

# 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: Backgrounds

Question 1. Please explain what your interest in information sharing is.

If you have an active involvement in personal information sharing, we would be grateful for the following information:

- What kinds of personal information do you collect, hold and share?
- How do you collect, hold and share such personal information?
- For what purposes do you collect, hold and share such personal information?

Comments:

The National Archives is a non-ministerial government department and executive agency reporting to the Lord Chancellor and Secretary of State for Justice. It has the policy lead on information management across government and on the re-use of public sector information. It is also the UK government's official archive, bringing together the Public Records Office, Historical Manuscripts Commission, the Office of Public Sector Information and Her Majesty's Stationery Office.

Our interest in information sharing reflects this remit. We are interested in the information management implications and in sharing as it bears on re-use and on archives. We hold the types of personal information most organisations hold – employee information, customer information etc. We also hold personal information specific to our functions, in particular in the archives, in catalogues and in licences.

Our responses to this consultation are also informed by our membership of the Information Assurance Group run by the Ministry of Justice that has been considering how the barriers to information sharing across the public sector can –be tackled, and by our support for the Knowledge Council, which is Government’s lead group of officials in Information Management across Government.

**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 and b) society? Please provide examples.

Comments:

The main benefits to individuals of sharing personal information are the improvements that can be made to service delivery. There are two main ways on which this is done – through analysis and research using personal data, or through sharing individuals’ personal data for the delivery of services to that individual.

We live in a society where sharing of individuals’ data for service provision is routine in services we encounter daily. Individuals can use multiple cash-points, gain credit in different shops, and renew insurance and car tax online as a result of this sharing. However, the key to success is that citizens perceive that the benefits of sharing outweigh the risks. We accept data sharing where it simplifies our lives – but expect to have a degree of protection as a result.

For society, there is also benefit in the sharing of personal data (often anonymised) for wider research and hence longer-term social benefits. Drugs trials, marketing segmentation and policy research can all benefit significantly from analysing patterns – which rely upon understanding what people did.

There are also circumstances where we expect individuals’ data to be shared for wider social benefit – e.g. details of offenders passed between certain parts of the judicial system and employment bodies to avoid sex offenders’ employment in schools). Here, the consequence of not sharing can be severe.

At the heart of both of these examples is the element of trust, and of the trade off between benefits and costs. We want simpler lives – and so are aware that data is being shared behind the scenes. We don’t ask questions if it goes right, but when it goes wrong there is far more concern about the justification for sharing. Sharing of data cannot be seen as an inherent good in its own right – it is a tool for delivering benefits, and needs to be done in the context of balancing risk and reward.

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

Comments:

The key risks of data sharing have been illustrated by the recent events in Government. Loss of data can cause major problems, ranging from inconvenience through to major

disruption to lives (or in the case of the sharing of very sensitive information, potential endangerment to lives).

However, this debate is not as simple as has often been portrayed. In the case of information not being shared which should have been (e.g. details of certain types of offenders between law enforcement agencies) the risk is to others who may be at risk as a result. Furthermore, individuals also have a responsibility. We are well appraised of this responsibility in our dealings with financial institutions, for example (by not disclosing our PIN numbers, and ensuring that our use of cash machines is not overlooked), but this responsibility is often not mentioned in the context of our dealings with the public sector.

At the heart of this question is the word 'risks'. Risks are not inevitabilities, but can be managed. All activities carry risks, and technological and social development requires us to manage those risks effectively. Unfortunately, whilst the management of financial and environmental (health and safety, asbestos etc) risks are well developed, the management of information risks is relatively new to business, both public and private. Risks must not be seen as inevitabilities, but as risks – and so there needs to be greater focus on the management of those risks where the benefit of sharing information is clearly worth it.

Question 4. As mentioned in the introduction, 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? Please explain your reasoning behind your response.

Comments:

One of the challenges of the information sharing debate is that data sharing is often seen as the issue in its own right. It's not. Information should only be shared where there is a strong rationale to do so, and potential or proven benefit, given the inherent risks. In recent years, government departments have relied on statutory legislative gateways that clearly set out the type of data that can be shared, to what purpose it can be used for and which bodies can receive it. This approach has provided departments and agencies with a degree of clarity and certainty on what is permitted. The main disadvantage with this approach is that the statutory powers are usually narrowly defined with little room for them to allow data sharing for purposes other than which is explicitly stated, and with the desire to transform services rapidly, and with fast developing technology, this is effectively setting limits on service transformation. Furthermore, it is (wrongly) focusing the debate on the activity of 'sharing' rather than the business purpose of the sharing, and the required subsequent debate about risk.

There is no one answer to 'how to share', and technology moves fast. In the current environment, where risks are apparent and high profile, the concept of standardising ways of sharing information appears attractive. However, we'd urge that you resist the desire to standardise too much. Information is shared in many different ways, with new technological options appearing regularly. Rather than standardising the 'how' approaches should, instead, focus on some of the principles of information sharing, with standards, guidance and stronger risk management.

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:

The National Archives is not in a position to provide examples.

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:

The National Archives is not in a position to provide examples.

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.

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:

Other bodies will provide examples. Examples experienced on a personal level with the public sector include the contrast between renewing car parking permits with a local authority vs. DVLA's new approach. The DVLA car tax renewal no longer requires multiple forms of documentation to be shown as the evidence is, instead, provided by data sharing from insurance and other bodies. In contrast, renewing a local car parking permit took 30 minutes to locate paperwork, and a journey to a local office to show it to an official. Here, data sharing would have saved thousands of individuals a lot of time.

We do have a strong awareness of the barriers through our work advising and supporting other Departments. There is a lack of clarity in many departments of how sharing can best be done under data protection legislation, and many myths surrounding the 'rules' and processes. Furthermore, there are often financial inequalities in the sharing of data – i.e. the body that makes the benefit is often not the body incurring the cost of supplying data. However, as big a factor is culture, and perception of risk.

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 National Archives not aware of any such examples.

### **Section 3: The legal framework**

Question 9. In your view, how well does the Data Protection Act 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:

The main weakness of the Data Protection Act is its complexity - it can be difficult to understand. There are many myths surrounding the DPA – it appears to be one of the most frequently cited yet least understood pieces of legislation. There are also many areas of

uncertainty, for example determining what is personal data and therefore within scope of the Act. A priority here would appear to be clearer guidance on what DPA means in practice, and clearer advice on DPA's implementation. All of this needs to, critically, be underpinned by strong training, and by embedding management of DPA into organisational governance.

The DPA is also frequently seen to contradict, or question, other pieces of information legislation. We have heard of examples where the DPA is used to dispose of records which the FOI and Public Records Act would mandate are retained. Clearer guidance on the cross-management of these pieces of legislation is also important. Related to this, there is a particular issue for archival bodies, or bodies holding historical information on individuals, when handling subject access requests. A search relating to an individual person usually requires an extensive search of the records that can take up a considerable amount of staff time. The fixed fee of £10, which applies to all bodies, does not take into account the fact archives are likely to hold more records that need to be searched compared to others. This is in contrast with the position under the Freedom of Information Act where it is recognised that it is reasonable to charge a research fee when enquiries have an opportunity to conduct their own research.

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

Comments:

The National Archives agrees that the second principle is important is that it provides protection against use of personal information provided for a purpose that would not be expected – or agreed to – by the data subject. It also, however, contains scope for an organisation to proceed with further use of the data that is different but nonetheless compatible, which we have found useful. The requirement in the first principle to be fair provides continued protection of the interests of the data subject.

The National Archives is not aware of other bodies ignoring this principle.

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

Comments:

The key barrier is lack of guidance on the how the Act should operate, and how it should relate to other related legislation. This leads to unrealistic expectations on the part of individuals as well as misplaced over-protection by organisations, of which there have been well-publicised examples (Soham, British Gas).

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

Comments:

There is a tension here between enforcement and persuasion. Our experience is that the biggest issues with DPA are not the legislation, but guidance on how it should be used, and lack of embedding of the risk management in organisational governance.

The National Archives supports the provision of increased powers to the Information Commissioner, for example to conduct an assessment without consent. We note that the Regulatory Enforcement and Sanctions Bill currently going through Parliament could offer an

alternative approach to dealing with compliance failures, such as enforceable undertakings. However, we don't believe that this is sufficient.

To really embed DPA, we need a greater focus on information management governance at Board level, with Information Risk management embedded in organisations. This is more likely to be achieved through 'softer' factors, such as well written guidance, training on information risk management embedded in mainstream training programmes and training for Accounting Officers, and a strong role for Audit Committees in managing information risk.

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?

Comments:

Many individual pieces of legislation make sharing difficult because they provide for information to be provided for specified purposes and give undertakings that the information will not be used for different purposes. This can be a direct impediment to information sharing.

Question 14. Are there any statutory powers unavailable that would enable better or 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?

Comments:

The National Archives has no specific suggestions to offer.

Question 15. Are there any parts of the legal framework that place an unreasonable burden on business?

Comments:

Not in our experience.

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

Comments:

The National Archives understands consent to be *one option* for the processing of personal data under Schedules 2 and 3. However, it is not clear at all whether consent needs to be explicitly obtained, and this area needs clarification. For example, when looking at sharing of personal information between services for the protection of wider society, consent requirements would be actively dangerous. There has been a lot of confusion recently in both the public and private sectors on what information can and should be retained, and can/should be shared.

We do need clarity on this question, both for the public and for organisations operating in this space. The answer to this question is not a simple one.

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

Comments:

One barrier would be volume - the sheer number of people to be contacted for consent. Another would be data quality problems. We are aware from our own internal systems that inconsistent details can be provided over time and clean-up exercises can be needed in order to ensure the most up-to-date contact details are used.

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 organisation be expected to do more to explain their use and sharing of personal information to the public? And if so, how?

Comments:

The issue of transparency is key. There are various options here, including a requirement on organisations to be explicit on what information they are holding, in a standard format.

Another option would be for personal data processing notifications to ICO to be more explicit on specific data sharing exercises. However, to achieve this it might be necessary to restructure the way in which notification details are provided and held. Individuals already have strong access rights and a subject access request should elicit details of current information sharing at least – as long as it is authorised and takes place in a properly documented way.

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:

In your view, how valuable is the Information Commissioner's recently published Framework code of practice for sharing personal information?

In your view, how valuable are privacy impact assessments along the lines announced by the Information Commissioner on 11 December/

Comments:

Despite its perceived complexity, we believe that the Data Protection Act is fit for purpose and is not a barrier to effective and secure information sharing. What is required is a wider and more detailed range of guidance documents and support from both Government and the ICO to assist organisations to help interpret the Act. The recent initiatives from the ICO are therefore welcome.

The recent ICO framework code of practice is valuable tool to assist bodies taking forward data sharing initiatives and we also believe that Privacy Impact Assessments are a valuable tool for determining whether a particular information sharing initiative should go ahead and, if so, on what basis. Public confidence in them would benefit from routine release of details of any PIAs carried out by an organisation.

## **Section 5: Technology**

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

Comments:

Technological advances have changed the approach to data sharing completely. Storage and processing capacity has increased to the extent that major exercises can be conducted very quickly. This makes information sharing more feasible for small organisations in particular. In addition, users expect to complete transactions online rapidly – and, in practice, this can be impossible without data sharing.

However, the development of Information Risk management, and the governance required to oversee this approach, have (perhaps inevitably) lagged behind the technical possibilities. In our view, the focus should not be on the technology, but on the risk management and governance required to respond to new technological options and assess them quickly for their acceptability, business benefit and risk.

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:

The National Archives does not believe that the law should mandate specific technical safeguards. Technology changes more rapidly than legislation and such law would be out of date very quickly. It would be preferable to enshrine principles and provide a framework with safeguards that can be applied whatever technology is currently in use.

Question 22. How, in your view, could 'privacy enhancing techniques', such as the anonymisation of 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:

Anonymisation is a crucial enabler for information sharing. However, it must be possible to show by positive tests that the information is genuinely anonymised and the individuals cannot be identified.

## **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?

Comments:

The National Archives is not sufficiently familiar with the regimes in other jurisdictions to offer any comments on this.

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:

The National Archives is not sufficiently familiar with the regimes in other jurisdictions to offer any comments on this.

Question 25. Do you have any knowledge of jurisdictions that have adopted a particularly permissive or restrictive approach to sharing personal information? What have consequences of this been?

Comments:

The National Archives is not sufficiently familiar with the regimes in other jurisdictions to offer any comments on this.

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:

The National Archives is not sufficiently familiar with the regimes in other jurisdictions to offer any comments on this.

### **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?

Comments:

The issue of personal information sharing and protection does not operate in a vacuum. We would urge that this review takes place in the broader context of information management and the management of information risk. One of the challenges we currently face is that Governance structures are not as familiar with the issues around information management and risk as they are around, say, financial or environmental risk. We believe that Boards need to address these issues actively, and do so around the whole concept of information risk. Therefore, we believe that management of personal information would be strengthened if it could be positioned in this context.

We also urge that this review doesn't just look at today's issues, but also tomorrow's. Technology, service design and customer needs are all changing very fast. It's a certainty that the issues being faced today are different from those we will face in 5-10 years. We need the recommendations of this review to be 'future proofed' for tomorrow's challenges as well as today's.

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

Comments:

See answer to Question 27.