

Consultation on the use of personal information

This is a reply to your consultation on behalf of the Department for Work and Pensions. It uses the structure in the consultation document and addresses those questions appropriate to DWP in, we trust, a helpful way.

Question 1

Please explain what your interest in information sharing is.

It is probably not entirely necessary to rehearse DWP's position in relation to personal information. However, by way of introduction to this response, a summary may be helpful.

The Department is one of the largest Data custodians in Europe, and treats the security of the personal information it holds very seriously. We are responsible for approximately 73 million customer records and have staff of around 100,000, the majority of whom are front-line staff processing personal information. The Department has several different business involved with benefit and pension payment, employment and training provision, and child support.

The information held about individuals will depend on their business with the Department. The information requirements are almost exclusively laid out in legislation. The primary source of information held, is, of course, the customers themselves. However, information may be supplied from other sources such as employers and financial institutions. Such supply is only when allowed by law and is relevant and proportionate to DWP business.

Information is stored on a number of IT systems relevant to the individual businesses. There is also the overarching Customer Information System. Paper records are also held where relevant. Needless to say, all of this record keeping is done in the context of a comprehensive document retention policy.

It will be understood that such a base of personal information lends itself to a potential host of data sharing possibilities. Some of these are for purposes directly or closely related to the Department's business such as sharing with local authorities for the purposes of housing benefit and sharing with HMRC for both departments' purposes. However, some of the data sharing, both in place and potential, are for public sector purposes outside the Department's immediate business. Examples are Her Majesty's Court Service using DWP data for tracing fine defaulters; the Legal Services Commission administering legal aid; and the Department for Children, Schools and Families administering free school meals. In the last year we have developed a data share with a private sector partner, British Telecom, to facilitate the administration of their social telephony scheme.

In every instance, the data share only involves information relevant to the purpose in question, starting from a simple yes/no confirmation of a customer's declaration that they receive a particular benefit. In some instances, the other organisation is given limited search facilities. It is the Department's policy that any form of direct access to information must be covered by a specific statutory gateway. This will be returned to in a later section.

Scope of personal information sharing (Qs 2 – 8)

Question 2

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

Delivering better services that will increasingly be less tied to specific organisations. They will become more devolved, localised and work as partnerships – as well as serving new agendas that respect choice and personalisation in how and when citizens access services. E.g. data sharing allows confirmation that benefit customers are entitled to free prescriptions, free school meals etc. In addition, for both organisations and individuals there can be greater efficiency savings and consistency for example, the 'Tell Us Once' project for dealing with changes in circumstances, who have contacted your review separately.

Creating better policy that relies more on understanding the complexity of people's lives and how public policy interventions can both create and respond to opportunity and need. This requires greater integration of information and capability to analyse and evaluate the insight provided by that information.

Improving performance and outcome measurement – as policy and delivery changes, so will performance and outcome measurement. Services tailored to the citizen need to tell the story of success – or otherwise – through the eyes of the recipient, not the service provider.

Providing stronger assurance – changing the way services are delivered will begin to erode conventional organisational boundaries, and so the need to provide assurance of success and propriety cannot be limited by who collects or holds key information. E.g. reduced fraud and error by identifying people working and claiming DWP benefits. Better information about the population allows analysis and research to be done which inform policy development.

Question 3

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

The risks involved with any data sharing are well known and are managed by the Department through various means.

The risk of loss of data is managed by extensive security measures, all of which have been re-appraised in recent months. The Department's policies relating to information security support and reinforce its responsibilities under the DPA. These have been developed by the Department's Security Team who work closely with DPA policy colleagues. The Department's IT systems comply with a range of recognised security standards. The Department's agencies endeavour to reduce the risk of unlawful procurement offences, by for example, reporting instances of bogus contacts, which are in turn disclosed to the Information Commissioner's Regulatory Action Division

The wider issue of staff being properly equipped for the correct handling of personal information is managed through the Department's induction process; extensive guidance on the Department's intranet, including interactive training material; good performance management; and through internal audit arrangements. Extensive support is available to staff from a national network of data protection officers and a specialist advice and guidance team, the staff and management of which are ISEB qualified.

New data shares are managed through a central specialist Data Sharing Strategy Unit. The unit has developed a protocol which guides departmental sponsors of new data shares through the steps to ensure its legality and soundness. The protocol ensures similar processes to those of a Privacy Impact Assessment. Following the publication of the ICO's PIA handbook last December further thought is being put to the development of the processes.

All of the above are supported by a specialist data protection policy team, brigaded with FOI, who advise on DPA compliance and the various specific legislation on the sharing of DWP data. They are supported by specialist lawyers.

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 the reasoning behind your response.

Bulk data sharing offers great opportunities for Government to reduce administrative burdens, the cost and complexity of administration, and to provide a better, more joined-up service for customers. The rapid advances in computer technology have meant that electronic data matching is becoming increasingly sophisticated. Using computers to compare large collections of information about our customers, often provided to different organisations for different reasons, is now an important tool.

For example, the Department carries out large scale data matches between our own various benefit databases and between DWP systems and those of Her Majesty's Revenue and Customs, the latter to identify cases where benefit is in payment while the person is earning without telling us.

Also by sharing HMRC data on employment the Department has been able to cut the burden on employers by being able to establish outcomes without the need to contact employers for confirmation in support of the Department's Job Outcome Targets.

On-line live data sharing also offers opportunities to join up services across government, i.e. linked IT systems are useful for joining up services to individuals. Utilising such services means that customers do not have to tell numerous parts of government the same thing. We already provide services through our Customer Information System (CIS) to a number of Government Departments. CIS is built on modern technology with a flexible architecture that makes use of the system, subject to legal and security conditions, easy to achieve for many common goals for Government, such as the effective storage and recall of accurate identity information.

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.

DWP is only one of many touchpoints with public services that citizens may encounter. We recognise that we play only a part – and that the true value of the data we hold is in using it to meet real world needs, which are not segregated by organisational boundaries.

For example, health can drive both short and long term work and pensions prospects. It is important that we not only understand the likely lifetime consequences of an individual's health but also the impact upon the household (on carers, for example). We must then use this understanding potentially to deliver a simplified benefits system that can work with, not against, periodical and unpredictable fluctuations in health and capability. We need to address the longer-term trust issues that see individuals sharing health information with, for example, insurance companies but not DWP.

DWP is an inherently financial organisation, yet the information we hold relating to existing and potential customers only offers a partial view of their financial resources. This limits what we can achieve.

The legal framework (Qs 9 – 15)

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.

Some of the response to the previous section relates to the legal framework in the context of DWP data sharing. However, the consultation's focus is on the Data Protection Act, and in particular the second principle about incompatible processing.

DWP's processing is fully compliant with this principle with information explaining the purpose of processing provided to the public both in the form of a general statement in use at the point of information gathering and more specific information relating to various customer interactions with the Department. This information has been redeveloped in recent times in a collaborative piece of work with the ICO.

The avoidance of incompatible processing through new data sharing initiatives is managed through the processes and specialist units referred to in the previous section, notably the data sharing protocol, which brings into play expert DPA advice.

The wider questions about the effectiveness of the DPA are not, perhaps, for officials in a central government department to comment on. However, officials who work in this field all regard its principles as encapsulating a common-sense and fair approach to the management of personal information.

It is often felt that problems with the DPA arise not from its content but from misunderstandings about its application. The complexity of the subject is illustrated by the large amount of guidance the ICO has issued. There might be some scope for the rationalization of that guidance.

Also, the way in which it is referred to generally can add to the perception that it is a barrier. Too often the DPA is communicated in a negative light. The only times the DPA is mentioned in the media is when it has been breached or when it has stopped something happening (for example in 'political correctness gone mad' style stories - e.g. 'DPA stops mum taking photos of nativity play' etc.) While we make efforts to dispel this with our own staff through extensive provision of guidance and particular DPA 'myth-busting' exercises, we would welcome further pro-activeness from the ICO in promoting good news stories.

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

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's approach is that bulk data shares should only be carried out under a specific statutory gateway. Case-by-case disclosures are carried out in the public interest often using common law powers as the risk is much easier to manage when all the circumstances of a particular case can be taken into account.

This need to rely on statutory gateways means that processes can be subject to the potential delays of finding suitable legislative vehicles and of the Parliamentary process itself.

Thought has been given across the public sector to the benefits of a wider data sharing power for Government. The practical benefits are obvious but also clear is that the taking of a wider power also has clear political implications and it is not the place of officials to comment on that balance in this consultation reply.

Consent and transparency (Qs 16 – 19)

Question 17

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

DWP has a number of data sharing initiatives which involve customer consent, with the consent in each case designed to be appropriate to the initiative in question.

Consent will not always be a practical option, especially where the data share is not something the individual is going to have an interest in progressing (like tracing fine defaulters referred to previously) and legislation will be needed.

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

The question on transparency has been partly addressed above (see answer to Q9) in relation to the Department's fair processing statement.

The Department takes its responsibility to subject access rights very seriously and resources the process through the network of data protection officers referred to above. Additionally, the Department does not charge a fee for access. Strengthened access rights would not give individuals anything they

do not currently have. The Department would not want any weakening of the exemptions to material which can be accessed, for example the ability to withhold information about fraud investigation processes.

Technology (Qs 20 – 22)

Question 20

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

The rapid advances in computer technology have meant that electronic data matching is becoming increasingly sophisticated. Using computers to compare large collections of information about our customers, often provided to different organisations for different reasons, is now an important tool. This has enabled and catalysed the sharing of bulk data, allowing us to utilise more secure methods for both on-line and off-line sharing.

It is clear that the use of removable media has introduced new risks that must be well managed. Encryption is an important safeguard against misuse.

Question 21

Should the law mandate specific technical safeguards for protecting personal information?

The DPA already requires that appropriate technical measures shall be taken to protect data, which is line with the European Directive. Very specific prescription is best avoided to allow appropriate flexibility and to prevent legislation becoming dated, which is likely in a changing field like IT security.

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? Is sufficient advice about the deployment of such techniques available? Are you confident about using them? What are the barriers to using them?

Anonymisation is already used where appropriate for various research and other purposes eg. National insurance numbers are routinely encrypted.

However, some of these techniques can be technically complex and need a lot of support to implement. It may be appropriate for ICO to work with the Office for National Statistics methodologists to develop this area.

International comparisons and additional questions (Qs 23 – 28)

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 been?

The US is understood to have some provisions where law enforcement authorities can gain access to data held by any organisation. Concerns about this have led to us not permitting research organisations based in the US to have personal data for analysis purposes.

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.

Anecdotally Scandinavian countries have much more data sharing and a generally more relaxed attitude by state and individuals to confidentiality of personal information

I hope this a helpful contribution to your consultation exercise. DWP is fully committed to the development of data sharing on the basis of “Do it more. Do it right” as well as taking our general responsibility to our customers’ personal information extremely seriously. We regularly work closely with the ICO and will continue to do so for the furtherance of lawful, necessary and safe data sharing.