Annex to the Explanatory Memorandum to The Electoral Registration Pilot Scheme Order 2014

Privacy Impact Assessment

1. Approach

This Privacy Impact Assessment (PIA) builds on the PIA conducted at the Bill stage of the Electoral Registration and Administration Act 2013 (the 2013 Act)[1], with a specific focus on exploring the data protection issues surrounding the power enabling the Secretary of State to make Regulations requiring Electoral Registration Officers (EROs) to disclose their registers for comparison with other data for the purposes of verifying information relating to a person who is registered or who is named in an application for registration, ascertaining the names and addresses of people who are not registered but who are entitled to be registered, or identifying those people who are registered but who are not entitled to be registered.

The Electoral Registration Pilot Scheme Order 2014 ("the Order"), made under powers in sections 10 and 11(3) of the 2013 Act, will establish a pilot scheme enabling information in electoral registers in specified areas of Great Britain to be compared with information held by the Secretary of State for Transport about individuals' driving records and vehicle registration documents. Information held by the Secretary of State for Work and Pensions may also be used in the exercise. The comparison must be made for the purposes of verifying existing entries in the electoral register and finding the details of people who are not registered but who are entitled to be registered. All disclosures of data under the Order must have taken place by 31st March 2015. Once the scheme has been evaluated the Lord President of the Council will inform the ministers and EROs involved in the pilot about the results of the comparison and the usefulness of the information in fulfilling its purposes.

Those expected to take part in the pilot scheme are EROs, the Department for Transport (DfT) and the Department for Work and Pensions (DWP), all of whom are well used to the handling, processing and security of personal data and all of whom will have produced their own PIAs for data matching. In addition, however, the Order requires the Lord President, the data holding organisations and each participating ERO to conclude a written agreement as to the processing of information (including its transfer, storage, security and destruction) before any disclosures of data are made. Cabinet Office will also expect those carrying out data matching operations to comply with the relevant legislation and the data protection principles that personal data must be:

- Fairly and lawfully processed;
- Processed for specific and lawful purposes and not further processed in a way that is incompatible with the original purpose;
- Adequate, relevant and not excessive;
- Accurate and up to date;
- Not kept for longer than is necessary;
- Processed in accordance with the data subject's rights;
- Kept secure;

[1] The PIA completed for the Bill stage of the 2013 Act – *Individual Electoral Registration: Privacy Impact Assessment Report* (May 2012) – is available at https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/61333/Privacy-Impact-Assessment-090512.pdf .

- Not transferred to countries outside the European Economic Area unless an adequate level of protection is ensured or an exemption applies.

This PIA explains in greater detail how the privacy issues which may arise from data matching are to be addressed and the risks mitigated.

The PIA is a living document and will continue to be updated as data matching policy and processes develop.

2. Background

The Coalition Agreement contains a promise to "reduce electoral fraud by speeding up the implementation of individual voter registration". Individual Electoral Registration (IER) was introduced in England and Wales on 10th June 2014 and is due to be introduced in Scotland on 19th September 2014. This is a fundamental change to our system of electoral registration. It will improve the accuracy of the electoral register, requiring electors to register to vote individually rather than by household. Before an individual can be added to the register, they must be verified through the cross checking of their information against trusted public data sources. This change will make the system less vulnerable to fraud and will provide an opportunity to support the completeness of the register by tackling under-registration.

An initial set of data matching pilot schemes took place in 2011, using powers in the Political Parties and Elections Act 2009, to test the usefulness of a range of public authority data sets for helping EROs to improve the accuracy and completeness of their registers. Participating EROs were enabled to match their registers against specified data sets in order to find potential electors who were missing from the register. Driving licence records were among the data against which certain EROs were able to match their registers. DWP data was also used.

Findings from the 2011 pilots indicated that matching electoral registers against data held by DWP might enable a significant proportion of the electorate to be confirmed on the register, producing substantial savings in time and money. Following refinement of the matching process and further testing in 2012 and 2013, this process for the confirmation of existing electors using DWP data is being used in the transition to IER. In the pilot scheme to be established under the Order the Government intends to test the possible use of DfT data for adding to the confirmation rate produced by matching register entries against DWP data, as well as for identifying potentially eligible individuals who are not currently registered to vote.

3. Personal data to be used

In the data matching to be undertaken under this Order, individuals' information held on the electoral register may be compared against the name, address and postcode of individuals appearing in databases kept by the Secretary of State for Transport and the Secretary of State for Work and Pensions, namely -

(a) data relating to persons in relation to whom the Secretary of State for Transport maintains a driving record;

(b) data relating to persons who are shown in records kept by the Secretary of State for Transport as being the keeper of a vehicle;

(c) data relating to social security (including information kept on behalf of the Department for Social Development); and

(d) data relating to working tax credit, child tax credit and child benefit kept on behalf of HM Revenue and Customs.

4. Data protection issues and risks of data sharing

The Government takes the handling of personal data and prevention of identity fraud very seriously. The changes that are being made to electoral registration (and which received cross party support) are intended to prevent fraud and maintain the integrity of the electoral system. This section provides details of data protection issues and risks for data sharing.

The following table sets out data protection issues of data sharing:-

Issue	**Description**
Retention and deletion of data received.	Data management policy will clearly set out retention and disposal schedules and will conform to the data protection principle of not keeping data for longer than is necessary. The Order provides that a written agreement must be made between the Lord President, the Secretary of State for Transport, the Secretary of State for Work and Pensions and the ERO as to the processing of information, including its storage and destruction.
Incorrect data from Public Authority	The action to be taken in the event of incorrect data being received from DfT and/or DWP will be determined according to the data management policy.

Issue	Description
Data received results in identification of fraudulent activity.	EROs will already have procedures in place for dealing with instances of suspected electoral fraud; data sharing merely provides an alternative way in which such instances may be identified and existing procedures will be followed.

The table below sets out data protection risks of data sharing:-

Risk Description	Controls/Mitigation
Data security breach – data is mishandled by the ERO or other authorised users.	Data management policy in place and monitored. 2013 Act and the Order provide for the making of written agreements as to the processing of information, including its security. Engagement with IT suppliers to ensure systems appropriate to protect data. Continued engagement with key stakeholders to ensure security of personal data is built into policy and processes.
Data is used for unauthorised purposes or shared inappropriately.	Data management policy in place and monitored. Will conform to data protection principle of data being processed for specific and lawful purposes.

Risk Description	Controls/Mitigation
	Engagement with IT suppliers to ensure systems appropriate to protect data. Continued engagement with key stakeholders to ensure security of personal data is built into policy and processes. The Order makes provision for an offence of onward disclosure of information.
Access to the data – data matching leads to the identity of an anonymously registered elector being disclosed.	The Order provides, and EROs must ensure, that anonymous electors are omitted from the data sent to Cabinet Office and DWP.
Storage of the data received – inadequate storage of the data could lead to loss.	Data management policy in place and monitored. Will conform to data protection principle of data being kept secure. 2013 Act and the Order provide for the making of written agreements as to the processing of information, including its storage and security.

5. Data Matching impact on an individual

We recognise that individuals are likely to have concerns about the implications of their personal data being shared between organisations. However, the data matching process provided for by the Order will not involve the transfer of any personal data other than Name, Address (including postcode) and Date of Birth.

There is unlikely to be any significant additional data protection impact because individuals are already required by law to provide EROs with the above information in order to populate

the electoral register. There is no option to opt out from registration for those eligible to vote. Consequently, these provisions do not have any significant further impact on an individual's privacy than the current legislative requirement – they simply support EROs in carrying out their legal duty to maintain the accuracy and completeness of the electoral register. The new provisions enable EROs to access from an alternative source personal data to which they are already legally entitled.

Some individuals may be registered to vote on the basis of their actual address while choosing to use a different address for correspondence purposes, with the result that the address held by other public authorities will not match that held by the ERO. It is possible that people in this position could find themselves subject to some follow-up activity (correspondence and/or visits) despite having already correctly completed all necessary forms, but any impact is expected to be low.

It is nevertheless acknowledged that the very processes of data matching and data sharing carry some degree of inherent risk. Any additional risk is however mitigated by the specific measures that will be contained in the data management policy and in the requirements as to processing of information which will be agreed between the Lord President of the Council and participating Ministers and EROs under the Order.

6. Consultation and general communications activity

The following organisations and key stakeholders have been involved in the assessment of data protection risks for the IER policy as contained in the 2013 Act:

- Information Commissioner's Office
- Metropolitan Police
- Association of Chief Police Officers
- Serious Organised Crime Agency
- HM Revenue and Customs
- Department for Work and Pensions
- Electoral Commission
- Association of Electoral Administrators
- Society of Local Authority Chief Executives
- EROs

7. Conclusion

The further piloting of data matching under the Order is likely to benefit EROs by enabling them to test whether access to the DfT databases concerned will help to improve the accuracy and completeness of their registers. It will do this by enabling an assessment of the potential of DfT data for adding to the confirmation match rate already being achieved by matching their existing register entries against data held by DWP, and also for identifying potentially eligible individuals who are currently missing from the register. The pilots will be essential for ensuring a strong evidence base for making decisions as to the costs and benefits of the wider-scale use of this data.

It is appreciated that individuals may be concerned about the possible implications for their privacy and the security of their personal data, but any small additional risk that may arise as a result of these data matching pilots will be mitigated by the wide range of safeguards explained in this Privacy Impact Assessment. Each individual data matching arrangement will be subject to its own PIA, which will contain details of the scheme, effects upon individuals, security measures and compliance with the Data Protection Act 1998.

8. Contact Details

For further information regarding this PIA please contact **Carol Gokce** at the Cabinet Office, tel 020 7271 2679: email Carol.Gokce@cabinet-office.gsi.gov.uk