

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: As a Local Authority, we share information out of necessity. We share personal information about our residents, services and children in order to carry out our duties and obligations as a statutory body. As such, we have numerous purposes for collecting personal information.

We collect information from residents, government agencies and third parties. We hold most of this information in various back office IT systems and we share the information usually by electronic means. In some cases we share the information manually by fax, e-mail, internet forms or letter.

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

Question 2.

Comments:

- a) Individuals
 - Ability to provide joined up services e.g. individuals asked for information once rather than multiple times.

- More efficient services – e.g. avoid collecting information multiple times.
 - Cost reduction of service provisions (efficient services = cheaper services).
 - Reduction of data held – e.g. the public sector hold far too much information, which in itself is a major risk.
 - Compliance with Government performance indicators e.g. NI14 is easier of data that is shared as service can be provided first time of contact.
 - Data accuracy will improve if the Government gets serious about the importance of people data quality. We have BS7666 for properties but need to enforce people standards.
 - We believe that with the modernisation of our services and the expectation of our customers, it is a necessity to share information, and in fact, to increase the amount of sharing.
- b) Society
- Reduction in fraud (hence reduced costs) – e.g. data matching through information sharing can identify possible fraud.
 - Targeted services – with data profiling through sharing information, the services that we have limited resources for can be targeted to where the demand is and that the right services are established.
 - Joined up government services – to the public that currently have to deal with numerous government and Local Authority departments, sharing information helps provide seamless services to society.

Question 3.

Comments:

The risks are outweighed by the risk of not sharing e.g. Soham murders and the Victoria Climbié case.

a) Individuals

- Security of information sharing. As highlighted with recent loss of personal data, the information needs to be protected and disclosure on sharing is exposed at its weakest point e.g. inconsistent policies, training and awareness.
- Accuracy of information that will be shared. An error could get distributed to multiple areas and cause errors to services being replicated leading to wrong service provision. People may no longer rely on the information.
- Information is retained for longer than is necessary after it has been shared. Information that lingers on may no longer be accurate.
- Information that is used for other purposes than the ones that the information was collected for. The individuals could lose control over their data, which may impact on their human rights.

b) Society

- Lack of trust with information sharing may lead to the cessation of information sharing, which will have a devastating impact on the ability to provide services efficiently, cost effective and in a modern manner.
- Data quality, if organisations cannot rely on the information being shared, it could bring sharing to a halt.

Question 4.

Comments:

a) Opportunities:

- Deliver real benefits to customers through efficient processing and use of their personal data e.g. ask for information only once.
- Reduce the cost of providing services by efficient use of personal information through sharing.

b) Risks:

- Maintaining the integrity of the purpose that the information was collected for. As information gets shared with different bodies, there is a significant risk that controlling the use of the information in line with the intended purpose will be difficult.
- Understanding where the data is being shared. Within large organisations, there is so much information that is shared to necessitate the organisation's processing. Not fully knowing where the information is shared poses a risk to the security and control of the information.
- There is a significant risk of disclosing information to the wrong people considering the volume of the information being shared.
- Sharing information takes place using many methods e.g. file transfers, disks, portable devices. There is a risk to the security of personal information as the personal information may end up being stored in multiple platforms.
- There is a risk of inaccurate processing if the personal information being shared is inaccurate or out of date.
- Because it is difficult to uniquely identify individuals, there is a risk of sharing information about the wrong person.

Question 5.

Comments:

Because there are restrictions on the sharing of information, the council holds too much information about customers because it has to duplicate and segregate personal information for each intended purpose. For example, there is a council tax database, which holds contact details of customers as well as a contact centre database (i.e. CRM), which holds the same contact information. The golden rule should be to store information once (accurately) and share where needed rather than duplicating the information in several places within an organisation (which makes it difficult to keep the information up to date).

The council could reduce the information it holds by ensuring accurate information about customers under a customer view, such as a client index. At present the council holds too much contradictory information about its customers in back office silos. If it is not accurate, it can't be relied on – hence the tendency to collect information again rather than using existing information.

In some cases information is needlessly held, e.g. Homecare financial assessment and DVLA data being needlessly held because DWP and DVLA prohibit online access.

However, there is not enough personal information held to uniquely identify an individual making it extremely difficult to link and share information about individuals.

The current process has to attempt to match personal details to find links, which has a risk of errors.

Question 6.

Comments: n/a

Question 7.

Comments:

- a) DWP and DVLA – wider online access to minimise the customer providing the same information.
- b) Inland Revenue and Benefit Assessment. Able to check customer information when making applications e.g. parking permit applications.
- c) Passport Office and Local Authorities. Able to validate individuals, which could improve the process of individuals applying for services.

Question 8.

Comments: None identified.

Section 3: The legal framework

Question 9.

Comments:

- a) Confusion exists as to what can and cannot be shared. Interactions between the DPA and legislation (e.g. 1992 Social Security Act) result in confusion and inconsistencies. There is no clear guidance for the public sector as to what data sets can be shared and with whom. Currently, this results in all 433 Local Authorities all interpreting things different ways leading to confusion for customers and a barrier to Transformational Government. We currently feed off snippets of information from the Information Commissioner (e.g. the use of Council Tax and the inconsistencies – i.e. strictly speaking, it is illegal to share the information but the IC will not pursue this unless there is a complaint). This makes it practically impossible to train staff and also staff are further confused if they come from different Local Authorities.
- b) Need sector variants i.e. Local Government DP framework in which Local Authorities can operate. This will stop all confusion and will make it easier for the public to understand. This framework could be based on the IC's phrases regarding council tax.
- c) The profile of data protection needs to be raised - needs greater emphasis on data quality and accuracy.

Question 10.

Comments:

The reality of the data protection act is that information is likely to be used for other purposes. It is important that the DPA considers this, as information cannot be contained for each individual purpose in the modernisation that is taking place. The purposes should allow for broader uses. For example, at a Local Authority level rather than at an individual service transaction level i.e. the purpose for processing information should be to provide services to customer in line with the responsibilities of a LA rather than to limit it to process a parking permit. The customer's expectation

is that the council shares their information within the council. Customers are often frustrated when they have to provide their personal information more than once and LAs have to segregate their information. It becomes difficult to know which information is the most accurate one. We should be providing cross service provision rather than transaction based services.

Question 11.

Comments:

- a) Definition of data itself. The revised definition following the Durant case does not make any logical sense – personal information is personal information regardless of how it is stored or accessed. If there is to be a special case for manually held information in unstructured files, it should be under a new exemption of the Act rather than an interpretation of what data is. The definition as it currently stands is hard for any staff to understand and apply to their day to day duties.
- b) The current notification process should be reviewed. Whilst it is OK to register the name and address of the data controller, the stated purposes are fairly meaningless e.g. the purposes are not linked to the sources and disclosures of information. We would suggest that the purposes are replaced in the notification process by a register containing a list of external organisations that information is shared with together with the specified purpose for sharing.

Question 12.

Comments:

- a) In order for organisations to take the DPA seriously, we would support the proposal to make certain breaches of the DPA a criminal offence, such as the wrongful disclosure of information and the lack of care in handling personal information.
- b) Most LAs are seeking to provide cross services rather than individual transactions, so it would be useful to revise principle 2 of the DPA to allow for a broader use of the purpose at an organisation level rather than a transaction level.
- c) Needs greater clarity regarding empowering the public sector to share information to improve service provision and reduce cost.
- d) Greater emphasis on data quality.

Question 13.

Comments:

Question 14.

Comments:

- a) A standard for protocol agreements would enable better and more secure sharing of personal information. A standard will help ensure consistency.
- b) A framework code of practice will help the public sector and private sector operate better sharing of information processes.
- c) Under the notification process, a register of information sharing will assist in controlling the information sharing process.

Question 15.

Comments:

Section 4: Consent and transparency

Question 16.

Comments:

Yes – there is suitable guidance on the issue of consent (when it is needed and when it is not needed). There is an issue over the maintenance of consent agreements.

Question 17.

Comments:

The key barrier is practicality – as no system exists that can care for the maintenance of agreements – there could be a backlash from customers if information has to be shared regardless of consent being given.

No major barriers on very small records based projects but significant implications on large data projects like Local Government. No system or process could administer a consent process. This would lead to chaos and confusion. The process could be mitigated by having clarity around what information public sector agencies share.

Question 18.

Comments:

A public register (via the notification process) of information sharing agreements.

A clear sector statement on what data LAs share with departments and other agencies.

Question 19.

Comments:

- a) By making it a legal requirement under the Act to have an information sharing policy in place.
- b) By linking information sharing to the Government strategy.
- c) By ensuring that data protection stays in tune with Government legislation and objectives in the public sector.

Section 5: Technology

Question 20.

Comments:

- a) Growth in data held as IT systems make it easy.
- b) Growth in inaccurate data.
- c) Duplication of data.
- d) Access to data easier.
- e) Growth in self-service requiring an increased need to share information.
- f) Increase in technologies to help process data in a more secure manner.

Question 21.

Comments:

Yes – It should be mandated that all personal data must be encrypted, but Government has to provide one solution and fund the roll out.

Question 22.

Comments:

Section 6: International comparisons

Question 23.

Comments:

Belgium where the law states that the public sector must share information.

Question 24.

Comments:

Belgium (as above)

Question 25.

Comments:

Question 26.

Comments:

Section 7: Additional questions

Question 27.

Comments:

- a) Funding for the public sector for data management – compliance and implementation of new technology.
- b) More standards, in particular about 3rd parties.

Question 28.

Comments:

The data protection act should be overhauled to enable Local Authorities to share information more consistently. At present, 433 authorities have different interpretations of what information can be shared and with whom.