is not always required to process personal data but as an organisation we do try to encourage this as far as possible. Consent can be verbal , written or can be construed from behaviour (e.g. when I join a company I give my consent to have my details shared with the wages section where I get paid, I don't have to physically consent to this my actions make it clear).

In the case of explicit consent I always advise having consent in writing or witnessed. I know in law this is not necessary but its more difficult to argue when you have provided a signature of consent.

Question 17.

Comments: I cant think of many, in fact I believe it would increase confidence and transparency in processing

Question 18.

Comments: Where records are electronic, subject access should be shorter than 40 days. Where manual records are concerned, the 40 days might still be required. There could be a two tier system, each organisation could publish (very much like the publication scheme in FOI) that data which will be released in say 14 days (some allowance needs to be made for system failure delaying things). This might help increase transparency and confidence in the system. This could go some way to making an identity authentication scheme more palatable.

Question 19.

Comments: The extension of the publication scheme to include data protection and the organisations that an authority shares data with would be an improvement. This would be opposed by private industry but maybe it could be confined to the public sector as that is the area that most sensitive data is processed in.

Section 5: Technology

Question 20.

Comments: The increase in the use of encryption has helped facilitate the acceptance of data sharing. On the other hand the development of memory sticks where vast amounts of data can be stored, used and possibly misused has increased the security risk associated with the technology. Stronger password protection would be useful although as an IT professional one of my greatest bugbears is people who forget passwords!

Question 21.

Comments: yes I believe an encryption standard would be very useful

Question 22.

Comments: The key to this is to make the technology simple to use. As ever transparency will be the key to acceptance.

Section 6: International comparisons

Question 23.

Comments:

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments: If a decision is made to have ID cards, a system such as operated by the credit reference agencies indication what organisation accessed a persons information in the recent past would be good for transparency.

Question 28.

Comments:
