

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

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: H M Revenue and Customs (HMRC) is a central government department that was created in April 2005 by the Commissioners for Revenue and Customs Act 2005 (CRCA) and is responsible for the collection of taxes and duties and strengthening the UK's frontiers. HMRC collects, holds and shares information in relation to its functions in accordance with the framework provided by CRCA 2005, Data Protection Act 1998 and the Human Rights Act 1998.

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

Question 2.

Comments: HMRC can only share information externally where it has the legal authority to do so for example where disclosure is for the purposes of HMRC's functions, where the person or organisation has given consent to the disclosure or where the duty of confidentiality is specifically overridden by legislation that permits disclosure. Information collected by HMRC can only be used further by sharing within HMRC if there is a business need to do so and subject to any provision

which restricts or prohibits the further use of information.

This sharing of information can be beneficial to individuals and society for example via legal gateways we have with the Serious Organised Crime Agency (SOCA) and the Department for Work and Pensions (DWP). This benefits society in the prevention of crime, protection of society from e.g. drugs, firearms etc. benefits to individuals can be seen from the clarification of individual's financial status in determining benefits to be paid etc.

Question 3.

Comments: The main risk in sharing personal information is the risk to the confidentiality of the information that is being shared. We are currently working to rectify any harm to public perception concerning data security within HMRC that has arisen from the recent loss of Child Benefit data. The CRCA does have strict provisions concerning confidentiality of information and not just personal information within the meaning of the DPA. In many senses the strict confidentiality imposed on all information held by HMRC is equivalent or greater than the requirements imposed by the DPA.

Question 4.

Comments: The sharing of personal data by way of legal gateways provides a level of certainty as to what information can be disclosed and can provide sanctions for the deliberate wrongful disclosure of information; or misuse of information. These procedures are subject to verification and audit. Electronic transfer provides an efficient and effective method of transfer but poses risks if the correct safeguards are not put in place. These risks can be mitigated by adherence to the DPA 7th principle and application of the security and risk assessment criteria that it requires.

Question 5.

Comments: No Comment

Question 6.

Comments: No Comment

Question 7.

Comments: No Comment

Question 8.

Comments: No Comment

Section 3: The legal framework

Question 9.

Comments: As the DPA and the access rights it provides have become more widely understood the scope of requests made has widened and requests are made in greater numbers. Access to personal data in this way is part of the general move to public access of information e.g. Freedom of Information Act 2000 however some of the requests now received under the DPA may not have been envisaged at the introduction of the Act. For example the act can be used in relation to obtaining information concerning disputes with other work colleagues or used as a time delaying tactic during

investigations.

Disciplinary and internal investigation files whether held manually or electronically could be exempted. Currently they can only be withheld if the release of the files were likely to affect the apprehension or prosecution of offenders or the prevention or detection of crime.

A potential way of managing DPA requests could be to allow exemption for any data that is subject to disclosure at a future pre-determined time (as in FOIA s22), e.g. if there is a court case or Employment Tribunal pending and the data is subject to the disclosure rules of the court or tribunal.

Increased data sharing demands transparency so that people/organisations that access data can be identified. A potential option would centre on the need to increase transparency in data sharing – data controllers could be placed under a requirement to publish annually a list of those people/organisations that receive personal data processed by a data controller. However there would need to be exceptions for some classes of data controller e.g. prevention of crime, security services, commercial confidentiality

Question 10.

Comments:

The second principle is valuable because it provides reassurance to the data subject which in turn helps to develop confidence that personal data is being used only where necessary, proportionate and lawful. This is particularly relevant for HMRC as we continually seek to restore and further develop taxpayer's confidence in the Department.

Question 11.

Comments:

The increased use and availability of information technology has been a benefit to society but the common perception is that the DPA has failed to keep pace with the speed of technological change – this is a barrier to the public's view of the effectiveness of the DPA whether or not this perception is real or imagined. Greater access to technological capability requires greater security, assurance and risk assessment.

Another societal barrier appears to be one of perception. People appear broadly supportive of the wider benefits of sharing of information where it is perceived to be for the greater good e.g. to cut benefit fraud and for counter terrorism purposes however opinions can change when individuals are the subject of the information being shared.

Question 12.

Comments:

At this stage of maturity of the legislation it may be an advantage if steps were taken to make some elements of the legislation more prescriptive. For example one idea would be to make the IC's guidance more like codes of practice that should be adhered to.

Question 13.

Comments: The introduction of the information access provisions in the Freedom of Information Act 2000 (FOI) and the Environmental Information Regulations (EIR) which have been widely publicised have raised the awareness of the right to access to personal data provided in the DPA.

The Human Rights Act (HRA) and, in particular, Article 8 – right to privacy - places an additional requirement on organisations to ensure that data sharing is necessary lawful and proportional.

Question 14.

Comments: A potential area for development could be the requirement that data sharing organisations increase their transparency with an easily accessible list of organisation with whom they share data. This could be published on the organisations website as an extension to their fair processing statement. However such a development may require extensive research and consultation on the impact any changes would have as well as the exemptions that may be necessary.

Question 15.

Comments: Some organisations may have found responding to requests for data under the DPA costly to satisfy. To discourage speculative requests consideration could be given to a “cost limit”, similar to that found in the FOI legislation, on the provision of data held in manual files.

Section 4: Consent and transparency

Question 16.

Comments: HMRC only seeks to rely on express consent to the lawful processing of personal data in limited circumstances preferring to rely upon statutory gateways. However where our customers wish their accountants or agents to act on their behalf HMRC has in place a formal system for recording this consent.

Question 17.

Comments: The most obvious barrier to the use of consent is that it can be resource intensive where large numbers of disclosures are made e.g. the administrative system to withdraw consent on request of the data subject.

Question 18.

Comments: The increased use of Privacy Impact Assessments (PIA) may help to make information sharing more transparent but the use of PIAs should be considered in the context of the information sharing taking place.

Question 19.

Comments: The framework code published by the ICO provides useful guidance as to good practice encourages a minimum level requirement and helps organisations in the development of their own codes of practice.

Section 5: Technology

Question 20.

Comments: See question 11.

Question 21.

Comments: Mandating technical standards for the protection of personal data may prove to be difficult as without the constant update of the law you inevitably end up with a minimum standard. The legal provisions may be constantly trying to catch up with technical advances. Furthermore, the imposition of statutory requirements could place significant cost and other resource burdens on organisations and could, as a result, inhibit legitimate data sharing. IT may also be difficult to reconcile mandatory requirements with the risk based approach to providing safeguards which has been the norm.

Question 22.

Comments: Whenever HMRC can use data that is anonymous it will do so. Anonymous data can be used in areas such as the testing of new systems or for training purposes which can help the development of the business area without impinging on the confidentiality of the personal data.

Section 6: International comparisons

Question 23.

Comments: No comment

Question 24.

Comments: No comment

Question 25.

Comments: HMRC have found Switzerland and Singapore are countries with particularly restrictive data protection measures, this has proved problematic for HMRC and its ability to carry out its functions. We are not in a position to examine the consequences.

Question 26.

Comments: Historically, Swedish society had an open attitude to sharing personal information. The culture was that transactions such as tax returns should be a matter of public record. Developments to EU Data Protection and other legislation have forced it to tighten up its own Data Protection laws.

Section 7: Additional questions

Question 27.

Comments: No comment

Question 28.
Comments: No comment

