

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.

Comments: Acxiom are world leaders at helping companies use information to improve their marketing and business results, ensuring efficient data manipulation to enable people to receive information that is relevant to them and not to receive information to excess – better targeting – better for the consumer – better for the industry -better for the environment. Acxiom’s marketing and information management solutions, provides its Clients with the ability to see all their customers and prospect information in one place - regardless of channel. Our solutions:

- Ensure the most relevant and timely offers are made at the point of sale
- Manage contact strategies across multiple channels
- Make recent customer activity available to all channels
- Improve customer relationships
- Personalise channel offers through accurate customer recognition
- Reduce risk and exposure to fraud.

We collect personal lifestyle and demographic data via questionnaires, websites and warranty cards and we also licence some data from third party suppliers. This data is stored securely in our state of the art secure centre in Leeds and licensed to our clients under contracts containing data protection obligations for their use in direct marketing campaigns and research and

analysis.

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

Question 2.

Comments: Benefit to individuals is that we are involved in highly targeted marketing – the in-depth level of data we collect means that we enable our clients to target people who have a genuine need to e.g. renew insurance on a specific date, instead of bombarding people with direct mail that is irrelevant to their needs which they will have no interest in.

Benefit to companies – by cleaning their existing customer databases and providing new or updated data where necessary we are helping them to decrease their marketing costs by reducing the number of mailings to duplicated or inaccurate records.

Benefits to both – via our Digital division – encouraging greater use of digital marketing rather than the traditional Direct Mail

Each of the above benefit society as a whole.

Question 3.

Comments: Appropriate measures when transferring data between companies, storage and limited justified access to storage areas together with adequate access control are areas where if not conducted appropriately can lead to risk of loss of personal information

β Need to ensure that there is adequate security for the data especially when it is transferred outside the EEA to countries which may not have data protection laws.

β No harmonisation of data protection laws in Europe which can make sharing personal data among European countries complex and cumbersome and can cause misinterpretation

β The more that personal data is shared, e.g. between financial services organisations, without adequate risk assessment and processes the greater the risk of data loss resulting in the increased of potential criminal activities

β Too much pooling of data could give the impression to individuals of a 'surveillance' society.

Question 4.

Comments: Appropriate sharing of information, not to excess and always only sending relevant data are key - The right information to the right person and the right time using secure and trusted methods of transfer are key performance indicators when assessing scope and methods of information sharing
Sharing personal data via email or the internet can be the most secure method of sharing information provided that encryption/passwords are used when appropriate. If encryption/passwords are not used then this can be a high risk method of information sharing, especially if the data is left on a laptop or other

portable device.

Sharing personal data via courier, post or fax would be more high risk as papers can be left lying around and fall into the wrong hands. .

Question 5.

Comments: As experts in data matching and the design of complex database applications, including access controls, we see significant risks in pooling or aggregating sensitive data such as medical records ('Spine') where life or death decisions may be made on the basis of matching algorithms and data merges that are far from foolproof.

Data aggregation between public authorities or government departments risks being excessive for the purposes, as we saw with the HMRC debacle, since business processes and controls are currently weak in this area, and there is little accountability or transparency – there appears no rigorous process to justify what is required, for what purpose, and some objective sufficiency tests.

Question 6.

Comments:

Question 7.

Comments: It would be in the Public interest if the register of deaths was automatically loaded into the Mailing Preference Service and thereby distributed to the Direct Marketing industry as a suppression file. MPS cleaning is compulsory for members of the Direct Marketing Association and the vast majority of UK marketers clean their mailing lists against the MPS on a regular basis, so this would be the most effective way to stop mail to dead people.

Currently the Mailing Preference Service has around 4 million records and it has operated for over twenty years with a commendable level of consumer satisfaction amongst those who have registered with it. However though in the past it has been very successful at getting registrations from living people who object to mail, only a small proportion of dead people have been registered with it.

In the past the Government has expressed concern at the idea of lists of dead people being available in case of inappropriate use such as marketing to the bereaved. While we're not aware of this ever happening to either this data or to the similar records available as part of the rolling register, there is the opportunity to blend deceased records within the larger MPS file and remove the marker indicating whether someone has died or merely no longer wants to receive mail this would achieve the industries objectives:

Environmental savings
Reduced upset to bereaved people
Costs savings for business.

Whilst also avoiding the hypothetical scenario which the Government has cited as its reason for not releasing this data.

Question 8.

Comments:

Section 3: The legal framework

Question 9.

Comments: Weaknesses/scope for change are:

- β unclear definition of personal data in the DPA as highlighted by the current difference of opinion between the court's and the Information Commissioner's interpretation.β Not much guidance on what legitimate interests really means in practice
- β No approved form of contract for transfers of personal data outside the EEA from processors to sub processors
- β Lack of knowledge/compliance with the DPA of so many companies – perhaps should make it legal requirement to have a privacy officer in substantial private organisations/public authority department
- β The boundary of responsibilities between a Data Processor and Data Controller is often unclear

Question 10.

Comments: We are unable to comment in general. However, our company is a private organisation and makes every effort to comply with the 2nd principle, however on some occasions we have needed advice from the ICO in relation to this principle, the length of time taken to obtain a definitive answer to our question has varied which is not always helpful in a commercial situation.

Question 11.

Comments:

- Lack of knowledge and understanding of the DPA. Following on from earlier suggestion of making it a legal requirement to have a privacy officer, this person should also have to obtain an official certification in the DPA and ongoing obligation to keep this up to date every year.
- Relatively new legislation so will take time for the courts/ICO to clarify its meanings.
- Lack of enforcement powers available to the ICO

Question 12.

Comments:

- β Need clear mechanism and approved 'model clauses' for dealing with onward transfers of personal data outside the EEA from processor to sub processor
- β Simplify process around binding corporate rules
- β Include a definition of personal data in the DPA to resolve current conflict between the courts and the ICO
- β Define what is meant by legitimate interests
- β Make it mandatory to have a certified privacy officer in substantial private organisations/public authority department
- β Clarify the Data Controller/Processor split

Question 13.

Comments: Negative aspects would be:

- ß Lack of harmonisation in the UK / EU legislation
- ß Hugely different enforcement regimes across Europe – eg – compare UK with Spain where the ICO is not publicly funded and generates all its revenue from fining companies for non compliance with the DPA – enforcement should be more standard across Europe to make it easier for pan-European companies to comply
- ß Please refer to previous comments on transfers outside the EEA from processor to sub-processor and legitimate interests.

Question 14.

Comments:

Question 15.

Comments: As previously stated we have implemented the DPA within our processes and have adequately trained staff responsible for the areas of Privacy and security - the danger in looking at 'unreasonable' is that this is in the opinion of the person you are asking and could quite well lead to a drop in standards and best practice

Section 4: Consent and transparency

Question 16.

Comments: As an organisation that collects a large amount of data via Lifestyle questionnaires we are well aware of the requirement for consent.

Question 17.

Comments: Transparency is key to gaining consent as it must be 'informed' we are not sure that any barriers are required for gaining consent - just enforcement action when it is not collected correctly
If this question is around removing the other legal conditions for processing set out in schedule 2 of the DPA and making consent the only condition to enable sharing of personal information then I wouldn't advocate such a change to the current practice. The Schedule 2 conditions in general are important and valid exceptions to seeking consent eg- without condition 4 doctors may not be able to administer life saving treatments to patients in hospital, and without condition 2 companies would not be able to contact people to chase a debt that is owed.

Question 18.

Comments: We don't have any information or statistics on the current efficiency of subject access requests so its difficult to comment here. In our company the subject access request process works very effectively.

Question 19.

Comments: There is a lot of information on the ICO website on this. From a quick review it looks like a good tool to use if a company is working on a large project which may have privacy law implications as this will enable the relevant organisation to identify and manage any privacy risks. with regard to the Privacy Impact Assessment - this document looks good but as we are unable to download as a

document and read it it is difficult to comment.

Section 5: Technology

Question 20.

Comments: Technological advancements have in some ways made it a lot easier to share personal information and to abuse information - the likes of websites like facebook have made it very easy for people to put information about themselves to share with friends, but they are not always aware of how this information could then get into the hands of others - ability to handle technology does not mean that we are not vulnerable to abuse. On the other hand technology like encryption has given us the tools to ensure that data sharing can be more secure - it only needs training and awareness to take advantage of this.

Question 21.

Comments: This would also depend on the type of personal data being shared and its sensitivity / scope for fraud or other criminal activities. The higher the sensitivity the more necessity there is for encryption. However, it is very difficult to define specific technological safeguards as they very quickly become out of date.

Question 22.

Comments: Yes we do believe that such techniques could help safeguard personal privacy. We have used this technique when creating research datasets where the ability to link the data back to an identifiable individual was not required. Pseudonymisation is also a tried and tested IT technique – if a programmer is running some analysis and doesn't need contact details but does need a URN to link back to the main database then this is a useful technique for conserving IT resource and designing in Privacy.

Section 6: International comparisons

Question 23.

Comments: As previously said one concern about the E U Directive is the way it has been differently implemented within each E U member state - hence we would respond that there could well be ideas in other EU States that would be good to use in the UK but would be difficult to be more specific at this stage - although having Privacy officers based in several E U member states we would be happy to discuss this further with you at a later stage should you feel it appropriate.

Question 24.

Comments:

Question 25.

Comments: We understand the data protection laws in Spain and Portugal make it extremely difficult to engage in sharing of personal data in those countries. This has the effect of preventing business.

Question 26.

Comments: We would assume that public attitudes to sharing data in Spain and Portugal are very different to those in the UK because of the restrictive nature of the laws in those countries.

Section 7: Additional questions

Question 27.

Comments:

Question 28.

Comments:
