

# 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.

Comments:

We are responding on behalf of the Northern Ireland Civil Service, which is composed of eleven Departments. All Departments hold personal information about its employees and also the citizens that they serve.

Details of the type of personal information our Departments collect, hold and process are available on the Information Commissioner's Data Protection Register, which is published on his Office's website: [www.ico.gov.uk](http://www.ico.gov.uk)

As an example, the Office of the First Minister and Deputy First Minister processes personal data for eight purposes: Staff Administration; Advertising, Marketing & Public Relations; Accounts & Records; Benefits, Grants and Loans Administration; Crime Prevention and Prosecution of Offenders; Education; Information and Databank Administration; and Research.

The level and frequency of the sharing of personal data held by our Departments is determined by business need, and carried out in accordance with our legal obligations.

We should also point out that the Northern Ireland Departments are connected to the

Government Secure Intranet (GSI), which is commonly used as a secure method of transmitting data between each of them.

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

### Question 2.

Comments: There are potentially many advantages for the public sector in a joined-up approach enabled by data sharing. In theory, at least, this approach should result in major efficiencies and reduction of fraud. From a citizen perspective, such an approach should release more funding and resources to the 'front-line' to deliver a better, cheaper, faster and more personalised service. In practical terms, we believe that the key benefits of sharing personal information to (a) individuals, as including: savings in time by having a single point of contact for updates due to life events, eg, change of address – extended into 24/7 web services, contact centres, walk-in 'one-stop shops'; cost savings, eg, no need to buy a full birth certificate or get a photograph for a passport application, as these are already in the public domain; improved services – even proactive, eg, car tax reminder on pre-filled form; better information, eg, portal approach with all information on a particular subject area presented seamlessly from a citizen perspective, rather than to suit the public sector; and more accurate information – ability for the individual to see and correct all information held about him/her. The key benefits for (b) society, are a safer and healthier world in terms of terrorism, other crime and the spread of communicable diseases. Reduction in fraud and better targeting of funding also allow for more relevant and balanced policies – localised – due to better and complete information available to policy-makers. And, having the right information available to the right people at the right time should enable us to protect those who are disadvantaged or vulnerable.

### Question 3.

Comments: We recognise that there are disadvantages - real and perceived - in data sharing for the public sector and for the citizen and society in general. Significant resources would have to be made available to put in place the required policies, legislation, regulations, agreements, procedures, mechanisms and technology to permit personal, and sensitive personal, data to be stored, kept up-to-date and shared as required in a secure, legal and timely fashion. And, having applied the necessary resources to these tasks, it would be necessary to sustain them in order to demonstrate to the public that data sharing is necessary and a 'good thing' that will bring tangible benefits to all. From the citizen's point of view, the main disadvantages would be the fear of 'Big Brother' invasiveness, and the loss and/or misuse of personal data. Moreover, in the short to medium term, given the present quality of personal data held, there is a very real risk of mistakes being made when data is merged from different sources - mistakes of this type can have implications for individuals ranging from embarrassment through to financial damage or even

live-threatening consequences, where medical information is involved.

Question 4.

Comments: There are undoubtedly tremendous opportunities to enhance public service delivery and, at the same time, reduce the burden on business. However, many of these opportunities are likely to involve using and sharing personal information beyond the scope for which it was collected originally. It would be too costly and labour intensive - in every case - to draw up the legislation or regulations necessary to make sure such re-use was legal. Therefore, other ways would have to be devised to make such re-use acceptable. Some form of risk assessment might be the answer - perhaps a privacy impact assessment, since it would go further than simply a data protection compliance check. Again, it may not always be feasible to seek the consent of the individuals whose personal data is in the spotlight, therefore it is essential that a sound assessment of the risks of not doing so is carried out. If major public policy initiatives are involved, like the development of ID cards, then public consultations would be appropriate.

Question 5.

Comments: Departments hold too much information in that they tend to duplicate personal information already held. The development and implementation of common IT systems and shared service centres, which form a key element in the Northern Ireland Civil Service Reform programme, should help to reduce, if not eradicate, unnecessary duplication.

Question 6.

Comments: We are not in a position to comment authoritatively.

Question 7.

Comments: For greater use and sharing of personal information to take place, legal certainty needs to be established, so that public bodies can pursue data sharing projects with confidence. Public trust must be earned by means of educational and promotional programmes, egs, leaflets and advertisements. And, major parts of the public sector must become more citizen-centric in approach. There are already examples of the amalgamation of public bodies to deliver better public services, eg, the Land and Property Services Agency.

Question 8.

Comments: We are not aware of any such cases within the Northern Ireland Departments.

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

Question 9.

Comments:

The Second Data Protection Principle (the purpose limitation principle) is probably the best protection that individuals possess against Data Controllers (in this case Departments) that wish to process their personal data in very extensive ways. It prevents them from using, for other purposes, personal data which they originally collected for a specific purpose. The Second Principle has worked well in that it has been a major obstacle to the uncontrolled use and sharing of personal information. However, it has also acted as a barrier to the

development of efficient, joined-up public services within central government and the wider public sector.

The Data Protection Act (DPA) is not a black and white area of law - there are many grey areas. Indeed, many compliance decisions are left to the discretion and subjective opinion of the Data Controller. The provisions of the DPA will not by themselves help Data Controllers make the right decisions. Court decisions and Information Commissioner Tribunal cases will help to inform the process of interpreting the Act but they will not always assist Data Controllers' thinking when dealing with day to day issues and difficulties.

The Information Commissioner has produced some useful Codes of Practice and a number of helpful guidance documents but a good deal more ground needs to be covered. In terms of the use and sharing of personal information, Departments are not always clear about whether a particular data share is, or is not, lawful. They are left to grapple with these issues and to decide whether or not it is worthwhile obtaining a legal opinion. The costs involved in assessing whether a particular data share is a viable business option does not encourage Departments to pursue the 'transformational government' vision.

If data sharing is to 'take root', then DPA will need to be amended or new enabling legislation introduced. These legislative changes would need to be supported by Codes of Practice and/or detailed guidance. It is difficult to judge just how extensive the legislative changes need to be and it may be that the necessary changes cannot be accomplished through national legislation alone - a further European Directive may be required.

Question 10.

Comments:

Departments are very conscious of the Second Principle and there is a strong adherence to it. The Second Principle is valuable in that it forces Departments to consider, and give due weight to, the citizen's position.

Question 11.

Comments:

The Data Protection Act is seen as a difficult and complex piece of legislation. Attempts to de-mystify its provisions have had limited success. The refusal to make personal information available in some high profile cases, eg, the Soham Murders, demonstrates this assertion. Public bodies are generally not comfortable with the Act and are reluctant to pursue goals which involve an interpretation of the Act. Furthermore, public bodies tend to be structured on a functional basis - in most cases for the benefit of the organisation rather than the individual citizen - and consider the personal data they hold to be their's alone.

Electronic matching of historical personal data requires certainty, or at least a very high degree of confidence, that two or more records relate to the same individual. While there are several national identifiers (eg, national insurance number) that can help with matching, the use of these can still pose practical difficulties and, in any case, most public bodies use their own identifiers. There are no universal data standards across public sector systems to facilitate data matching and sharing, eg, each public body's database can have different storage and validation rules around something as basic as a person's name. A substantial amount of work is required in this area to facilitate wider data sharing. And, in many cases, mechanisms will need to be put in place to obtain the consent of individuals to share their data. The burden and cost of this for the public sector would be substantial and may well

cancel out the efficiency gains.

Question 12.

Comments:

More investigative and enforcement powers for the Information Commissioner should be considered. And, perhaps additional and dedicated resources should be channelled into his Office's work on the area of data sharing. Moreover, it may be necessary to consider the establishment of a specific regulator, who would oversee major data sharing programmes or projects.

Further and more stringent penalties may be necessary to ensure that the attention of Data Controllers, and individuals who are accountable, is focussed firmly on the safeguarding of personal information.

Question 13.

Comments: We would only observe that the European Directive on Data Protection (95/46/EC) has been implemented in various ways by the various Member States, and that diverse interpretations and practices can lead to difficulties when sharing information outside national boundaries.

Question 14.

Comments: The introduction of statutory powers which would require public authorities to install systems that would facilitate and manage identity authentication would be worth considering. Such systems would allow more employees to work from home more easily, and promote flexible working in a secure and controlled environment.

Question 15.

Comments: See responses to Questions 4 and 11 as regards the burden of obtaining the consent of individuals for the use and sharing of their personal information.

#### **Section 4: Consent and transparency**

Question 16.

Comments: Our Departments are not always clear about whether and when to seek individual's consent to share information about them. Unless clear precedents have been set, Departments are inclined to use their discretion in deciding whether to approach individuals for their consent in sharing personal information. If Departments are reasonably confident that consent will be forthcoming, then they will make an approach; if they are not confident, then they tend not to take any action. Further guidance, perhaps in the form of a Code of Practice, would be of benefit to our Departments.

Question 17.

Comments: Lack of administrative and financial resources present a considerable barrier to obtaining consent from individuals on a routine basis. Further and more detailed guidance is required from the Information Commissioner to enable Departments to identify cases where consent can be assumed.

Question 18.

Comments: It will be incumbent on our Departments to communicate more with the public and explain why and how their personal information is to be handled and shared, especially in the light of the recent and various high profile losses of personal data. We would use public consultations as a principal means of communication, though greater use of websites and leaflets would also help us get our message across. The inclusion of material about information sharing in Departmental Publication Schemes would be another means of making more transparent our activities on this front.

Question 19.

Comments:

There has been an increasing demand for policy development and advice by the NI Civil Service following devolution, and civil servants at all levels have expressed the need for more guidance on the policy development process generally. The model and process of devolved government are unique, and the policy development process is highly inclusive and transparent. There is also now much more public debate than in the past about policy issues for which the devolved administration is responsible. We believe that the use and sharing of personal information should not be seen as the preserve of a few specialists. Those involved at the 'front line' of service delivery have a vital role in helping to gauge what is deliverable. They have a keen awareness of what really matters to the citizen. Therefore, we are keen to contribute to and avail of means such as training sessions and guidance to engage with those familiar with delivery issues. Of course, this is an increasingly resource-intensive process and our ability to pursue our aims and objectives will always be subject to various constraints.

While our Departments have generally not employed Privacy Impact Assessments (PIAs) in their policy initiatives to date, we would encourage and support their use in cases where the use and sharing of personal information is involved. It makes sense identifying privacy concerns at the early stage of an initiative, so that these can be addressed and safeguards built in, rather than added later at greater cost to the public purse. We hope to learn more about the use of privacy impact assessments and about the lessons learned by public authorities that have used them. And, we would encourage the Information Commissioner to continue his promotion of PIAs by means of seminars, workshops, etc.

One of our Departments, Finance and Personnel, has carried out a PIA. See link for further details: [http://www.ratingreviewni.gov.uk/privacy\\_impact\\_assessment.pdf](http://www.ratingreviewni.gov.uk/privacy_impact_assessment.pdf)

The Information Commissioner's recently published Framework Code of Practice for sharing personal information is, in our view, a very useful document. It sets out in plain English how public bodies can help themselves in developing consistent standards, and informs staff so that they are better placed to make well-informed decisions. Documents like this help and encourage public bodies to adopt and follow good practice in the use and sharing of personal information. This, in turn, engenders public trust and enhances corporate reputation.

We believe that it is important for the Information Commissioner to be able to contribute to

new initiatives involving the use and sharing of personal information to ensure that data protection implications are considered and compliance measures are built into schemes from an early stage in order to avoid any data protection non-compliance issues once the schemes are implemented. Indeed, we would consider inviting the Commissioner's Office to be represented on Departmental/cross-Departmental project/programme Boards, where personal information/data sharing issues are likely to be of central importance.

## **Section 5: Technology**

### Question 20.

Comments: Processes and procedures concerned with the handling of personal information have not kept pace with rapid technological advances that have taken place. We believe that it is essential to have appropriate controls in place - changes in the use and sharing of personal information should not be driven solely by technology. Through extensive engagement with the public, central government needs to put regulatory and governance frameworks in place that minimise and manage the risks, while ensuring that the benefits are delivered. Without this intervention, the risks will not be controlled but nor will the potential benefits be realised.

### Question 21.

Comments: We would support the Information Commissioner's view that sensitive personal information should be protected using approved encryption software, and that portable devices (eg, laptops) used to store and transmit personal information, the loss of which could cause damage or distress to individuals, should be protected using approved encryption software which is designed to guard against the compromise of information.

### Question 22.

Comments:  
'Privacy enhancing techniques' such as encryption are well known and understood within the Northern Ireland Departments. Indeed, options for encryption of laptops and removable media are being explored presently. However, the use of 'anonymisation' or 'pseudonymisation' would not be prevalent. Staff would need access to detailed guidance and instruction on the use of these less well known techniques, so that they would possess the confidence needed to employ them successfully.

## **Section 6: International comparisons**

### Question 23.

Comments: We are not in a position to comment authoritatively.

### Question 24.

Comments: We are not in a position to comment authoritatively.

### Question 25.

Comments: We are not in a position to comment authoritatively.

Question 26.

Comments: We are not in a position to comment authoritatively.

**Section 7: Additional questions**

Question 27.

Comments: We have no further comments.

Question 28.

Comments: We believe that the Information Commissioner could usefully compile a glossary of terms that are commonly used when the subject of data sharing is discussed. Standardisation of meanings would bring clarity to proceedings and empower staff to a greater degree. On occasion, we have found that confusion or misunderstandings can arise when terms such as 'data sharing' and data transfer' are used.