



THE ASSOCIATION OF ELECTORAL ADMINISTRATORS

Formal response to Data Sharing Review consultation paper on the use and sharing of personal information in the public and private sectors

Introduction

This is a formal response from the Association of Electoral Administrators (AEA) to the above consultation paper issued on 12th December 2007.

The AEA's response is restricted largely to its interest in and concerns about the use of the electoral register and the impact this has on the wider issues of participation in elections and general democratic engagement.

Since 2001, the electoral register has been available for sale to credit reference agencies for matters relating to credit and money laundering and to government departments and other bodies for the prevention and detection of crime, enforcement of the criminal law and vetting of employees and persons relating to national security. The register is also available to local authorities and the police for similar reasons to those outlined above. There is also available for general sale an edited register which contains the details of any elector who has not opted out of this version of the register.

Question 1

The AEA's members are involved in the creation and maintenance of the electoral register and other records relating to registration and elections. All registers and related records are stored as data on i.t. systems.

Question 2

It is the AEA's policy that the electoral register should only be used for electoral purposes except for purposes relating to national security. The fact that information from the register is used for other purposes and shared with other organisations acts as a dis-benefit and disincentive to persons wishing to register as an elector. This leads to lack of accuracy and completeness in the register and interferes with the democratic process. This is particularly true in cases where the information is provided to private sector organisations but the same argument can be advanced in terms of data sharing with the public sector.

An advantage can be when information from other public records is available to assist with verification of entries on the register.

Question 3

Disincentives to register (see 2 above). Citizens who do not register cite various reasons for not so doing ranging from not wanting to receive junk mail to personal security fears. There is little doubt that, if the register is used for non-electoral related purposes which are likely to affect an individual's position, financial or otherwise, many people choose deliberately not to register, e.g. poll tax, benefit checking exercises etc.

Question 4

The greatest risks arise from members of the public not being aware of how their personal data provided for electoral purposes will be used. This often leads to difficulties in persuading citizens to register in the first place and/or to renew registrations if they feel that their personal data is being misused. The use of inaccurate information by credit reference agencies and the claims made by organisations such as 192.com are cases in point and this was reinforced by a recent BBC Watchdog programme.

Question 5-7

No response

Question 8

Under present legislation, the electoral register has to be sold to credit reference agencies (CRA). However, the data is then often not processed correctly which means that a person applying for credit will be told by the CRA that they are not registered at a particular address when they very clearly are. The problem is then often raised with the local authority which does have the correct data and it is extremely difficult to get CRAs to correct the information which they hold. All of this is extremely wasteful in terms of public resource and does little to persuade the public that their records are safe in the hands of their local authority.

Question 9

In general terms, we believe that the DPA works well. However, the problem arises when some elements of legislation cut across the DPA e.g. the Representation of the People Regulations 2001. The problem lies with the latter, not the former.

Question 10

There is clear evidence that elements of the private sector do not take sufficient care in the processing of data that has been obtained, lawfully or otherwise, from a public source (see questions 4 and 8 above). As stated in the opening response, the AEA holds the view that information obtained for a specific purpose should only be used for that purpose where the overall effect of not so doing could be to deny a citizen their democratic right.

Question 11

No response

Question 12

The 2nd principle should be changed from "limited" to "specified" to make clear to any citizen providing information the actual purposes for which it will be used prior to the information being provided.

Questions 13-15

No response

Question 16

Yes in both cases. However, these provisions are often honoured only in the breach. A recent example of this is the Audit Commission's request to use electoral register data for the purposes of a national fraud initiative. No information was provided to citizens registering for the electoral register that their data would be used for this purpose. There are further examples across many parts of the public sector.

Questions 17-19

For the reasons stated above, the AEA believes that it is essential that all citizens should be aware of the use to which the electoral register is to be put if it is not limited solely to electoral purposes. This should be explicitly stated at every point during the registration process.

Question 20

Clearly, technological advances have greatly permitted the sharing of data with consequential adverse affect on registration levels for the electoral register. It is stated that several million citizens are not registered who are entitled to be. If that is the case, those interested in the democratic process and the fact that those elected to represent them should be representative of the will of the people should be very concerned at this franchise deficit. The use of the electoral register and the ease with which it can be done has encouraged this state of affairs. If we are to move to a position where those not registered are encouraged so to be and then to participate in elections, it is critical that the sharing of data is not permitted in this particular area of work so that public confidence in the overall process can be restored.

Question 21

Yes, it is essential. All data held on portable devices or to be transmitted in any way must be encrypted to suitable and appropriate standards.

Question 22

No response.

Questions 23-26

No response.

Question 27-28

As stated above, this issue cannot be divorced from the central issue of democratic engagement. Appropriate safeguards must be built into the data protection legislation to support this principle and then enforced rigorously. Similarly, it should not be permissible to use other legislation to then “get round” the restrictions imposed by the primary legislation governing the use of such data.

February 2008