

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

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 Direct Marketing Association (UK) Limited (DMA) welcomes the opportunity to respond to the Data Sharing Review's consultation on the use and sharing of personal information in the public and private sector. The DMA is Europe's largest trade association in the marketing and communications sector, with over 930 corporate members and positioned in the top 5% of UK trade associations by income. The total value of direct marketing to the UK economy was £43.7 billion in 2006. This comprises three separate figures; £ 16.4 billion on expenditure on direct marketing media and activities, £ 15.6 billion on employment and £ 11.7 billion on overheads resulting from employment (Economic Impact Analysis 2006: the Direct Marketing Industry published by the DMA). The DMA

represents both advertisers, who market their products using direct marketing techniques, and specialist suppliers of direct marketing services to those advertisers - for example, advertising agencies, outsourced contact centres etc. The DMA also administers the Mailing Preference Service, the Telephone Preference Service and the Fax Preference Service. On behalf of its membership, the DMA promotes best practice, through its Direct Marketing Code of Practice, in order to maintain and enhance consumers' trust and confidence in the direct marketing industry. The Direct Marketing Authority is an independent body that monitors industry compliance. Please visit our website www.dma.org.uk for further information about us.

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: a) individuals

- one stop shop for consumers when dealing with public organisations which may give them better services through a joined up approach
- reduction in fraud
- targeted marketing
- Sharing of individual's registration(s) on the Preference Services under controlled licensing arrangements allows suppression to function and helps the industry to be environmentally responsible.

b) Society

Reductions in crime/fraud as offenders are likely to be identified before they commit further offences and appropriate help can be provided to them.

Better delivery of public services

Greater consumer awareness of data protection legislation and their rights

Greater awareness amongst organisations involved in data sharing of their obligations under the Data Protection Act which should lead to better compliance with the Act.

Question 3.

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

Comments: a) Individuals

Perception that they have lost control of how their personal information is used, leading to fears of a 'surveillance society'. This is particularly the case if organisations are not transparent about the reasons for data sharing and the security measures taken to protect data.

Increased risk of data security breaches, particularly if organisations are not aware of their obligations under the Data Protection Act and are therefore not complying with it.

b) Society

As per individuals 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: Data sharing without the explicit consent of individuals provides the greatest opportunities, for example developing a one-stop shop for citizens across all government departments and the private sector. However, it also provides the greatest risks of leading to a 'surveillance society.'

Organisations can mitigate these risks by telling consumers who their data will be shared with. An example of this is the new wording which financial services companies now use to deal with sharing of information with the credit reference agencies which was introduced around 2000 in conjunction with the Information Commissioner's Office.

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: The DMA is not aware of any examples.

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: The DMA is not aware of any examples.

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: DMA is not aware of any examples.

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: The DMA is not aware of any examples.

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:** The Data Protection Act (DPA) provides a sound set of principles for protecting citizens' privacy rights without overburdening organisations which collect and process data.
- The problem is the lack of enforcement powers of the Information Commissioner's Office (ICO) which means that organisations have in the past believed that if they breached the DPA the consequences would not be serious.
- However, that has changed with the new ICO approach and enforcement strategy over the last 18 months to 2 years.
- The lack of enforcement powers is particularly an issue with electronic marketing, especially in the case where an organisation appeals against an enforcement notice. The appeal means that no further action can be taken, even if the organisation continues with the activity referred to in the enforcement notice, until the appeal is heard by the Information Tribunal.
- The ICO's recent paper Data Protection Powers and Penalties The case for amending the Data Protection 1998 provides a way forward which the DMA supports provided any new enforcement powers are used in a proportionate way against persistent and wilful offenders who are not making any effort to comply with the DPA, rather than those organisations which are making an effort to comply but make an honest mistake.
- The DMA would welcome the opportunity to work with the ICO in producing best practice guidelines on compliance with the DPA for the direct marketing industry with particular relevance to data security issues

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: The DMA believes that public authorities and private organisations generally adhere to the second principle of the DPA.

DMA Members are also subject to the DMA Code and monitoring by our Compliance Department. The Direct Marketing Authority takes enforcement action against DMA members who breach the DMA Code, We believe that the majority of our members tell consumers that the information they give will be used for the purpose of sending out marketing communications.

We believe that the second principle is very valuable and is important that citizens are told the purposes for which organisations will use the personal information citizens have provided to them.

The DMA believes that the existing legal framework under which citizens need not be told

that their personal information will be used for certain purposes which are ancillary to or self-evident from other purposes, which they have been told about, should remain in place.

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

- **Comments:** Lack of financial resources at the ICO means that all their activity has to be prioritised
- Lack of knowledge of the DPA means that organisations hide behind the DPA (e.g. utility companies refusing to disclose to social services the fact that the gas supply had been cut off to a house where elderly couple living)

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

Comments: The DMA believes that the ICO should have more enforcement powers – please see response to Question 9 above for details.

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: There are problems with an organisation, which has branches in different Member States of the EU, sharing data which it has collected in one Member State with branches in other Member States due to the different ways in which the Data Protection Directive has been implemented into the national legislation of Member States. For example, some national data protection authorities require transfers of data to other countries within the EU to be notified to them, even though this is not a requirement under the Directive.

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: The DMA believes that before looking at increasing or changing statutory powers to make the sharing of personal information more secure, the Government should encourage better compliance with the DPA. Most of the recent data security breaches have been caused by failure to comply with the security principle of the DPA. Businesses do not need more legislation in this area; they need more help in ensuring compliance with the existing legislation. The DMA is happy to work with the ICO in developing specific guidance for the direct marketing industry.

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: The standard Notification Fee for all organisations, regardless of their size, places an unreasonable burden on small businesses. Larger organisations

should pay an increased Notification Fee based on a sliding scale.

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: No, it is not clear. Consent is only one of the grounds in Schedule 2 of the DPA which will allow the sharing of personal data. However, many organisations are probably not aware that this is the case and more guidance should be provided in this area on the other grounds for the sharing of personal data in Schedule 2. Again, the DMA is happy to work with the ICO on producing specific guidance for the direct marketing industry.

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

Comments: In some cases, such as disclosure of information in the interests of justice, it would be impractical to gain individual's consent.

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: The DMA believes that there should be a wider public debate led by Government about the benefits and risks of greater sharing of information particularly within the public sector and between the private and the public sectors.

Once the public debate has taken place then organisations should be expected to do more to explain their use and sharing of public information.

Citizens need to be given the right to subscribe or unsubscribe to or from, depending on the communication channel used, having their personal information shared with other organisations, where this is appropriate, for example in the case of direct marketing.

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)?

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

Comments: The DMA has no practical experience of using these documents.

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: The development of the internet has clearly made the sharing of personal information easier. However, it has also brought greater security risks as sending an unencrypted file over the internet is the equivalent of sending a postcard in the postal service. Many of the recent data security breaches have occurred because of the lack of basic IT security measures such as encrypting information and /or password protecting it. Similarly, the increase in the processing power of personal computers and laptops has meant the large customer databases can now be stored on such equipment. The recent data security breaches caused by the theft of laptops have highlighted the danger and risks of this development.

The use of web- analytical tools (cookies, web beacons and gifs) enables email marketing to be more targeted and relevant. However consumers must be told that such tools are being used, the benefits of the use of such tools, and how to unsubscribe from their functionality.

The development of privacy enhancing technologies, such as for example the ability to block cookies, should help to ensure that citizens have greater control over the disclosure of personal information online.

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: While there is some merit in this proposal, the risk is that any legislative change will be quickly out of date owing to technological developments. It would be preferable to use non- legislative methods, such as guidance notes issued by the ICO, which are more likely to be able to be updated in line with technological developments. Again, the DMA would be happy to work with the ICO in producing specific guidance for the direct marketing industry.

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: The DMA has no direct experience of the use of privacy enhancing technologies in such areas.

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: The DMA is not aware of any jurisdictions that contain features that could be useful in a UK context.

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: The DMA is not aware of any examples.

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: The DMA is aware that other European countries have implemented the European Data Protection Directive in a more restrictive manner. The consequences of this are that 1) it is more difficult for UK organisations to carry out their activities in these countries and 2) it is more difficult for UK organisations to have data protection policies and procedures which they can apply on a global basis.

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: Yes, the DMA is aware of significant differences, particularly in other European countries that were ruled by totalitarian dictatorship regimes in the twentieth century.

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: Yes, the DMA would welcome the opportunity to work with the ICO on producing guidelines on data sharing for the direct marketing industry, particularly dealing with data security issues.

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

Comments: Please see response to Question 27 above.