

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:

1. Inter departmental sharing within local govt. in order to develop and deliver 'quality services' to the public.
2. Inter organisational sharing (where cooperation between Local Govt., Police, PCT, College, Ethnic groups etc.) need to develop and deliver services throughout the borough or more widely.

Employment details : name, address, financial, health, criminal, age, ethnicity, sickness
Previous dealings, communications, services received from Local Govt.

Restrict data holding/sharing between those 'services' who need to know, then only to trained staff using specific procedures relating to either/both manual/computer data.

Taxes, benefits, licences, employee salaries & expenses, planning & building regulations, social services. , education, elections, insurances, legal, education, recruitment.

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

Question 2.

Comments:

- a) Of advantage to the individual who receives a swift and competent and integrated service.
e.g. notification of benefits they didn't know about, including greater convenience through e.g. single smart cards
- b) Improvement in society's perception of local govt. as an efficient and responsible organisation that makes the individual of paramount importance.
e.g. neighbourhood safety initiatives, efficiency savings to the public sector bodies

Question 3.

Comments:

- a) Unauthorised sharing could result in actions being taken that disadvantage individuals contrary to organisational policy or ethical standards. Potential loss of reputation or privacy, even financial loss if information gets into the wrong hands
e.g. engender religious or ethnic problems in a community.
- b) With mistrust comes an unwillingness of individuals to provide all relevant and accurate information - a case of the 'minimum necessary' (in the eyes of the individual, and then maybe not 100% accurate). This could result in the service falling below desired/acceptable levels.
e.g. Benefits incorrectly calculated.

Question 4.

Comments:

Scope - Opportunities -

- 1. Development of common procedures making cooperation between organisations easier and more effective i.e. joined up services across geographical and organizational boundaries
- 2. Central Govt. development/influence of common procedures to a national standards.
- 3. Chance for organisations to report success statistics into the media.

- Risks -

- 1. Need for a 'walk before run' approach to establish basic standards.
- 2. Lack of time as such should already be in place.
- 3. Seen as a Big Brother society

Methods - Opportunities -

- 1. Standardisation of data held for a joint purpose, clarification of purpose data held for, security standards agreed.
- 2. Identification of appropriate staff/contacts in each organisation and the development of 'teams' that build up a strong effective working relationship.

- Risks -

- 1. Failure to agree standards at a basic level - possibly due to vastly differing 'own organisation' drivers.
- 2. There are wider organizational issues about interoperability including system design
- 3. Failure to train new staff and to monitor that standards are being effectively met

- and continually operated.
4. Bad publicity if only mistakes get into the media - 'bad news sells more papers than good news'.

Question 5.

Comments:

Too much -

Legal Cases and other records that are developed through internal partnership working within local authorities.

Reason -

Tend to have too much duplication through lack of co-ordination between involved parties or lack of policies on retention of originals(copies for magistrates, social workers and external barristers all held in one folder).

Too little -

nil

Reason -

nil

Question 6.

Comments:

Too much -

1. Contact details circulated throughout commercial organisations.

Reason -

1 Result being junk mail. Should be 'opt-in' not opt-out' for info. to be circulated.

Too little -

1 Often sales forces and debtor sections don't link their data sufficiently or swiftly enough.

Reason -

1 Results in reminder letters, debt chasing, general time wasting

Question 7.

Comments:

- Confusion lies in the fact that Guidance from the ICO appears to be contradictory to the legal standing of the DPA Principle 2 - the information collected was for a specific purpose but is now required to be shared for other reasons.

Requests from different departments within the authority to access e.g. the CT and Benefits system, are often met with resistance. This historical resistance to allow access is because of the conflict between the Act and the ICO guidance. There can be an obvious advantage to the data subject to share the information but should someone wish to challenge then they may have a case.

It is often easier to say no.

- Organisations don't try to share, because of rigid silo structures, because of their tasking, because they don't trust each other, because individuals can't be bothered.

- Interoperability. It is difficult to change the operating structure of a system that has been running in isolation for many years. New systems can be designed with sharing in mind.

- Security and ID issues. Need clarifying, building in to any operating system and staff re/up trained.

Question 8.

Comments: -

Section 3: The legal framework

Question 9.

Comments:

Strengths -

1. Any scenario can be related to one or more of the DPA Principles.
2. ICO guidance has increased greatly over the last few years, decision notices being helpful.

Weaknesses -

3. DPA is reasonably clear, what is confusing is the ICO guidance on using personal info. to the 'advantage' of the individual - which, in many peoples' minds, may counteract DPA Principle 2.
4. DPA Principle 2 reinforces Principle 1 - the 'fair processing' requirement.

Changes -

5. More emphasis required re the DPA 'not stopping the processing of personal information - just getting organisations to do it in a legal and responsible way'.
6. More specific training from ICO would be welcome rather than just 'general guidance'.

Question 10.

Comments:

Adherence -

1. In some instances adherence is too strong and this prevents normal everyday interactions working smoothly and effectively.
e.g. Citizens seeking confirmation of their meetings with council officials. If the citizen already know all the detail then why be concerned over disclosing?
2. Private sector abuse of info - no knowledge.

How valuable -

1. The principle is now somewhat confused ... re Q9, S&W'S, point 3.

Question 11.

Comments:

Technical -

1. Growing move towards 'secure networks' may lead to a diluting of access controls to specific database data sections because of a belief in overall security.

Institutional -

1. Data files are often structured in relation to departmental/service 'silos' although it may be difficult to do otherwise.
2. Assumption by an increasing number of organisations that all individuals are 'computer literate and have access to such'.

Societal -

1. Public trust is hard to win and sometimes the effort may not be seen to be worth it.
Instead rely on the 'legal right' to do what we want with data.

Question 12.

Comments:

Periodic checks on organisations that they have -

1. Clearly identified employees with responsibility for leadership.
2. Structures and procedures are in place for processing SAR's and other queries and

problems.

3. Procedures exist for dealing with errors and shortcomings.

nb This may appear to be an internal/external audit function but results could be somewhat lost in 'statistical reports' and have little meaning in the workplace. It needs an 'outside check' to reinforce the responsibility of individual managers.

4. Establishing appropriate protocols and citizens' charters e.g. data sharing should follow a national standard.

Question 13.

Comments: -

Question 14.

Comments:

Would help enormously if there was a general presumption that public bodies (or at least Local Authorities), being constrained under statute to be open/trustworthy/auditable, should be allowed to share personal data for the furtherance of their services to the public.

Presumed access to some registers e.g. the Electoral Roll, Births/Marriages & Deaths.

Question 15.

Comments:

Applications for social services details via DPA rather than direct requests to a Local Authority.

Remove the necessity for the Data Controller to 'recognise' Subject Access Requests and then deal with them in a rather constricted DPA methodology.

Section 4: Consent and transparency

Question 16.

Comments:

Every case needs to be judged on it's own merits. Generalisations about sharing data can only be accepted up to a point.

Decision making on sharing requires either -

1. Depts/services understanding specific legislation other than DPA that will meet the Schedule 1/2 criteria or
2. Having a policy of always obtaining consent.

Examples -

1. Clear and concise data sharing policy/policies required.

Initiatives -

1. Developing a Personal Information Sharing Charter (for inter organisational use) that makes consent the focus of personal data processing.
2. SAR policy & procedure for employees
3. Smart cards

Question 17.

Comments:

1. Could cause considerable work in developing computer systems that work differently when consent/no consent is a factor.
2. Could be easier to use the 'of benefit to the individual' approach to decide when to share.

Question 18.

Comments:

1. Pro-actively state any data sharing Arrangements on each organisations website.
2. Needs careful agreement on what all sharing parties should say, how and when updates to any agreement should be applied.
3. Right to know who organizations share info with (if this doesn't already exist) parallel to the right to find out what info organizations hold on you

Question 19.

Comments:

Develop Personal Sharing Agreements -and advertise their existence.

Certainly covers all the ground necessary - but still leaves some confusion re whether or not to share based on 'to the advantage of the individual'.

Good idea but currently looks excessively long with a large amount of effort needed to complete it in its entirety. Organisations may be averse to carrying IA's out. Much quicker and easier for a responsible employee to make a 'mental assessment' - but to record the reasons behind any decision.

Section 5: Technology

Question 20.

Comments:

1. Can be very effective but requires substantial resources to set up on individual organisations' own data systems.
 - e.g. LoCTA - would give HMRC open access to Council Tax and Revenues & Benefits databases - currently not participating.
 - e.g. ITIFLA -The DWP allow Benefit Assessors to have access to information re the claimants income. It avoids the claimant to have to provide the information twice plus speeds up the processing time of the HB/CTB claim.

Question 21.

Comments:

Yes - see Q22 comment.

Question 22.

Comments:

1. Could certainly work - but it could give an override to 'consent' .. and inadequate anonymisation could still enable identification of individuals.
2. Needs either appropriate application software that allows the user to do this or requires specialist ICT resource within the organisation.

No - often export data to spreadsheets which is then easier to manually manipulate.

Being truly 'user friendly' and then training appropriate staff to using them correctly/appropriately.

Section 6: International comparisons

Question 23.

Comments: -

Question 24.

Comments: -

Question 25.

Comments: -

Question 26.

Comments: -

Section 7: Additional questions

Question 27.

Comments:

DPA is too strict in the Benefits & Taxation arena - when making financial transactions (payments) on behalf of third parties. You are not asking for third party details but making payment , giving rather than taking.

No

Question 28.

Comments:

1. Need to recognise the resource implications on organisations to develop/install/operate comprehensive DPA data management systems e.g. employee training.
Avoid the enormous duplication created by independent development of systems, leading to cost and creating disjuncture - national guidance required which can be cascaded throughout an organisation.
2. Organisations should have a central control unit from which all the direction and guidance emanates.