

# 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:

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

Comments:

We hold a wide range of personal data and sensitive personal data.

Information is held electronically and on paper and protected according to its sensitivity in line with statutory requirements such as the Data Protection Act and the Public Records Act.

Personal information is collected, held and shared for the following purposes:

To provide services to British nationals and business that:

- support the British economy
- support British nationals abroad
- support Managed Migration for Britain

To achieve the FCO's policy goals:

- Counter terrorism, weapons proliferation and their causes
- Prevent and resolve conflict
- Promote a low carbon, high growth, global economy
- Develop effective international institutions, above all the UN and EU

To maintain a network of Embassies and Consulates overseas in order to underpin the delivery of essential services and policy goals

Staff administration

**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? Please provide examples.

Comments:

Individuals

Effective public services - for example passport services and Consular Protection overseas for British nationals in distress such as victims of crime, hospitalisation, arrest or imprisonment, and during a crisis.

Society

Effective public services such as:

- To prevent evasion of immigration controls in order to work illegally, engage in criminal activities or terrorism, or otherwise cause harm to the UK. This may involve assuming a false identity or submitting false documents. In 2006/07 alone, over 12,000 fraudulent documents were used to support applications at one of our busiest Visa Posts. Terrorists also exploit international travel, by planning and training for a plot in one country before executing it in another.
- Data sharing, by checking visa applicant data against other databases, or by setting up "Fraud and Forgery Strategies" in co-operation with local authorities (backed by specific MOUs and in line with requirements under the Data Protection Act 1998) are some of the ways UKvisas counters these threats.
- Greater social cohesion within the UK due to high levels of public confidence in firm and fair visa services.

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

Comments:

Individuals

Personal information which is lost or shared inappropriately risks causing harm or distress e.g. through reduced personal security, identify theft, damage to reputation, and other crimes or misuse.

Society

Loss of personal data may undermine the integrity of the organisation responsible, and actively discourage the public to share important personal information with any public body.

Potential risk of security being compromised e.g. at events, visits, and other functions

Question 4. 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?

Greatest opportunities:

- Sharing data across national borders helps to counter terrorism, prevent abuse of immigration rules, prevent and solve crimes, and safeguard national security.

Greatest risks:

- Compliance with the Human Rights Act (Article 8)
- Compliance with the 'fair processing conditions' and the seventh principle.
- Abuse of shared personal information due to inadequate data protection laws outside the EEA.

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.

Comments:

We are working to develop a system where we notify the Department of Work and Pensions of the deaths of British Citizens overseas. This would strengthen DWP's ability to identify and act against pension fraud.

We envisage that in a crisis we may need to share some limited personal information with the governments of other countries e.g. where we have to rely on assistance from other Governments, police and other organisations in another country to help British nationals to evacuate.

UKvisas has recently agreed a Memorandum of Understanding, in compliance with the Data Protection Act, with the USA Department of Homeland Security (DHS). Under the terms of this MOU, the biometric data of those applying for a UK visa will be checked against US government watch-lists. This includes data of known and suspected terrorists, those being sought by the Police or subjects of warrants, visa refusals, those deported from the US and those likely to be inadmissible to the USA.

We consider that this biometric information vetting and sharing arrangement will support and enhance the immigration control agendas of both countries and lead to more informed decision-making by our Entry Clearance Officers.

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:

### **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: 1. The structure of the Act is not user friendly. The Principles are not set out in an obvious position and the use of interpretative section in Schedule 1 is undermined in its completeness because there are further interpretative sections in Schedules 2 and 3.  
2. The definition of " Personal data" is insufficiently clear.  
3. The IT Rules are lacking in detail.

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: No comment

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?

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?

Comments:

Yes, the FCO provides training on the Data Protection Act and maintains a network of Liaison Officers who can advise FCO staff on whether that individuals' consent is required to share information about them. However, the DPA recognises that there may be circumstances when compliance with one or more of the Act's data protection principles may prejudice other interests, e.g. national security; crime and taxation; and disclosures required by law or made in connection with legal proceedings. Under such circumstances, the FCO may be obliged or consider it necessary to share personal data with the law enforcement/police, other government department or court concerned. Any such release would be proportionate and comply with the remaining data protection principles.

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

Comments:

A requirement to gain consent would create a barrier to:

- Dealing effectively with both routine and emergency consular protection work. Obtaining consent is often difficult to achieve within an appropriate time-scale or is practically impossible. Examples of this include: when a British national has been arrested overseas and cannot be seen by consular staff; in the event of a British national subjected to a forced marriage overseas; during a crisis when we need to rely on members of the public to provide details about individuals. Under such circumstances, we may need to share personal data in "the vital interests of the data subject" e.g. passing information to the host government, local police, hospitals, airlines, Honorary Consuls, Consular Wardens. If a formal requirement for consent were introduced without provision for such situations, it would have a significant impact on our ability to provide consular assistance to British nationals overseas.
- Efficiency and the cost-effectiveness of activities by Government and Business. There is also a risk that it will be regarded as overly bureaucratic, convoluted and wasteful of resources.
- If consent were withheld by e.g. by participants in Conferences, events and visits there may be security risks and operational constraints in an emergency.


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: Individuals should be made aware, perhaps by way of a specific notice, that their data can be shared.

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: No comment

## **Section 5: Technology**

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

Comments:

### Positive Impact

- We are able to access information and do our jobs more quickly therefore giving a better service to our customers
- electronic storage/encryption enhances security
- secure electronic transfer of large amounts of data

### Negative Impact

- Too much information could be shared with too many people because of indiscriminate use of ICT.
- Increased risk when transferring data electronically
- Lack of compatibility between ICT systems

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: No comment

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 any significant differences in public attitudes to the sharing of personal information in other countries? Please provide examples and an explanation of 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

