

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 have no involvement in "personal information sharing". The reason I am responding to your consultation is that , as a private citizen, I am very concerned by the potential for harm that will be caused, and is being caused by the present fashion for collecting and then sharing personal data. The many recent revelations of sheer incompetence by many government departments confirm the grounds for such fears.

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

Question 2.

Comments: I find it difficult to see any "key benefits". Yes there may be cost savings to the various holders but these are, in my view, generally outweighed by the risks to personal safety and freedom. I do think that one needs to firstly separate privately held data from publicly held. Private data are given voluntarily and public data are not. This does not mean that there should not be better controls on private data.

Question 3.

Comments: The key risks of sharing private data are:
Use for purposes other than those intended
Risk of financial loss
Increased risk of fraud as the data are spread around.
the key risks of sharing public data are many:

Loss of personal freedom as the relationship between the state and the people is changed. Risk of unfair penalty if the data are incorrect as they will, to some extent, inevitably be. Risk to safety: eg large amounts of data are to be collected on children and shared between perhaps 300,000 individuals on a "need to know basis" . But who will decide who "needs to know" and by what criteria? Who will - effectively- monitor use of these data? Who will ensure that authorised individuals are removed from any access when they leave? Inevitably the data will be at least accidentally misused and /or mislaid as recent revelations have shown. Also it is clear that the data will be revealed to persons whose aims are to misuse it. How will control be enforced when the work is contracted out to India or Kansas? These sorts of questions will arise with regard to ID cards and other sources of data..

Question 4.

Comments: No comment

Question 5.

Comments: A clear example of public authorities holding data is the Contactpoint scheme referred to in Question 3.

Question 6.

Comments: No comment

Question 7.

Comments: Rarely. If required, as in child protection cases, sharing should be on a case by case basis. The present defensive attitude of some bodies will have to change as they realise that their duty is to the individual and not to the body they they represent

Question 8.

Comments: I understand that the DVLA are prepared to let private businesses such as car parking companies have details of car owners and drivers. This is a clear example of data being used both for a purpose not originally intended and to profit a private company.

Section 3: The legal framework

Question 9.

Comments: No comment

Question 10.

Comments: See example of the DVLA in 8 as an example of misuse.

Question 11.

Comments: The DPA needs to be reinforced with a major campaign to change attitudes to personal data. What on earth was a naval officer doing with the data on maybe 500000 people on a lap top in his car?

Question 12.

Comments: Clear effective and genuine penalties on individuals whether employed by private or public bodies.

Question 13.

Comments: No comment

Question 14.

Comments: No. Sharing should be restricted between public bodies and banned between public and private bodies.

Question 15.

Comments: No comment

Section 4: Consent and transparency

Question 16.

Comments: It is often not clear when consent is required.

Question 17.

Comments: Hopefully many barriers.

Question 18.

Comments: Individuals should be given strengthened access rights. Organisations should not be allowed to share information.

Question 19.

Comments: I support the Information Commissioners code of practice and the the idea of assessmants.

Section 5: Technology

Question 20.

Comments: Clearly data bases have much increased the risks to personal data.

Question 21.

Comments: The law can only lay down general principles

Question 22.

Comments: No comment

Section 6: International comparisons

Question 23.

Comments: No

Question 24.

Comments: No

Question 25.

Comments: No

Question 26.

Comments: No

Section 7: Additional questions

Question 27.

Comments: No comment

Question 28.

Comments: Whilst the review will have to work within its remit it should not shirk from considering the total impact on individuals of the vast mass of data now being collected and shared. INFORMATION BRINGS POWER and businesses are keen to have the power to earn more and, MORE WORRYINGLY, GOVERNMENTS are keen to increase their power over the individual. Some "inefficiency" will be the price we should all pay to protect our freedom.