

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

Responses to Questions for Consultation

Section 1: Background

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?*

The Ministry of Justice is responsible for UK policy on data protection and data sharing, and represents the UK in European data protection negotiations.

There is no single source of law that regulates the powers that a public body has to use and share personal information. The collection, use and disclosure of personal information are governed by a number of different areas of law. In domestic law, these include:

- the law that governs the actions of public bodies (administrative law)
- the Human Rights Act 1998 (HRA) and the European Convention on Human Rights (ECHR)
- the common law tort of breach of confidence
- the Data Protection Act 1998 (DPA)

The Ministry of Justice holds a broad range of information on citizens or residents of the United Kingdom. Information gathered by the Ministry falls out of the requirement to perform its statutory functions and duties.

The information the Ministry gathers includes sensitive data relating to people charged with offences, and/or convicted offenders, and also includes a wide range of personal information about citizens or residents to support its constitutional and judicial responsibilities.

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.

Government is committed to ensuring that information sharing and data protection is undertaken in a secure manner, recognising that legal and process controls must be in place to ensure that information is not shared inappropriately or disproportionately.

From the Ministry of Justice's perspective, some of the key benefits of sharing personal information for individuals are:

- More effective individual risk management of offenders through cross-organisational boundary information management.
- Reduction of re-offending behaviour on an individual level, and better protection for victims and witnesses
- More effective intervention assessments, and multi-agency arrangements for an individual

From the Ministry of Justice's perspective, some of the key benefits of sharing personal information for society are:

- Improved intelligence for security matters.
- Co-ordination of resources through releases of prisoners with the Police, Probation, etc.
- Partial identity management through the use of databases held by Prison services, Police, etc.
- Reducing re-offending through effective partnerships with other Criminal Justice Organisations and Non-Governmental Organisations.
- Reduced re-offending rates.
- Effective resource planning and obtaining best value for inputted resources, for example, in National Offender Management Systems not having to do the same interventions again.
- Better communication for other Criminal Justice Organisation objectives such as Department of Work and Pension payments for prisoners released.

Question 3

What in your view are the key risks of sharing personal information to:

a) individuals; and

b) society?

Please provide examples.

Once information has been collected, the Government is very careful in ensuring that sharing can only take place when it is not incompatible with the original purpose of collection. This is an important protection in the Data Protection Act and the EC Directive which the DPA implements. The public needs to be satisfied that a proper balance is maintained between the benefits of sharing information and the right to privacy.

From the Ministry of Justice's perspective, possible risks of sharing information to individuals are:

- Poor identity management
- Poor controls of access to information pools – having disparate systems of personal data without clear information protocols for sharing.
- Inaccurate data and the need to control and maintain accuracy

From the Ministry of Justice's perspective, possible risks of sharing information to society are:

- Poor quality data shared, or inadequate sharing, leads to public mistrust of regulation and institutions.

The Ministry of Justice has a central role in providing advice on policy and legislative proposals which engage on data protection and data sharing, and ensuring that all parts of Government apply the legal framework in a consistent manner.

Section 3: The legal framework

The Data Protection Act (DPA) regulates the processing of information, including its obtaining, holding, use and disclosure.

The second principle of the DPA is as follows:

“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 purpose or those purposes.”

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.

The DPA regulates the collection, use, storage and distribution of personal data. It is underpinned by the framework of the ECHR, particularly the right to a private and family life under Article 8, which is now part of domestic law by virtue of the HRA. Neither the HRA nor the ECHR prevents the lawful and proportionate sharing of data. Where confidential information is concerned, at common law or where there is a statutory discretion to disclose, it is only possible to share information where it is in the public interest to do so. Ministers of the Crown may also be able to rely on common law or prerogative powers to share information. However, where there is a relevant statutory provision this may operate so as to exclude these common law or prerogative powers.

The DPA provides a framework for the lawful processing of personal data. Organisations and individuals must comply with the data protection principles in order to process personal data unless an exemption applies. These principles include ensuring that data processing is fair and lawful, that data are processed only for specified and lawful purposes and that data are accurate. Additionally the processing has to meet certain statutory conditions. In many of these conditions it is a requirement that processing be “necessary” for a particular function or purpose, e.g. for the performance of a contract or to protect the vital interests of the subject. Where sensitive personal data is involved, such as data related to political opinions or health, the processing must also meet a further set of conditions, e.g. that the processing is necessary for the administration of justice or for medical purposes.

Question 12

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

Government is committed to ensuring that information sharing and data protection is undertaken in a secure manner.

In November 2007 the Government also announced a review of data handling procedures within Government (refer to the Cabinet Office report on Data Handling Procedures in Government: Interim Progress Report, paras 44-46 on the Cabinet Office website http://www.cabinetoffice.gov.uk/reports/data_handling.aspx). This review recommends enhancing the Information Commissioners' ability to provide external scrutiny of data protection arrangements. The Ministry of Justice is currently preparing a consultation document due for publication in the next couple of months.

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.

The Data Protection Act 1998 implements into UK law EU Directive 95/46/EC. The Ministry of Justice believes the Directive was a landmark piece of legislation in the field of data protection, that it has led to significant improvements in the standard of safeguards offered by all Member States. There have been a number of other pieces of European law in the field of data protection that the UK believes have impacted positively on data sharing and protection. Most recently, the Data Protection Framework Decision will, if adopted, seek to ensure common standards of data protection for personal data exchanged between Member States in the field of law enforcement. We welcome this proposal.

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

One of the conditions for processing is that the data subject has given his consent to the processing. However, consent is not defined in the Act. The existence or validity of consent will need to be assessed in the light of the facts. To assist in understanding what may or may not amount to consent in any particular case, it is helpful to refer back to the Directive. This defines "the data subject's consent" as: "any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed."

Section 5: Technology**Question 20**

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

The social and technological advancements of recent years have given citizens greater expectations and opportunities than ever before. They can expect tailored services from the private sector as well as personalised services from government agencies. In order to achieve this the effective and proper use of personal information is needed.

Citizens rightly expect that when providing personal information to facilitate the delivery of modern public services and to ensure public safety, that their personal data is secured properly and used appropriately. For example they should expect to see greater individual security through the reduction in crime without unnecessary impingement on their individual privacy or freedoms. The Government's aim is to make sure that information is only shared when there is a benefit to the public and that any information sharing is lawful.

Responsible information sharing ensures that citizens have a say in how their personal information is shared among service providers. Efficient use of this information will, for example, avoid citizens having to give repeatedly the same information to a range of service providers.