

# 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: 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?

I am the legal counsel for Europe who provides advice to all GM European entities on compliance with data protection laws. In my answers I will refer to "GM" which will mean the GM European entities.

We collect various types of personal data. Most importantly about employees (including former employees) and customers. Employee data is collected from the employees when they join the company and ongoing as extra information is needed for new purposes (often information is collected via intranet systems). Employees are required to keep HR informed of any changes of their personal data. Employee data are basically kept in Europe. We use Safe Harbor and

Standard Contractual Clauses for some international transfers, including a PeopleFinder system on our intranet website. Sharing of employee data in principle only takes place with the head office.

Customer data is collected by the dealers when they accept orders for new vehicles. Based on a privacy statement in their sales terms they will share some customer information with the GM sales company. GM also collects customer data from persons visiting GM websites for which a privacy statement is in place. GM also collects personal data from persons participating in sales campaigns and visitors to e.g. motor shows (for which separate privacy statements are used). We do not share customer data with other GM sales companies. GM uses personal data for example for various direct marketing initiatives and aftersales service.

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

### Question 2.

Comments: What in your view are the key benefits of sharing personal information to a) individuals and b) society? Please provide examples.

Without the sharing of personal information our employees would not be able to function in our company. Simple information like contact details are also considered personal data. The sharing of such data is a key requirement to operate effectively. Also, the HR process (from payroll and benefits up to appraisals and career planning) requires that employee data is shared with other persons (mostly within the company) who have a valid need to access the data.

In their capacity as customers, individuals benefit from the sharing of their data as certain transactions, such as buying a vehicle, only require them to provide their contact data once. Both dealer and GM will have access to some relevant personal data that will make customer contacts take place more efficiently. The customer care center will have a history of the vehicle in case of mechanical issues and in the event of a complaint. Based on the vehicle licence number in some countries, systems are in place that allow the dealer to retrieve all relevant technical data of the vehicle he will be servicing before the vehicle actually enters the garage. The dealer can already check whether he has the required spare parts and/or service available which avoids losing time for the customer.

For society, the sharing of personal information can be beneficial as long as it is adequately regulated which governmental agency shares which data with whom.

### Question 3.

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

A risk for individuals would be that their personal information is shared with third parties without their knowledge and agreement. Involuntary loss or theft of personal information is also a risk.

Question 4.

Comments: 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?

Transferring unencrypted files with personal data via open email systems is risky as is sending data storage devices through regular mail. Encryption and strict use of (periodically changing) strong passwords are helpful.

Access to personal data must only be provided based on a clear written policy that is audited as well.

Question 5.

Comments: 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.

Question 6.

Comments: 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.

Question 7.

Comments: 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.

Question 8.

Comments: 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.

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

Question 9.

Comments: 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.

The Data Protection Act, as based on the EU 95/46 directive on the protection of personal

data, in general works well as it provides a set of legal principles to guide individuals, governments, businesses and other entities.

However, the requirements for the international transfer of personal data within multinational companies and with their service providers are too complex. The Binding Corporate Rules are for most companies far too detailed and require a high investment in preparation and legal fees. An alternative might be that the head office of a multinational company would be permitted to officially declare (certifying on a specific EU website much like the current one for Safe Harbor) on behalf of all its subsidiaries globally that may be involved in the processing of personal data originating out of the EEA, that they will all comply with the key EU data protection principles. As data transfers often change (both the data elements and the parties / service providers involved) no detailed agreements would need to be signed and registered. One subsidiary in the EU would be appointed as the representative of the group of companies and will deal with any complaints, be the contact for Data Protection Authorities and have to pay any fines.

#### Question 10.

Comments: 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. Second principle: Personal data shall be obtained only for one or more specified and lawful purposes, and shall not be further processed in any manner incompatible with that purpose or those purposes.

It is more important for an individual to know what kind of personal information a organization has regarding him or her and that it will not be shared with third parties without prior consent.

#### Question 11.

Comments: What technical, institutional or societal barriers stand in the way of the effectiveness of the DPA? Please provide examples.

It is necessary to have robust processes with "error-proofing" techniques built in to ensure that a single employee error does not result in the release of personal data.

#### Question 12.

Comments: What further powers, safeguards, sanctions or provisions do you believe should be included in the DPA.

#### Question 13.

Comments: 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.

See answer 9.

Question 14.

Comments: 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.

Question 15.

Comments: 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.  
See answer 9

**Section 4: Consent and transparency**

Question 16.

Comments: 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.  
Yes. We ask for consent when sharing e.g. customer information with our automotive finance affiliate and when collecting specific employee information via website surveys (e.g. storing results of on-line training courses)

Question 17.

Comments: What, if any, barriers would a requirement for gaining consent create to the sharing of personal information? Please explain your reasoning.  
Asking consent of a large number of data subjects (e.g. all your employees) is generally time consuming and difficult to handle for those who can not provide consent on-line.

Question 18.

Comments:  
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?  
Access rights are clear and broad enough but in practice hardly ever used. One can conclude that this in general shows data subjects have confidence in the way their personal data are processed. From our experience, there is not evidence of demand for greater access rights or more explanations but there would be additional cost and administrative work to do so.

Question 19.

Comments: 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))?

Companies will normally specify the details of the information sharing in the service agreement with the data processor or in an internal document when sharing with other affiliated companies (e.g. headoffice) takes place.

### **Section 5: Technology**

Question 20.

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

Question 21.

Comments: 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?

Setting general security requirements that apply EU wide could be beneficial. They should be dynamic (take into account that technology continues to develop) and only prescribe protection based on open technology standards in order to avoid the risk of closing markets to new entrants.

Question 22.

Comments: 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?

For companies like ours the bulk of the information is about employees and customers. Anonymisation of their data most often makes using their data impossible (e.g. performance appraisals or sending direct mail). In cases where identifying data is not important, (e.g. statistical research), this is done without storing names and addresses.

## **Section 6: International comparisons**

Question 23.

Comments:

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.

Australian law in general exempts employee records from the scope of the data protection law.

Question 24.

Comments: Do you have any international examples of good practice in the sharing of personal information that could or should be adopted by the UK?

Question 25.

Comments: 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?

Question 26.

Comments:

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.

## **Section 7: Additional questions**

Question 27.

Comments: 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?

Question 28.

Comments:

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