

# 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: I am a member of the public who is concerned about privacy.

I am also data controller for a web-based psychology business, and it is the nature of our work that our customers reveal sensitive information about their mental state while using our services. Our service runs from a secure server, and we conform to professional confidentiality guidelines. In fact we do not even ask our customers to reveal their names or addresses, in order to maximise privacy as well as confidentiality. Unfortunately the bank that processes payments for us does require this information, and they make it available to us whether we want it or not; we would prefer they didn't.

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

Question 2.

Comments: a) When reputation is at stake, there is a benefit in revealing personal information in order to associate the individual with their actions for example, a journalist putting their name to an article). b) The same applies in the interests of society for example, an accused person identifying themselves to the court).

Question 3.

Comments: a) Risks to the individual arise because other people may not have their interests at heart for instance, an address coupled with travel plans would tell a burglar when a house will be empty; similarly a woman in refuge would not want her address revealed to her abusive partner). b) Society rarely shares these risks, and therefore society (through government) will tend to press for greater information sharing than individuals.

Question 4.

Comments: Any automated, networked systems for information sharing will pose both the greatest risks, because a) responsibility for the data is diluted across many people, b) it is more difficult for responsible staff to spot errors and breaches, c) networked computers make it possible for unlimited numbers of people to access data unseen, d) electronic media allow much larger amounts of data to be copied and removed, e) it is not easy, with current technology, for responsible users to securely store or even delete personal data from storage media.

Question 5.

Comments: In my view, public authorities nearly always collect far too much personal data. For example, name and address are nearly always required but are seldom really necessary; even if the service in question involves the delivery of goods, these could be delivered via a PO Box or other intermediary. Another common example is the intrusive request for ethnic group.

Question 6.

Comments: Private sector organisations tend to request name and address even when this is unnecessary. For instance, all a hotel really needs to know is that I will pay for the service, and my name and address is none of their business. Usually personal details are harvested for marketing purposes, which is annoying but not dangerous).

Question 7.

Comments: I cannot think of any examples. If I want my personal data to be shared, then I can arrange the sharing myself.

Question 8.

Comments: There are countless examples in the public sector, including the national sharing of medical records across the NHS, the DVLA selling data, obtaining and sharing of passenger details and credit records. In all these cases the freely-given consent of the individual has not been obtained, the data is not being collected and shared for sufficiently limited purposes, and there are risks to the individual of breach of privacy, the potential for crime to be committed against them such as blackmail or theft, or for administrative accidents to lead to a loss of liberty.

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

Question 9.

Comments: The DPA principles are good. What I do not understand is the utility of the notification process (which I have been through several times now). The notifications are far too general to be useful to the public, and should be abandoned. This would bring data protection in line with most other law, where breaches are enforced, but universal registration of good behaviour is not required.

Question 10.

Comments: The second DPA principle is good. However the government seems to believe that passing a law to enable data collection and processing is sufficient. It is not. The process of transformational government rides roughshod over the principle of limited purposes, and there are examples of this right across the public sector. I would like to see legislation challenged in the courts where the DPA principles are breached.

Question 11.

Comments: I don't know what technical or institutional barriers exist. The only societal barrier I can think of is a general lack of public awareness of the dangers of endemic information sharing; however awareness has increased rapidly in 2007.

Question 12.

Comments:

Question 13.

Comments:

Question 14.

Comments:

Question 15.

Comments: Yes, the requirement to notify under the DPA should be abolished. I cannot see that it serves any useful purpose, yet it is very burdensome. I have personally had to go through the process several times, and it's even more difficult than VAT.

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

Question 16.

Comments: In my role as data controller for a psychology service, we collect and share data to the absolute minimum and ensure its secure storage as much as possible. Sharing and consent are governed by the professional codes of conduct for psychologists, which are tougher than the DPA, and they are very clear. The only instance where we have provision to share personal data is when employers purchase the service on behalf of employees, and again we are clear that explicit opt-in consent is required.

Question 17.

Comments: It would create many barriers, but then surely that is the whole point. I would

strongly support a move in that direction. However I am sceptical about compliance by the public sector.

Question 18.

Comments: I am not convinced that further progress down this route would be productive. It could create a vast paperchase without actually improving privacy or security.

Question 19.

Comments:

### **Section 5: Technology**

Question 20.

Comments: Networked databases and automated processing have totally transformed the whole issue. If the Child Benefit records had existed as a roomful of files, it would have been impossible to lose a copy in the post. If it took a policeman with a pencil to record the numberplates of cars driving down the motorway, it would be impossible to create a National ANPR Data Centre logging the movements of the innocent.

Question 21.

Comments: No, the technology will inevitably change faster than the law. It is sufficient to require reasonable safeguards. In any case, the focus should be more on privacy than security. However there is scope for the computer industry to make security easier to implement. Encrypted drives are much more vulnerable to minor write errors, and operating systems tend to leave copies of unencrypted temporary files lying around on the hard drive. There is scope to make encrypted data storage more secure and easy to use, but this should be a matter for encouragement not law.

Question 22.

Comments: Anonymisation is a valuable safeguard and should be used much more, but it is often applied badly for instance removing name and address, but leaving postcode and date of birth, does not represent anonymisation of medical records). Pseudonymisation which I understand to mean reversible anonymisation) is in my view vulnerable and should not be relied on in most circumstances.

### **Section 6: International comparisons**

Question 23.

Comments: Ontario has a privacy commissioner; good idea.

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments: Germany: unconstitutional to create a National Identity Register.

**Section 7: Additional questions**

Question 27.
Comments: Consideration should be given to regarding personal information to be the intellectual property of the data subject.

Question 28.
Comments:

