

# 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.** Please explain what your interest in information sharing is.

If you have an active involvement in personal information sharing, we would be grateful for the following information:

- What kinds of personal information do you collect, hold and share?
- How do you collect, hold and share such personal information?
- For what purposes do you collect, hold and share such personal information?

#### **Comments:**

The NAO does not typically share personal information.

The NAO reviews information held by organisations it audits and receives information from them and the information may involve personal data. This access to information is required to fulfil the NAO's statutory purposes, to undertake financial audits and value for money examinations. For example the NAO may review government case records of criminals being investigated by the Asset Recovery Agency or receive payroll information. Access to information is provided through the NAO's governing legislation. The Data Protection Act provides for this information to be reviewed or used for statutory purposes under the

exemption in Section 35. Personal data held by the NAO in the course of this work is recorded in our secure information systems. If it needs to be shared with others, such as financial audit contractors, this would be subject to specific agreement with them regarding its transfer, storage and destruction.

The NAO also collects personal information in the course of its work, for example in public surveys and in information supplied to it by members of the public writing to ask the NAO to investigate their concerns about public services. It does not share this information with others and if others need to see the analysis supporting NAO work, it would be supplied in such a way that did not involve sharing personal data.

The NAO also holds personal information relating to its employees and its contractors.

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

**Question 2.** What in your view are the key benefits of sharing personal information to a) Individuals and b) society?

### **Comments:**

For individuals (as service users and citizens) there may be benefits from greater efficiency in public services from the sharing of personal data (so long as the efficiency benefits outweigh the costs of establishing and maintaining the additional processing capacity needed and the costs of the extra data security measures needed). For example the DVLA's work is made more efficient by e-delivery of its services such as obtaining a driving licence and the annual licensing of a vehicle – bringing lower costs to the Exchequer (and hence the taxpayer) and reducing the costs to the individual applying for the licences.

Citizens may also benefit if data sharing allows better identification of those entitled to benefits or services, such as better targeting of the promotion of benefit entitlements (including not targeting those already found not to be eligible or not wishing to take up entitlements), or identifying pressing needs e.g. for child protection.

Society can benefit from the ability of public services to use personal information from other sources, for example: to identify potential fraud or detect criminal offences.

**Question 3.** What in your view are the key risks of sharing personal information to a) individuals and b) society? Please provide examples.

### **Comments:**

The sharing of personal data risks its loss.

The key risks to individuals from data sharing and its loss are their loss of privacy and the potential to be subject to identity fraud.

The key risks to society arising from data sharing and its loss are loss of confidence in government's ability to protect privacy and data security resulting in individuals not cooperating with data sharing and the loss of benefits from data sharing (as set out above).

**Question 4.** As mentioned in the introduction, there are wide variations in the scope and methods of personal information sharing. What scope and what methods, in your view, pose the greatest opportunities or risks? Please explain the reasoning behind your response.

**Comments:**

The NAO's data review has identified that risks are highest in relation to the most sensitive personal data and data transferred in large quantities.

**Question 5.** Please provide examples of where, in your view, the public authorities hold too much data or not enough personal information, and the reasoning behind your response.

**Comments:**

No comment

**Question 6.** Please provide examples of where, in your view, private sector organisations hold too much personal information or not enough personal information, and the reasoning behind your response.

**Comments:**

No comment

**Question 7.** Please provide examples of cases where you believe the sharing of personal information between two or more bodies would be beneficial, but where it is not currently taking place.

Please explain as fully as possible why information is not being shared, detailing what the barriers to the sharing of personal information are – e.g. legal, cultural, financial, institutional – and how these barriers can be overcome.

**Comments:**

The NAO has identified the benefits from further data in the following studies:

**Electronic service delivery in the Driver, Vehicle and Operator Agencies in Great Britain**  
HC 204 2007-2008

The C&AG recommended that the DVLA should explore the potential and practicality for validating identity using the Department for Work and Pensions' electronic Customer Information System, to help reduce the rejection rates for first time applicants for driving licences

[http://www.nao.org.uk/publications/nao\\_reports/07-08/0708204es.pdf](http://www.nao.org.uk/publications/nao_reports/07-08/0708204es.pdf)

Several examinations of the benefits system have highlighted advantages if data could be more effectively shared, matched or transferred between the systems used to administer different welfare benefits. This could involve the Department for Work and Pensions, HMRC and local authorities. Key issues relate to complexity and benefit take-up. See

[http://www.nao.org.uk/publications/nao\\_reports/02-03/020337.pdf](http://www.nao.org.uk/publications/nao_reports/02-03/020337.pdf)  
[http://www.nao.org.uk/publications/nao\\_reports/05-06/0506592.pdf](http://www.nao.org.uk/publications/nao_reports/05-06/0506592.pdf)  
[http://www.nao.org.uk/publications/nao\\_reports/05-06/05061178i.pdf](http://www.nao.org.uk/publications/nao_reports/05-06/05061178i.pdf)

Additional benefits may relate to outreach activity and targeting disadvantaged groups – see  
[http://www.nao.org.uk/publications/nao\\_reports/03-04/0304484.pdf](http://www.nao.org.uk/publications/nao_reports/03-04/0304484.pdf)  
[http://www.nao.org.uk/publications/nao\\_reports/06-07/0607609.pdf](http://www.nao.org.uk/publications/nao_reports/06-07/0607609.pdf)

The scope for reducing tax fraud by data sharing or matching between separate tax systems and between tax and benefits systems and data held by credit reference agencies is discussed in

[http://www.nao.org.uk/publications/nao\\_reports/02-03/0203429.pdf](http://www.nao.org.uk/publications/nao_reports/02-03/0203429.pdf)  
[http://www.nao.org.uk/publications/nao\\_reports/07-08/0708102.pdf](http://www.nao.org.uk/publications/nao_reports/07-08/0708102.pdf)

**Question 8.** Please provide examples of cases where you believe that personal information is being shared between two or more bodies, but where this should not be taking place.  
Please describe the information-sharing concerned and why you believe it should not be taking place, including the risks involved in such information-sharing.

**Comments:**

No comment

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

**Question 9.** In your view, how well does the DPA work? Please outline the DPA's main strengths and weaknesses and any proposals for changes you would like to see made, including suggestions for their implementation.

**Comments:**

We have no comment on how well the DPA works overall and in our view it is sufficient to address the risks to data security.

In our own recent review of how well the Act has worked in our organisation we have found that we have policies and procedures which enable us to comply with the requirements of the Act. Our IT and physical security measures are sufficient, if applied appropriately, to properly safeguard the personal data we hold, and we have identified no loss of personal data entrusted to us. Almost all the personal data we hold was requested, processed and secured appropriately, but we hold onto significant amounts for longer than required.

We have identified that we can make improvements and our review did not identify the need for changes to the Act to secure improvements in our practice.

**Question 10.** In your view, how well do public authorities and private organisations adhere to the second principle of the DPA? How valuable do you believe the second principle is? Please provide examples and the reasoning behind your response.

**Comments:**

No comment.

**Question 11.** What technical, institutional or societal barriers stand in the way of the effectiveness of the DPA? Please provide examples.

**Comments:**

Our recent review found no insurmountable problems standing in the way of improved practices. There needs to be a cultural shift to support greater awareness of the importance of data security and it will be important not to lose the heightened awareness as a result of the loss of the HMRC data discs. There are also technical challenges around the use of encryption, but these are surmountable.

**Question 12.** What further powers, safeguards, sanctions or provisions do you believe should be included in the DPA

**Comments:**

No comment

**Question 13.** Are there any other aspects of UK or EU law (such as EU Directive 95/46/EC) that impact positively or negatively on data sharing or data protection? Please provide examples.

**Comments:**

No comment

**Question 14.** Are there any statutory powers unavailable that would enable better and more secure sharing of personal information– for example for identity authentication purposes – between a) public authorities and b) public authorities and private organisations? If so, what are they?

Please provide examples and any steps you believe could be taken to improve matters.

**Comments:**

No comment

**Question 15.** Are there any parts of the legal framework that place an unreasonable burden on business? Please provide examples.

Please outline your proposals for streamlining the legislation to ensure that such burdens are minimised.

**Comments:**

No comment

**Section 4: Consent and transparency**

**Question 16.** Is it clear whether and when you need individuals' consent to share information about them? Are you clear about the form that consent should take? Please provide examples.

Please provide details of any initiative you have been involved in that has been based on consent.

**Comments:**

Yes, it is clear.

**Question 17** What, if any, barriers would a requirement for gaining consent create to the sharing of personal information? Please explain your reasoning.

**Comments:**

If gaining of consent were made required, this may inhibit further sharing with the result that the benefits listed above would not be realised.

**Question 18.** Do you have any suggestions on how to make the sharing of information more transparent?

For example, should individuals be given strengthened access rights? And if so, how? Should organisations be expected to do more to explain their use and sharing of personal information to the public? And if so, how?

**Comments:**

No comment

**Question 19.** How can we best ensure that information sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability?

For example:

In your view, how valuable is the Information Commissioner's recently published Framework code of practice for sharing personal information ([http://www.ico.gov.uk/upload/documents/library/data\\_protection/detailed\\_specialist\\_guides/pinfo-framework.pdf](http://www.ico.gov.uk/upload/documents/library/data_protection/detailed_specialist_guides/pinfo-framework.pdf))?

In your view, how valuable are privacy impact assessments along the lines announced by the Information Commissioner on 11 December ([www.ico.gov.uk](http://www.ico.gov.uk))?

**Comments:**

The framework code of practice on sharing personal information is helpful and clear.

Privacy impact assessments are appropriate in some cases but may be excessive in others. It is therefore important that they should not be mandated more widely than is appropriate.

### **Section 5: Technology**

**Question 20.** What impact in your view have technological advances had on the sharing and protection of personal information? Please provide examples.

**Comments:**

Technological advances have enabled the collection and efficient sharing of large quantities of personal data, with significant benefits as set out above.

Protection of personal data and the protection of personal data transfers between organisations are critical and the technical complexity is manageable, if costly.

**Question 21.** Should the law mandate specific technical safeguards for protecting personal information?

For example, should there be an explicit requirement that all personal information held on portable devices be encrypted to a particular standard?

**Comments:**

The mandating of technical safeguards would need to be carefully considered to ensure that the available technologies would be suitable for all situations and would not impose undue cost of implementation and on-going administration and support.

Currently a range of encryption tools/methods are in use and even if they were all to apply the same standard, there would be considerable challenges to the auditor in being able to handle the range in use. If the standards were mandatory, we would also need to introduce mandatory tools internally and there would be costs associated with this new requirement.

**Question 22.** How, in your view, could 'privacy enhancing techniques', such as the anonymisation or pseudonymisation of personal information, help safeguard personal privacy, whilst facilitating activities such as performing medical research?

Is sufficient advice about the deployment of such techniques available? Are you confident about using them? What are the barriers to using them?

**Comments:**

No comment.

## **Section 6: International comparisons**

**Question 23.** Are you aware of any jurisdictions whose legal framework for sharing and protecting personal information contains features that could be useful in a UK context? Please provide examples.

**Comments:**

No comment

**Question 24.** Do you have any international examples of good practice in the sharing of personal information that could or should be adopted by the UK?

**Comments:**

No comment

**Question 25.** Do you have any knowledge of jurisdictions that have adopted a particularly permissive or restrictive approach to sharing personal information? What have the consequences of this been?

**Comments:**

No comment

**Question 26.** Are you aware of significant differences in public attitudes to the sharing of personal information in other countries? Please provide examples and an explanation for why you believe this to be the case.

**Comments:**

No comment

## **Section 7: Additional questions**

**Question 27.** Are there any additional issues on the sharing of personal information and protection of personal information that this review should be considering?

Do any of these issues apply specifically to your sector?

**Comments:**

No comment

**Question 28.** Please set out any additional suggestions or observations you have that you believe will be of assistance to the review.

**Comments:**

No comment

