

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. Explain what your interest in data sharing is – what personal information do you hold, collect, show, how do you collect and for what purpose

Comments: The comments made on this form have been submitted by various individuals from Southwark Council that represent areas such as Knowledge & data service, Council tax, Performance Management and Parking. The personal details held revolve mainly around name and address data.

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 b) society – provide examples

Comments:

- More efficient, faster services to the customer, customer only has to provide the data once + more joined up service delivery to meet central government directives
- Necessary for the delivery of statutory duties e.g. at risk children.
- Expected of us by public – e.g. public don't want to report anti social behaviour to police, and then report again to council.
- Improved recovery of C-Tax/Rent debts by providing information such as forwarding

addresses and employment details and use additional income to provide more services to benefit society as a whole

- Prevention of Housing Benefit & Council tax fraud.
- Better targeting of people in need
- More efficient administration will reduce costs of service provision
- Reduction of data held - public sector hold far too much information which in itself is a major risk.
- Data accuracy will improve, require a people data standard in the same way as we have BS7666 for properties.

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

Comments:

- Can list usual risks BUT then from public sector perspective point out risks are outweighed by risk of not sharing data eg Soham, Climbie etc.
- Risks of inaccurate data being shared which triggers wrong service provision e.g. if a person is wrongly assessed by a credit rating agency as a risky person to lend money to, everyone using that information may mistakenly refuse that person credit
- The wider the audience is to data the bigger the risk that the data will be misused e.g. identify fraud
- Data can be mis-interpreted or people's prejudices come into play e.g. former convict moves into an area and is victimised by community due to information being more widely available

Question 4. There are wide variations in the scope and methods of personal information sharing. What scope and methods, in your view, pose the greatest opportunities

Comments:

- Master Data Management. E.g. in the delivery of the OneTouch service – one call gets you a number of different services.
- Risk management. E.g. Can use data collected by public organisations to assess key risk factors of children going into care – prevention rather than remedy.
- On-line mapping service allows more rapid interpretation of data and more informed decision making e.g. being able to plot where single parent families enables better planning and location of services to support them

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:

- Social Care of children or vulnerable people – issues arise where individuals are known to some services but not to others through lack of data sharing
- Individuals that come to the attention of a service (e.g. police) but not referred on (e.g. to social services).
- Difficulty in identifying repeat cases due to incomplete address/personal data e.g. a blue badge being sent out to the wrong address due to duplicate records being stored for the same person with different addresses
- Numerous copies of the same spreadsheet being sent around a council and between agencies sometimes with far more details than is required for the intended recipients due to poor data scrutiny
- The data held by the DVLA is 4 -5 months out of date which restricts our ability to recovery revenue arising out of penalty charge notices for parking offences, if the the

DVLA collected NI or passport number it would make tracking an individual to an address much easier and avoid the expense of passing warrants onto bailiffs for collection

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:

- Could use examples like Homecare financial assessment where DVLA data is being needlessly held because DWP and DVLA prohibit online access.
- When a payment is made with a payment card in a shop, even though the payment is authorised with the payment card company by means of a realtime transaction, some companies will also record the details of the payment card into their own database, which is unnecessary and potentially putting your details at risk – companies should be obliged to ask the payment card holders permission first before they record their details in these instances
- When making a simple purchase in a shop or an enquiry over the phone some organisations will insist on taking personal details when it is totally unnecessary – it should be made much clearer to the customer which details they are not obliged to supply to obtain the service
- Many companies will attempt to collect a broad range of information for their own marketing purposes e.g. Nector card, some people will supply their information thinking it is obligatory or are totally unaware of how it will be used
- Some companies providing on-line services, often require their customers to register first, making some personal details mandatory for registration which are unnecessary.

Question 7. 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:

- Full version of the Electoral Roll is not available to other departments within the council due to legal statutes
- Register of births can only be shared with a limited number of departments again due to legal statutes
- Use of NI and NHS numbers is restricted by legislation, this could be a very useful identifier for matching people between departments within the council and with other public agencies
- As before – non referral between agencies is an issue, largely due to cultural and legal issues. Would have considerable benefits in terms of prevention/risk management.
- To assist in the collection of penalty charge notices it would be useful to have access to TFL systems such as the automated number plate recognition system and Met police data who can access our data but we cannot have theirs
- To assist in the collection of Council Tax /NNDR it would be greatly beneficial to have access to personal information held by the DWP & HMRC. Council Tax regulations and S29(3) of the DPA already allow for such data to be disclosed to billing authorities, but historically the DWP & HMRC have refused to provide the data. We

have very recently secured agreement from the DWP that they will share personal data, but no such agreement has been forthcoming from HMRC. Historically, HMRC have bombarded local authorities with requests for data disclosure under the DPA, but have not been prepared to disclose information in return when requested by LAs under the same part of the Act. Therefore the barriers are cultural rather than legal.

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 sharing of contact details between mobile phone suppliers. When a contract for a mobile phone is nearing expiry other network companies will make unsolicited, calls to the individual to persuade them to change suppliers. Often these calls are made in such a way that the customer is confused as to who is contacting them and what is being offered.
- The unsolicited marketing of individuals by post should be better regulated, often individuals are deluged with marketing mail that is put straight into a bin, this is not only very wasteful environmentally but poses a risk to the name and address data on the letter
- Faxing of personal information is not a safe way to share information as most faxes are not located in secure areas, however it is common practice to share information in this way especially in the legal industry.

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:

- Confusion exists as to what can and cannot be shared due to the greyness and wooliness of the legislation – it is very open to interpretation. Any freedom of information request has to be evaluated on a case by case basis, so application of the DPA is very variable across the public sector as it is so subjective
- Needs greater emphasis on data quality and accuracy
- The DPA is often used as an excuse to avoid doing things
- Is difficult in practice to be 100% compliant with historical documents
- The area of data disclosure - the Act would work better if disclosure (where legitimately requested) was a legal obligation with penalties rather than voluntary.

Question 10. In your view, how well do public authorities and private organisations adhere to the second principle of the DPA?

“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 purposes or those purposes”

How valuable do you believe the second principle is? Please provide examples and the reasoning behind your response.

Comments:

It is one of the most important, and will continue to become more important as more efficient ways of collecting data become available. E.g. London Low Emission Zone, or Congestion Charging Zone both monitor vehicles in and out of London. Fine for administrating the zone, but also could easily be mis-used, even if not intentionally. E.g. data could be provided to Bailiffs to assist in the administration of court fines. All ok, until one bailiff realises that he can use the system to identify when an individual is not at home and target more vulnerable relatives or clamp their car when they are some distance from home, thereby holding them to ransom.

Increasingly important will be also the 5th principle. It should be tightened from “as long as necessary”, which basically means as long as you want to “as long as necessary to administrate that transaction or event”. By building up data on an individual it is possible to build up a pattern of behaviour, or a personality type, and use that data to their disadvantage E.g. internet usage – its fine to monitor the use of an online banking website to administer things like payments, and even to monitor website usage. However someone who accesses their online bank account daily, would clearly be an individual concerned about their financial status. This could lead to pressure sales techniques for a bank loan, or adverse credit ratings, without the person actually having done anything. Its similar to ASBOs – ASBOs limit a pattern of behaviour – a series of events or actions which individually are not unlawful.

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

Comments:

- Suspicion on the part of the public.
- People posting personal data themselves on social networking sites being unaware of how they exposing their personal details to misuse.
- Again, in the area of disclosure, the apparent institutional culture of non-disclosure amongst some government departments is a barrier. There is an emphasis currently on ‘joined-up government’ but there is a danger that when it comes to collecting the taxes that pay for local services, joined –up government will not apply.

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

Comments:

- Needs greater clarity re public sector sharing information to improve service provision and reduce cost
- Greater emphasis on data quality
- Greater detail on timescales
- Greater obligation on making a collecting of information to inform their customers of their rights

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:

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? Provide examples.

Comments:

Question 15. Are there any parts of the legal framework that place an unreasonable burden on business? Provide examples. Please outline your proposals for streamlining the legislation to ensure that such burdens are minimised.

Comments:

- The freedom of information (FOI) legislation is increasingly being abused by the media to 'get a story', often a council will have to pour many resources and hours of effort into servicing these requests. Normally the results of these types of FOI's are not reported as they are not deemed newsworthy enough. There should be a limit on the number of FOI's a particular individual can raise and a valid reason for the request other than just 'fishing for a story'.

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

Comments: No

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

Comments:

- Manageable on a very small records base but massive implications on large data integration projects like local government. No system or process could administer a consent process and would lead to chaos and confusion. Better to mitigate by having clarity around what information public sector agencies share.
- Often we have found that the public expect us to share information, particularly internally and often between local services (e.g. PCT and council – many people can't understand why if someone is discharged from hospital, why they are not immediately known to social services)
- Multi-cultural adult literacy could be a barrier for people needing benefits

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:

- Clear sector statement on what data LAs share within depts and other agencies.
- Stronger access rights, particularly on-line to the individual in the public sector. In many cases it would strengthen service delivery and reduce fraud.

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: 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:

- Privacy impact assessments are valuable in raising the awareness of data and any associated DPA issues at the planning stage of the project, sometimes these are overlooked until well into the development stage when any necessary remedial action can be far more costly
- Training on DPA issues should be given to any person dealing with personal data to ensure they not only understand their obligations but the importance of good quality data

Section 5: Technology

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

Comments:

- Growth in data held as IT systems make it easy
- Growth in inaccurate data
- Duplication of data
- Access to data easier
- Self service
- MDM

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:

- Yes data should be encrypted but Gov has to provide one solution and fund roll out
- Similar concerns about wireless technology. E.g. Wi-Fi hot spots for use in council buildings could be hi-jacked by criminals 'lisening in'

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:

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? Provide examples

Comments:

Belgium where law states public sector must share data

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:

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:

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:

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:

- Funding for public sector for Data Mgt, compliance and implementation of new technology
- Any approach taken should be pragmatic, it should not over burden a process to make it impractical

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

Comments: