

# 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.

### Data Sharing Review Secretariat Note:

Please note that comments in this submission are not necessarily those of SEEDA as an organisation.

### Section 1: Background

Question 1.

Comments:

As a citizen within the Information Age, a former Civil Servant, teacher of ICT and now ICT Development Manager for the South East England Development Agency.

Obstacles stand in the way of the expansion of eServices. To fulfill its potential, consumers' trust and confidence in trading on-line, users' privacy and consumer rights, interoperability issues and more, need to be ensured.

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

Question 2.

Comments: The key benefits of being able to share information is that access to data becomes the oil in a well tuned society. Everything that needs to be known can be quickly, in order to make informed decisions when they are best applied.

Question 3.

Comments: Dangers lie in those who have access, having a lack of a duty of care and appreciation of the implications of inappropriate storage and sharing. Personal data when available to other interests invalidate the right to privacy so that personal circumstances can be taken advantage of by others.

Question 4.

Comments: Large scale mass storage of personal data collected for governmental purposes can often seem far removed from any need for privacy and maintenance of individual dignity when floated around for statistical exercises. Lack of care and sense of a need for protection and secrecy can easily occur and items of data not be contained within certain confines of operation and communication.

Question 5.

Comments: No comment

Question 6.

Comments: No comment

Question 7.

Comments: Any organisation or department that has a legitimate interest in data of the subject in connected circumstances, may benefit from information gleaned of those circumstances, and may be able as a result to understand the needs and general predicament of a subject.

Question 8.

Comments: Such general (if already legal) circumstances are not envisaged. Sharing of data is important as long as it can be done in a non invasive, accurate, reliable and detached way.

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

Question 9.

Comments: The DPA has grown in significance and real involvement with day to day data handling too slowly. There needs to be more of an assessment of data gathered at the data collection and verification stage. Too often a tiny little box to tick typifies the current contempt held of the process and implications of data protection generally.

Question 10.

Comments: It is difficult to judge but once the data is held it would be too easy to see potential for other uses and although these would probably be innocuous and innocent would not be for the original purpose. Having said that I would

question if there would be any breach of personal privacy that would have a negative effect on the data subject. So perhaps data collected could be legitimately used for other purposes if the data is related and pertinent to helping in other circumstances.

Question 11.

Comments: It can often seem that too often one is asked for data by many different organisations. Would it not be better to be able to contribute to one central file on each individual at one time with updates by the individual to it when appropriate, perhaps being checked and authenticated and guided by an official, with some aspects being able to be done on line by the subject if they are competent to do so.

Access to this central database would then be by need to know, by granted authorities, of certain relevant aspects of the data. In view of recent difficulties this would no doubt cause alarm and disbelief in some quarters but I believe it should in the future be possible to establish such a system and for it to be secure.

Question 12.

Comments: It will be essential to have encryption on all data held and for the use of public and private keys for access and transmission. Levels of access, areas of access, editing and deleting will need control and monitoring. Encryption should be a clear requirement of any organisation holding potentially sensitive data.

Question 13.

Comments: No comment

Question 14.

Comments: This would need to enforce and protect all vested interests from all sides connecting to the data and data subject. This would evolve when there is a system that can be protected.

Question 15.

Comments: Unreasonable burdens are an excuse not to do things properly and with the thought and diligence necessary. If there is going to be a system that is secure, protected and reliable for the needs of the next century, data protection needs to be replanned and restarted soon or there could be resulting chaos and electronic systems that cannot be trusted for anything.

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

Question 16.

Comments: Information needs to be based on numerically based data and fact, and not subject to a qualitative comment. If this is the case then there should be no concern as to when it is collected.

Question 17.

Comments: The access to data and the granting of consent to access data, needs a process of examination, cross checking and granting of authority, limited to the needs of the body asking for permission.

Question 18.

Comments: I am not sure I like the idea of transparency as this would suggest a thin veil that probably wouldn't protect different interests adequately. Access to data for reasons given above needs to be confined and regulated.

Question 19.

Comments: As before.

### **Section 5: Technology**

Question 20.

Comments: Technology has enabled data to be shared too easily. Data has not hitherto been adequately categorised and identified as needing protection. Data collection needs to be more rigorous and personal data that will need to be kept secure marked for separate secure storage.

Question 21.

Comments: Yes.

Question 22.

Comments: Certainly such techniques are essential but with keys of trust that can be exchanged, sources of which can be checked and traced centrally, data can be given to those who need to know. A significant leap in education and the way that data is handled, along with the process by which this is managed needs to be made. Just patching and trying to improve what we are currently doing piecemeal is unfortunately not likely to go far.

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

Question 23.

Comments: Certainly more examination of new techniques and data transmission technologies may be of benefit. Card and mobile technology generally may have techniques that could be adopted for these purposes.

Question 24.

Comments: No comment

Question 25.

Comments: No comment

Question 26.

Comments: No comment

### **Section 7: Additional questions**

Question 27.

Comments: No comment

Question 28.

Comments: You will certainly need high level support and significant investment to begin to

change a very flaky situation. Good luck!