

# 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: I hold personal information related to participants of a specific sporting activity. The information is supplied by race entrants. Information may be shared with associated sporting bodies on request (e.g. a race organised for another club or group may be requested to provide personal details of prize winners to invite them to a presentation. The data stored on electronic media is of a non-financial nature (e.g. name, address, previous race results). Bank account details may be transcribed from an enclosed cheque to the entry form for subsequent reference if there is a query)

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

Question 2.

Comments: There are situations where data sharing is necessary to the smooth running of society without over-burdening individuals to provide the same information on multiple occasions to closely linked bodies.

Question 3.

Comments: There are, in general, two significant risks to the individual associated with data

sharing: 1. Erroneous data may be propagated widely, beyond the control of the individual, which cannot be corrected simply. 2. The propagated data may be misused by those bodies receiving it indirectly (i.e. not used for the purposes for which it was originally provided).

Question 4.

Comments: The greatest risk is posed when data is transferred in bulk, without regard to the required purposes and without the removal of unnecessary data. This risk is increase where the transmission can be intercepted and the data is not encrypted. This may occur on any open transmission medium (e.g. the internet) or where portable media is used.

Question 5.

Comments:

Question 6.

Comments:

Question 7.

Comments:

Question 8.

Comments:

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

Question 9.

Comments: The DPA is cited by many bodies as a reason not to speak to you about specific concerns you have with their operation. Even where personl data is not involved or requested.

Question 10.

Comments: Even where the second principal is 'adhered to' by a corporate body, it is often violated by the sharing of data with other bodies who do not also adhere to the principal within the declared data usage of the first body.

Question 11.

Comments:

Question 12.

Comments: The DPA should mandate that:

1. a complete audit trail is maintained of all data sharing ativities at the level of the individual data record. A full audit trail of all subsequent data sharing activities must also be available to each data sharer. A copy of the full audit trail must be made available to each individual data supplier, on request, free of charge to the individual.
2. It is the responsibility of the original recipient of personally data to ensure that ALL subsequent processing of that data, whether within that body or external to it, is performed in accordance with its own declared usage of that data.

Question 13.

Comments:

Question 14.

Comments:

Question 15.

Comments:

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

Question 16.

Comments:

Question 17.

Comments:

Question 18.

Comments:

1. The use of catch all phrases (e.g. may be shared with our partners or other similar companies) in requesting data consent should be prohibited. Explicit details should be provided for opting IN to data sharing (e.g. Do you want us to share your details with irrelevant marketing companies so that they can bombard you with unwanted advertising?)
2. The provision of personal data, at the request of a providing individual, must include full details of all data held by the organisation, details of all data sharing activities relating to that individual (both direct sharing and subsequent sharing) together with a copy of all the data held by each of the bodies with whom that data has been shared, either directly or indirectly. (Any charge for providing this data to an individual should not exceed £2.00)

Question 19.

Comments:

#### **Section 5: Technology**

Question 20.

Comments: The ability to transfer data in bulk has led to excessive data sharing, both in terms of the number of occasions when data is being shared and in the amount of data being transferred which is unnecessary for the recipient's purposes.

Question 21.

Comments: It should be an absolute requirement for all personal data, of a financial or sensitive nature, held by any portable device (including laptops, disks, or other storage media) to be encrypted. The use of encryption mechanisms should not be at the discretion of the user, nor able to be circumvented by them. This provision should also be extended to the direct transfer of personal data beyond the company's internal LAN.

Question 22.

Comments:

## **Section 6: International comparisons**

Question 23.

Comments: The US has a very significant law in regards to the loss/misplacement of unencrypted personal data. It is the responsibility of the organisation sending the data to inform every individual, whose data has, or may have, been lost or misplaced, together with the provision of identity theft protection for a guaranteed time period at no cost to the individuals involved. (With the direct cost of data loss typically running into several millions of dollars, this provision has had a significant impact on the utilisation of encryption technology as the norm)

Question 24.

Comments:

Question 25.

Comments:

Question 26.

Comments:

## **Section 7: Additional questions**

Question 27.

Comments: Significant effort must be invested in the 'verification' of a remote enquirer when handling personal information. The typical provision of a single (occasionally several) public domain items of knowledge is totally inadequate to confirm the identity of a caller. It is not unreasonable to institute a call-back process to a specific land-line telephone to continue the process, or to confirm an alternative contact mechanism to be used on that occasion.

The scope of the personal information to which this consultation applies should be clarified to that information of either a sensitive or (direct or indirect) financial nature, and hence the less significant data usage, such as mailing lists, are excluded.

Question 28.

Comments: It should be made the responsibility of every organisation receiving shared data to actively confirm the correctness of that data, except where the original data provider has explicitly permitted data sharing with that named body. This must require, as a minimum, that the receiving organisation contact the individual, providing a copy of the received data, with a request that the validity of the data be confirmed or corrected, at no cost to the individual. If any aspect of the data is corrected by the individual, the held data must be amended, together with a notification to the original data supplier of the data error. If the amended data has been shared with any other organisation, the correction must be propagated to them.

