

# 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](mailto: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 your interest in Information Sharing**

There are two distinct ways which the Department for Communities and Local Government is interested in information sharing.

Firstly as a Data Processor, registered with ICO, the Department collects, holds and shares personal information. The nature of this activity include HR related information for Departmental staff management; managing grant based programmes and the management of stakeholder consultation lists in various policy areas across the Department.

Secondly, CLG has a strategic interest in information sharing from a policy development perspective in the context of the Local Government White Paper, which sets out a system of Local Area Agreements and performance indicators designed to improve outcomes for citizens in relation to the key areas of worklessness, crime, liveability, education, health and housing. In particular, information sharing has an important role to play in facilitating better strategic planning and personalised service delivery for vulnerable groups and deprived areas.

This paper has been addressed in the context of the latter.

**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?**

There is a general recognition across the public sector of the potential to deliver more efficient and effective public services, and bring benefits to society as a whole, through better use and sharing of information. The benefits to society include providing greater citizen convenience, improving opportunities for the most disadvantaged, reducing crime and fraud, and reducing the burden on business. The appropriate sharing of personal information can provide great advantage to individuals who might receive improved public services and to society through more efficient operational processes.

A) The individual can benefit both level through direct experience of better, more personalised services and on a more generic level as a member of the community.

The benefits for local communities and services users include:

- Improved services (eg though seamless links between providers; time savings; services better tailored to individual needs.)
- Reduced requests for the same information.

B) Local Strategic Partnerships (LSPs), partners within a Local Area Agreement, and partnership agencies more generally through sharing information can:

- better understand the needs and opportunities of the local community through a shared evidence base:
- target services and improve service delivery;
- improve performance management through more integrated data;
- gain a greater shared understanding of the local area needs and provide a basis for joint planning;
- foster better partnership working;
- achieve efficiency savings through pooled resources and less duplicated effort; and,
- provide better services and have higher staff satisfaction as results and achievement increase.

**Question 3. What in your view are the key risks of sharing personal information to a) Individuals b) Society ?**

The risks to sharing information can be varied. Often it is assumed that risks only occur when the information is shared. But there are also significant risks when the information is not shared securely or when the information is not shared at all. This is particularly the case in the delivery of public services which are often the only or last form of support to some individuals, particularly those who are vulnerable.

**Question 4. 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?**

The scope and methods which may afford a range of opportunities or risks will vary according to the facts and circumstances of the case, the nature of the information being shared and the purpose for disclosure. These and other factors vary for each and every circumstance and thus giving a generic opinion on scope and method of sharing information is not possible.

**Question 5. 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.**

The Department has no comments on this question.

**Question 6. Provide examples where, in your view, private sector organisations hold too much data or not enough personal information and the reasoning behind your response.**

The Department has no comments on this question.

**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.**

The Department is currently reviewing the sharing of personal and non personal information amongst Local Strategic Partners. To support the sharing of information in a proportionate and appropriate way relevant to the proposed purpose, the Department has commenced work in developing a tool in the form of guidance, to help front line practitioners determine, on a case by case basis, if it is appropriate to share personal information for their specific purposes.

**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.**

The Department is not aware of information sharing taking place within its area of responsibility which should not be taking place. Where we have been asked to share data with other bodies, public or private, we have considered whether this is appropriate on a case by case basis and in some cases declined to share the data. We are aware that much of the data given to us is given voluntarily and this may cease if we do not ensure that it is only used for the purpose it was obtained.

### **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 change you would like to see made, including suggestions for their implementation.**

The DPA puts in place a framework for the protection of personal data, balancing the privacy rights of individuals with the legitimate needs of organisations to make use of such data. It seeks to strike a balance between individual concerns and the common interest. This balance is constantly evolving influenced by circumstances, needs and the changing perspectives of our society. The Act rightly puts into place not only safeguards for the use of individuals information but also a 'checks and balances' approach in requiring vires from additional legislation. The result being; that when information is shared, and is done according to all 8 Data Protection Principles, the benefits of sharing are far more likely to outweigh the possible risks.

However, as the Act is drafted in a way where it is able to adapt to these ever changing needs and requirements which may arise in the protection and use of personal information, it is a complicated piece of legislation. The practical implication therefore, has produced an environment of inconsistent interpretation and implementation of the Act (which is more restrictive than may be necessary) and has created a culture of resistance and uncertainty towards information sharing.

#### 'To share or not to share'

The decision making process required to determine if information can be shared can be onerous and involve complex legal analysis which has led to apprehension of the Act and has arguably had an impact on the delivery of public services. Feedback the Department has received from stakeholders during the development of its information sharing guidance has repeatedly requested greater clarity on what they can and cannot share. Front line practitioners are often looking for clear, unequivocal statements on when they are able to share information no matter the circumstances. However the legal framework rightly does not allow for a simple 'black and white' framework- rather we recognise the need for greater clarification in guidance supported by appropriate training and training materials.

#### Determining 'vires'

It is difficult for public authorities to determine 'lawfulness' in the data protection principles (in particular the 1<sup>st</sup> and 2<sup>nd</sup>). While there has been much debate on the legal theory of 'lawfulness' and to the extent it is informed by Article 8 of ECHR, common law and implied or expressed statutory powers etc- we would like to note from a practical and implementation perspective- that determining vires to meet the 1<sup>st</sup> Data Protection Principle is very difficult for many public sector organisations.

When it is not very clear that such powers exist, for example it is not expressed on the face of statute, advisors become nervous and are likely to be more risk adverse. There is also concern where there is an express power to share for specified purposes, if implied powers may still be considered to share for other purposes which are not specified in the legislation. While it might be appropriate to rely on implied powers in some circumstances to share

information, the practical applications may not reflect this. Relying on implied powers can mean relying on possibly ambiguous statute which derives a range of legal opinions and creates a higher risk to sharing information legally within the DPA framework.

There is evidence to suggest how the law in theory can be applied is not the same as how the law is actually being applied. CLG believes it would be to the benefit of local service providers and public sector bodies to address this issue and this has resulted in the Department developing tools and guidance to help front line practitioners make decisions on sharing personal data. These tools are currently being finalised and should be published later this year.

**Question 10. In your view, how well do public authorities and private organisation 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.**

The Department has no comments on this question.

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

There are a number of cultural and institutional barriers which exist and can limit the public sector's ability to deliver the benefits properly. Barriers are generally characterised as institutional or cultural, legal, financial and in some, cases technological. Examples of these include;

- a lack of clarity and formal arrangements for information sharing
- difficulties in sharing and comparing data across geographical and other institutional boundaries
- lack of knowledge of or confidence in data standards and protocols, which facilitate sharing;
- Lack of awareness of the common objective or local goals preventing effective partnership working; and
- Incompatible or insecure IT systems, particularly systems which pre-date the Internet era.

The barriers provide a significant risk that the desired benefits may not be achieved either for the individual or for society.

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

The Department has no comments on this question.

**Question 13. Are there any other aspects of the UK or EU law that impact positively or negatively on data sharing or data protection? Please provide examples.**

The Department has no comments on this question.

**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?**

The Department reiterates the comments outlined in the response to Question 9 regarding the unrealised potential for better service delivery which comes from the legal uncertainty of implied powers and the inherent risks for statutory authorities in relying on them. The Department does not believe a statutory power will enable 'more secure' sharing. A statutory power will enable the sharing of personal information for a specified purpose; secure sharing, or ensuring that the assurance standards are being met, can be enabled through standards, protocols, codes of practice and training and support.

**Question 15. Are there any parts of the legal framework that places an unreasonable burden on business? Please provide examples.**

The Department has no comments on this question.

#### **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.**

The Department addresses consent, transparency and the public interest in the detail within its guidance tools for front line practitioners. Balancing an individuals' right to privacy against the public interest and the reasonable expectation of the individual involved is a difficult decision for frontline service delivery staff. Whether information could be confidential because individuals would not reasonably expect it would be shared can be less straightforward to determine.

Providing fair processing notices to individuals setting out how information will be shared will help ensure that all the parties understand how information will be used and shared and that no breach of confidence occurs.

While the Department encourages and recognises it is good practice to seek consent where possible and appropriate- there are some cases where consent is not required. We will discuss these examples in our guidance tools and where possible provide exemplars to show the balance of consideration needed by practitioners when making their decision.

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

See Question 16

Question 18. **Do you have any suggestions on how to make the sharing of information more transparent?**

The Department has no comments on this question.

Question 19. **How can we best ensure that information sharing policy is developed in a way that ensures proper transparency, scrutiny and accountability?**

The Department has no comments on this question.

### **Section 5: Technology**

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

ICT can help to transform services at the customer interface and within the back-office. It can lead to better co-ordination of services between the many different agencies that those with complex needs typically have to deal with. There are good examples of **Service Transformation** where disadvantaged people have been the main beneficiaries, such as single electronic benefit assessments and *virtual viewings* of social housing by prospective tenants.

The sharing of personal information between agencies enables the coordination of efforts and better targeting of support to the most disadvantaged around their unique, individual needs. There are some good examples, such as NOTIFY — a system that enables London boroughs to share information on homeless families and individuals living in temporary accommodation in London, in order to improve service delivery.

**Operational Data Sharing** can support ‘passporting’ where an application for one form of benefit results in an automatic entitlement to another. *Government Connect* delivers tools to enable local authorities to share information securely. It will also enable data sharing between central and local government.

Giving frontline staff and service designers the level of support and tools they need is an important enabler to transforming services for the disadvantaged. ICT can **Support Frontline Staff** in focussing less on administration and more on rewarding, value added work with clients. For example, mobile working technologies are particularly effective at cutting administration; they enable remote access to case management systems, mobile incident reporting and work scheduling on the move. Examples include the use of digital pen and paper in Leeds to provide benefit application services in people’s homes and the *Responsive Repairs* project in Harlow for the mobile scheduling of maintenance work in social housing.

ITC is also important to support **service designers**. There are many off-the-shelf toolkits for developing services, some of which are particularly relevant to reaching disadvantaged groups such as the *DigiTV* national programme, *NOMAD* for mobile working and *iTEX* for SMS services. *LINK122* is a secure, web-based client recording system which allows an organisation to input and monitor details of clients and the work done with them.

Homelessness agencies are using *LINK* to help ensure that services can be more effectively delivered to clients.

In the push to increase data sharing, care still has to be taken to achieve the right balance with service confidentiality. There are examples where any hint of increased data sharing could impact willingness to access services and run counter to social inclusion policy goals e.g. young people using sexual health services. Clearly, each case needs to be made on its merits by balancing the benefits of information sharing against the potential unintended consequences.

**Question 21. Should the law mandate specific technical safeguards for protecting personal information?**

Safeguards technical or otherwise, should always be proportionate to the nature of the information, its use, the purpose it was collected for and the impact it may have on the individual if it were inappropriately disclosed.

When considering the mandating of standards the size and nature of the data controller (i.e. the organisation) need also be taken into account. For example, while it may be reasonable to mandate a sophisticated technical encryption requirement for the bulk sharing of personal information between larger organisations that handle and deal with significant amounts of information, the same technical applications would not be reasonable for a small voluntary organisation delivering local services within the community. Any law should not be drafted in a 'one size fit all' approach and an enormous amount of consideration should be afforded not just to the size of an organisation, but also whether it be a public, private or third sector entity and the reasonable burden it may place on the organisation and government objectives.

Any law which mandates standards of technical nature would also need to ensure it does not grow out of date as technology changes rapidly.

**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?**

The Department has no comments on this question.

**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?**

The Department has no comments on this question.

**Question 24. Do you have any international examples of good practice in the sharing of personal information that could or should be adopted in the UK?**

The Department has no comments on this question.

**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 case?**

The Department has no comments on this question.

**Question 26. Are you aware of significant differences in public attitudes to the sharing or personal information in other countries? Please provide examples and an explanation for why you believe this to be the case.**

The Department has no comments on this question.