EXPLANATORY MEMORANDUM TO

THE ELECTORAL REGISTRATION DATA SCHEMES ORDER 2011

2011 No. [XXXX]

1. This explanatory memorandum has been prepared by the Cabinet Office and is laid before Parliament by Command of Her Majesty.

2. Purpose of the instrument

2.1 This Order gives effect to proposals by local authorities to run data matching pilot schemes. It allows electoral registration officers to use other public authorities' data sets to assist them to identify eligible electors who are missing and to improve the accuracy and completeness of electoral registers. The Order also sets the date by which the Electoral Commission must evaluate the schemes.

3. Matters of special interest to the Joint Committee on Statutory Instruments

3.1 None

4. Legislative Context

4.1 Sections 30 to 34 of the Political Parties and Elections Act 2009 ("the Act") make provision for the introduction of individual electoral registration in Great Britain.

Schemes for provision of data to registration officers

4.2 Section 35 of the Act provides for the Secretary of State to make an order providing for schemes for the provision of information to electoral registration officers by other public authorities. The schemes are intended to support the wider work ensuring and improving the completeness and accuracy of electoral registers as part of the overall transition to individual electoral registration. The schemes will also identify whether and how access to public authority data sets might assist electoral registration officers in meeting their duty under sections 9 and 9A of the Representation of the People Act 1983, primarily by comparing electoral registers against other data sets.

Schemes under section 35: proposals, consultation and evaluation

4.3 Section 36 of the Act requires the Secretary of State to consult the Electoral Commission, the Information Commissioner and the public authorities holding the data sets before making the Order. It also requires the Electoral Commission to assess and report on the outcomes of the data matching pilot schemes.

4.4 Article 3 of the Lord President of the Council Order 2010 (S.I. 2010/1837) provides that the powers conferred on the Secretary of State under the Act (with exceptions which are not relevant to this Order) are exercisable concurrently by the Secretary of State and the Lord President of the Council.

The Representation of the People (Electoral Registration Data Schemes) Regulations 2011

4.5 It is intended that a connected set of regulations, the Representation of the People (Electoral Registration Data Schemes) Regulations 2011 will be made at the same time as this Order. The Regulations would enable electoral registration officers to provide their electoral registers to another person so that, where a scheme under this Order provides for a public authority to provide data to a registration officer, the registration officer can use a service provider to undertake a comparison of the registers and the data set held by the public authority.

5. Territorial Extent and Application

5.1 This instrument applies to all of the United Kingdom.

6. European Convention on Human Rights

The Minister for Political and Constitutional Reform has made the following statement regarding Human Rights:

In my view the provisions of the Electoral Registration Data Schemes Order 2011 are compatible with the Convention rights.

7. Policy background

7.1 The Government has made a commitment to introduce legislation to speed up the implementation of individual electoral registration by July 2014. Current legislation allows individual electoral registration to be brought into force on a voluntary basis in this Parliament and on a compulsory basis from late 2015 at the earliest.

7.2 The Government intends to amend this position so that electors will be asked to register individually from 2014 in order to modernise the electoral registration system and tackle fraud. Electors will be asked to provide identifying information which will be checked before they are added to the electoral register. The process will replace the existing system of household registration.

7.3 As part of the transition to the new system, electoral registration officers will run data matching schemes during 2011 to see if existing public authority databases can be used to improve the accuracy and completeness of the electoral register. These schemes are designed to identify individuals not on the electoral register who are entitled to be registered, as well as to show up false, duplicate and inaccurate registrations.

7.4 Electoral registration officers will be able to review and remove entries on the electoral register that contradict data matched against other public records and are shown to be fraudulent or inaccurate. They will also be able to identify individuals who appear on public authority data sets but not on the electoral register, to contact them and encourage them to register.

7.5 Electoral registration officers and the data holding authorities will need to agree in writing the arrangements for the transfer, storage, destruction and security of

data during the schemes. As part of this process the registration officer may pass a copy of the electoral register to another person to allow the register and data from another database to be compared.

7.6 The Electoral Commission will evaluate the success of the schemes.

8. Consultation outcome

8.1 The Electoral Commission, the Information Commissioner and data holding authorities have been consulted on this instrument as required by section 36(2) of the Act. The Electoral Commission cautioned that particular attention should be paid to the detail of the schemes, especially around the security of data, methodology and timing. Where practicable, those and other suggestions have been incorporated into the development of the pilots. The Electoral Commission remains integral to work to design and develop the pilot schemes. Cabinet Office has acted to reassure the Electoral Commission by involving it in the development of the methodology and acknowledging that the agreements under Article 4 will be required to cover in detail arrangements in each scheme for the management of data. (A template Article 4 written agreement is available at Annex A). The Electoral Commission has agreed the evaluation date.

8.2 The Information Commissioner's Office recognises that the creation of a statutory gateway goes a long way to delivering compliance with the requirements of the Data Protection Act 1998 and ensures such data matching is lawful. It also welcomed the requirement for agreements detailing requirements as to the processing of data. The Information Commissioner's Office explained its concern about the secure transfer of data and that it is vital that all parties understand and take the appropriate measures to mitigate the risks inherent in transferring large personal data sets.

8.3 The Cabinet Office will continue throughout the development and implementation of the pilot schemes to concentrate on ensuring that appropriate measures are in place for the secure transfer and processing of all data.

8.4 The Information Commissioner's Office also raised its concern about the extent to which it is necessary to share all of the data in each of the data sets. While it did not wish to raise an objection to the Statutory Instrument being laid in its current form, it expected the evaluation of schemes to examine which of the data sets was relevant to their purpose and which was excessive and did not significantly contribute to the purpose of increasing registration.

8.5 Cabinet Office does not intend that data will be shared that does not have a relevant application to the purposes of the pilot schemes and will evaluate, as is suggested, how successful the pilot schemes are in restricting the exchange of unnecessary data. The full response sent on behalf of the Commissioner is attached at Annex C.

8.6 This instrument has also been developed in partnership with each of the data holding authorities listed in the Schedule. Each has contributed to its inclusion in the data matching pilot schemes by way of this Order.

9. Guidance

9.1 There is no general application of this instrument as it is specifically designed for the data matching pilot schemes. Cabinet Office will be working closely with the Electoral Commission, the Information Commissioner and the individual data holding authorities and electoral registration officers affected by the Order about the practical details of the working of the schemes.

10. Impact

10.1 A full regulatory impact assessment has not been prepared for this instrument because no impact on the private or voluntary sector is foreseen. An overarching privacy impact assessment of the data schemes is available at Annex B.

10.2 A privacy impact assessment will be prepared for each scheme as it involves the processing of personal data of individuals.

11. Regulating small business

11.1 The legislation does not apply to small business.

12. Monitoring & review

12.1 The Electoral Commission is responsible for evaluating the outcome of the data matching pilot schemes as required by section 36(3) of the Act. It will report on each scheme to assess its effectiveness and to what extent the scheme has enabled electoral registration officers to meet their registration objectives.

13. Contact

Mark Hughes at the Cabinet Office, Tel 020 3334 3824: email: Mark.Hughes@justice.gsi.gov.uk can answer any queries regarding the instrument.

Annex A

Outline Electoral Registration Data Schemes Agreement

1. Under the Electoral Registration Data Schemes Order Statutory Instrument, an agreement needs to be in place before personal data to support Electoral Registration can be shared between Electoral Registration Officers (EROs) and Data Holding Organisations (DHOs).

Purpose of the agreement

2. The purpose of this agreement is to:

- Explain governance arrangements for data transfer and matching
- Explain the expected outputs and inputs for this process
- Set out information security standards
- Detail timescales

Governance Arrangements

3. This agreement will be signed off by the DHO at Director level, and by the Electoral Registration Officer.

4.

- The DHO will destroy securely (according to Government policy on secure information disposal as specified in CESG Infosec Manual S) all ERO supplied data by the end of December 2011.
- The DHO will use the data received from the ERO solely for the purpose of providing the ERO with a matching report. They will not use it for any other purpose.
- The ERO will use the data produced by activity under this agreement solely for the purpose of the data matching pilot:
    i. Improving the accuracy and completeness of the electoral register.
    ii. Evaluation of the data matching pilot by the ERO, Cabinet Office and the Electoral Commission.
- The data will not be used for any other purpose by the ERO.
- All data received by the ERO from the DHO will be securely destroyed by the end of December 2011 according to Government policy on secure information disposal as specified in CESG Infosec Manual S.

5. The ERO and the DHO will both provide monthly progress reports including the number of electors processed, matched and followed up, and highlighting any difficulties encountered. They will also each produce a final evaluation report. These reports will be reviewed by the DHO Director, the ERO, Cabinet Office and the Electoral Commission.

6. The DHO and the ERO will provide contact details of technical staff who can be contacted in the event of problems, and more senior staff up to Director/ERO level, to whom serious concerns will be escalated.

7. The DHO will develop matching rules based on a Matching Document to be supplied by the Cabinet Office. This Matching Document will draw together current best practice on matching, using information supplied by EROs and other Data Holding Organisations. The matching rules will be the same across all EROs. Individuals missing from the electoral register but present in other data will be reported. Matching Reports will allow for the possibility of ‘fuzzy’ (inexact) matches. In these cases, the match will be returned to the ERO

in the matching report and the ERO will exercise discretion about which entries should be followed up.

Expected Outputs and Inputs

8.

- The DHO will match the ERO extract against data from the DHO's information system.
- The ERO extract sent to the DHO and the DHO matching report returned to the ERO will be in the agreed standard attached as an annex to this agreement.

Information Security and Data Transfers

9.

- All activities under this agreement (including the extract, transfer, storage and use of the information in the matching report by the ERO) must conform to legislation, including any applicable provisions of the Data Protection Act 1998, and HMG policy, including Government Information Assurance Standard 6 (IS6).
- The DHO and the ERO will follow the process to be notified to them by Cabinet Office in advance of the data matching pilots to ensure the safe extraction, transfer and loading of data.
- The ERO undertakes to ensure that all staff involved in using information supplied by DHO complete information assurance training (to be provided by Cabinet Office). Alternatively, the ERO could provide locally arranged information assurance training approved by Cabinet Office. The ERO confirms that their organisation as a whole continues to comply with the GCSx Code of Connection (CoCo), or with the GSX CoCo in Scotland.

10.

- Both parties undertake that electronic copies of information supplied under this agreement will only be stored on hardware located in secure areas, and will not be taken away from secure areas in removeable media (e.g. laptops and memory sticks).
- Electronic data will at all times be classified as "RESTRICTED".

11. The ERO undertakes that paper copies derived from matching information (which will be used by canvassers) will be treated as "PROTECT", and that a paper or bundle of papers with information about 50 people or more will be treated as "RESTRICTED". This means that the forms will be kept on the canvasser's person or locked away at all times. Processing of the forms will be done at secure ERO premises.

12. Both parties undertake to notify immediately any information security failure to:

- Their internal Data Security Teams
- Their counterparts in the process – i.e. ERO to DHO and vice versa
- A nominated contact at Cabinet Office

In the event of a security breach, "near miss" or risk being identified, both parties will stop data transfers until the risk or issue is resolved. In the event that the breach either cannot be resolved or is very serious (in the view of Cabinet Office), data transfers between that ERO and the DHO will be stopped. Neither the ERO nor the DHO will be obliged to resume data transfer until they are satisfied with the security arrangements.

13.

- Data Transfers will follow the Guiding Principles for Data Movement included

within the CESG Guide.

- Data will be transferred both from the ERO to the DHO and from the DHO to the ERO using a Secure Electronic Transfer with data encrypted before transfer on every occasion that there is a transfer.
- Responsibility and accountability for information security (including the data transfer process) will rest with the DHO Data Guardian or the ERO.
- Precise arrangements for transfer and encryption will be as directed by Cabinet Office prior to the first transfer.
- This transfer must only be performed by named individuals in the DHO and the ERO's staff, and they undertake to do this personally and not delegate the task to other staff.
- On every occasion that an ERO makes a transfer, the ERO's internal security team must first confirm that encryption has been performed correctly.

Timescales

14. Data may be sent by the ERO to the DHO for matching at any time between June and November 2011, provided that applicable Statutory Instruments are in force. The DHO will return the matching report to the ERO within 5 working days.

Annex B

Privacy Impact Assessment – Data Matching Schemes

1. Approach

This Privacy Impact Assessment (PIA) builds on the PIA conducted at the Bill stage of the Political Parties and Elections Act 2009 (the 2009 Act), with a specific focus on exploring the data protection issues surrounding the power enabling the Secretary of State to make Orders requiring public authorities to provide Electoral Registration Officers (EROs) with data for the purposes of enhancing the electoral register.

Those taking part in the data matching schemes will be EROs and a selection of data-holding public authorities, all of whom are well used to the handling, processing and security of personal data and all of whom will be producing their own PIAs for this project. In addition, however, the Electoral Registration Data Schemes Order 2011 (the Order) will require the public authority and ERO to conclude a written agreement as to the processing of data (including its transfer, storage, destruction and security) before any data matching scheme can commence. Cabinet Office will expect those operating the schemes 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;
- 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 these schemes are to be addressed and the risks mitigated.

The PIA is a living document and will continue to be updated as the policy on data matching schemes develops.

2. Initial Privacy Impact Assessment

This document develops further the previous assessment of the data protection issues to which the data matching provisions of the 2009 Act[1] may give rise. This assessment provides a basis for the PIAs which will be required for each of the Orders made under the powers.

Some key points from the initial PIA:-

- Data which EROs need to access from public authorities relate to two areas – people and properties.
- The 2009 Act stipulates that information provided to EROs may not be disclosed to any person other than one to whom the officer may delegate his or her functions (with exceptions for registration purposes and for legal proceedings).

[1] See Appendix 1 for details of sections 35 and 36 of the 2009 Act.

- The purposes for which the ERO can use the data have been clearly defined in the legislation to ensure proportionality. The overarching 'purpose' of the data matching exercise is to enable the ERO to carry out their registration duties.
- EROs will only be entitled to receive information that is relevant to register electors or assists them to use that data for that purpose – individuals' residence; the location of residential properties which would allow for cross checking different databases (which could help reduce the risk of electoral and financial fraud) and age data.
- Data will be shared between a specified ERO and a specified Public Authority.
- The 2009 Act would not change the type of data accessed, but will make it easier for EROs to access data from a wider range of public authorities.
- The data matching process that is provided for in the Act will not involve the transfer of any other personal data except Name, Address and Age or Date of Birth.
- There are unlikely to be significant additional data protection impacts because individuals are required by law to provide EROs with the above information to populate the electoral register.
- The provisions in the 2009 Act enable EROs to access personal data to which they are legally entitled from a different source, where a household has not provided accurate data.
- The provision will support EROs in ensuring the electoral register is as accurate and complete as possible.
- The targeted data matching approach will enable the Cabinet Office to further test the impact on individuals and to gauge the level of concern about data sharing impacts before proceeding.
- Each individual data matching scheme will require approval from the Secretary of State, who must consult with relevant bodies – including the public authority from whom information is being requested and the Information Commissioner and the Electoral Commission (the Commission) – before laying an Order introducing a scheme before Parliament.
- Each individual data matching scheme will have its own PIA, which will need to be produced in conjunction with the Cabinet Office as part of the application process.

3. Background

The basis for electoral registration in Great Britain is an annual canvass of households. In addition, individuals may register to vote throughout the year by completing an individual "rolling registration" form. The electoral register is maintained by EROs who are appointed by, but independent of, local authorities, and each register is maintained on a local authority basis.

To fulfil their registration duties EROs have access to a number of datasets to assist them in compiling the register and ensuring its accuracy; the specific types of information that a registration officer might need access to are likely to be full names of individuals, their full addresses and date of birth.

EROs are already legally entitled under Regulation 35 of the Representation of the People (England and Wales) Regulations 2001 to access any dataset held by the local authority that appointed them. They already make use of the following datasets:

- the register of births and deaths;
- council tax records;
- registers of households in multiple occupation;
- local land and property gazetteers;
- housing benefit applications;
- lists of persons in residential and care homes; and - where allowed –

- details of “attainers” (those aged 16 or 17) held by education departments[2].

However, there are limitations on what can be achieved under the existing statutory duties. Currently, the Secretary of State may make regulations allowing EROs to "inspect" records held by *any* public authority; such regulations may only permit a registration officer to inspect records in the form in which they are held. This is only permitted for the purposes of `registration duties`, the relevant condition is provided for by paragraph 5 of schedule 2 of the Data Protection Act 1998.They do not place an obligation on another public authority to supply the registration officer with information at a time and in a format which is useful to them, or to put in place a tailored regime for the matching of information.

The provisions in the 2009 Act enable the Secretary of State to pilot schemes where specified public authorities are required to provide specified EROs with specified data for the purpose of fulfilling their registration duty. The purpose of the schemes is to allow the Government and EROs to explore which kinds of databases would be most useful in identifying eligible electors and cross-checking registration data, as well as to test the rigorous data security processes that would be needed. An arrangement of this kind will allow the Government to consider the case for taking these steps on a wider scale.

4. Registration Improvements Project

The overall aim of the Registration Improvements Project (the Project) is to improve the accuracy and completeness of the electoral register through measures that complement and enhance Individual Electoral Registration (IER). The 2009 Act specifically enables the setting up of data-matching schemes to identify potential data sources for validating registration and aiding the EROs to fulfil their statutory duties (as set out in sections 9 and 9A of the Representation of the People Act 1983).

The objectives of the Project, initially through the data-matching schemes, is to help EROs improve the accuracy and completeness of the electoral register by providing them with access to a wider range of data sources to help identify people who are eligible to register but are not currently on the register and to confirm the relevant data. The evidence of effectiveness gathered through the data-matching schemes between EROs and public authorities will be assessed (by the Commission - which is under a statutory duty to carry out the assessments) and consideration will be given to how the benefits of the most effective schemes can be replicated or used more widely.

The Project will also support EROs in targeting under-represented groups to ensure the accuracy and completeness of the register throughout the transition towards the implementation of full IER (currently programmed for after 2015).

Local authorities were asked to bid to undertake the data-matching schemes and the successful applicants will enter into agreements to establish best working practices. Assessment criteria and timing will be agreed with the Commission.

5. Personal data to be used

The data that EROs need to access from public authorities is of two kinds:

- information about the location of individuals who are (or shortly will be) old enough to vote; and

[2] In England, only EROs appointed by Unitary Authorities have access to all of the council records for the area. In two-tier areas education records are not held by District Councils but by County Councils; EROs appointed by a District Council are therefore not able to access those records. There is an intention to take forward legislation to address this restriction.

- information about properties where eligible voters may be resident.

The provisions of the 2009 Act expressly allow the matching of data only for the purpose of enabling EROs to fulfil their registration duties, and this in turn limits the scope of the information that can be shared. Furthermore, the 2009 Act states that information provided to EROs may not be disclosed to any person other than one to whom the officer may delegate his or her functions (with exceptions for registration purposes and for legal proceedings).

Broadening the range of data that EROs could access beyond local authorities to other public authorities will have two potential benefits: it will provide EROs with a wider range of sources of data from which they can identify people not registered, or individuals who ought to be removed from the register; and it may assist in detecting fraudulent attempts at registration.

6. 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 proposed to electoral registration (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 will be destroyed following the conclusion of the pilot and no later than 31 December 2011.
Incorrect data from Public Authority	The action to be taken by the ERO in the event of incorrect data being received from the Public Authority will be determined according to the design of the particular pilot concerned.
Data received results in identification of fraudulent activity.	EROs are under an existing duty to pass concerns of fraudulent activity to the Police.

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

Risk Description	**Controls/Mitigation**
Data security breach – data is mishandled by either the ERO or the Public Authority.	- As part of their applications to take part in the pilots, EROs were required to demonstrate how they would ensure that electoral register data would be securely transmitted to the Public Authority and to confirm that data received would be securely held. - Ensure that information management arrangements are in

Risk Description	Controls/Mitigation
	place and are monitored. - Cabinet Office is working with EROs and Public Authorities to agree the most secure mechanism for transfer of data. The agreed approach will conform to HM Government IA Standard No. 6 (Protecting Personal Data and Managing Information Risk) and will be signed off as part of the Agreements which will be put in place prior to the data matching schemes commencing. - Every participating ERO will conduct its own PIA, in which it will address security issues/concerns. - Engage with ERO to determine processes and procedures for data handling issues. - Engage with suppliers of electoral services to determine processes and procedures for data handling issues.
Access to the data – data received by the ERO is handled by more than one person – i.e. unauthorised personnel or unauthorised external parties.	- As part of the application, the ERO was required to state who would be responsible for the data received from the Public Authority. - The agreement between the ERO and the Public Authority will specify the security classification of the data that will be received from the Public Authority. -
Access to the data – data received by the ERO is shared with other departments in the Local Authority - Data received is used for unauthorised purposes or shared inappropriately by EROs.	- Use of data received will be clearly defined in the agreements as to processing of data which will be put in place between EROs and Public Authorities prior to data matching commencing. - The agreement between the ERO and the Public Authority will require that the data be used solely for the purposes of the data matching pilot and not for any other purpose. - All data obtained from the Public Authority and not added to the electoral register will be securely destroyed.
Access to the data – data matching leads to the identity of an anonymously	- EROs to ensure that anonymous electors are omitted from the data

Risk Description	Controls/Mitigation
registered elector being disclosed.	sent to the Public Authority.
Storage of the data received – inadequate storage of the data could lead to loss.	- Storage measures had to be clearly set out in the application. - Ensure that storage has the appropriate access controls in place. The agreed approach will conform to HM Government IA Standard No. 6 and will be signed off as part of the Agreements which will be put in place prior to the data matching schemes commencing - Ensure that protection of information training is provided for canvassing and other staff that need to handle forms including matched data on follow-up visits.

The above identified issues and risks will be monitored as part of the Project's overall issues log and risk register.

7. Data Matching Scheme proposal

The legislation clearly sets out how EROs can use the data. The overall purpose of the data matching schemes is to enable EROs to carry out their registration duties. These are to ensure that individuals included on the electoral register are entitled to be there; that individuals who are entitled to be registered are on the register; and that any information held by the registration officer about electors is accurate.

These purposes are based very closely on provisions inserted into the Representation of the People Act 1983 by the Northern Ireland (Miscellaneous Provisions) Act 2006, which permit the Secretary of State to require public authorities to share data with the Chief Electoral Officer for Northern Ireland. This effectively entitles EROs to receive information that is relevant to the entitlement to register or assists them to use that data for that purpose –i.e. the details of individuals' residence; the location of residential properties which would allow for cross checking a different database (which could help to reduce the risk of electoral and financial fraud), and age data.

The 2009 Act allows for the establishment of a number of data-matching schemes to investigate how access to data held by the public authorities (which they currently cannot access) can assist EROs to improve and maintain their electoral register.

The data will only be shared between a specified ERO and specified data holder i.e. public authority. With this in mind, the process for the data – matching scheme would be as follows[3]:-

[3] See Appendix 2 – Flowchart for Data Matching Schemes

Stage One – Potential Data Holders

The initial stage involved identifying potential data holders and determining the viability of the data held for the purposes of the scheme. Discussions were also undertaken with the Information Commissioner's Office (ICO) and efforts made to ensure that data protection principles were built into the data matching scheme.

Stage Two – Application process

This stage included issuing a prospectus to local authorities. Interested EROs submitted applications to carry out data matching with one or more viable data holder. The applicants were asked to consider requirements to:-

- demonstrate the feasibility of delivering the scheme successfully;
- demonstrate an understanding of the risks and issues associated with the scheme and how these would be addressed;
- demonstrate an understanding of the contingencies needed – particularly to protect the security and integrity of the data;
- have a clear and comprehensive communications plan covering all stakeholders;
- include project planning and management arrangements, including availability of staff on completion of the scheme to contribute to the evaluation process;
- set out plans for management of service suppliers;
- ensure that appropriate data handling and management safeguards were in place; and
- demonstrate that a PIA had been conducted on their proposal.

The Minister for Political and Constitutional Reform on behalf of the Lord President considered each application after its assessment by Cabinet Office officials against the criteria as set out in the prospectus.

Stage Three – Application approved

The Minister for Political and Constitutional Reform on behalf of the Lord President after consulting others, has laid an order authorising public authorities to provide the data.

In deciding to lay the order, the Minister for Political and Constitutional Reform on behalf of the Lord President has taken into account the justification for the project, compliance with the data protection principles and the outcome of consultations undertaken with relevant groups, which have included the ICO, the Electoral Commission and civil society groups with a particular interest in civil liberties, privacy, the use of information and data protection.

The discussions at stage one with potential data holders included the process for exchanging data between the ERO and the Public Authority. The process is outlined below.

Stage One – ERO to transfer Electoral Register to the Public Authority (or Public Authority to extract and send data to ERO)

It is envisaged that in most instances the ERO will securely transfer the Electoral Register, or such section(s) of it as are to be included in the data matching scheme, to the Public Authority.

The Public Authority will compare its data with the electoral register, using the data sets and the fields specified in the Schedule to the Electoral Registration Data Schemes Order 2011, to establish successful matches, uncertain matches and unsuccessful matches. The outcome of the data matching process will form an Exception Report which will be securely transferred back to the ERO.

In some exceptional cases the process may operate the other way round, with the Public Authority extracting and sending data to the ERO so that the ERO may undertake the matching. In that event, the Public Authority will extract data only for the relevant local authority area as stated in the Order that:-

(a) Only relevant data (name, address, and Date of Birth) is provided; and (b) ensuring that only data relating to that geographical area is provided.

The Public Authority will:-

- transfer the data to the ERO - via an appropriate, secure method
- only be allowed to transfer data of relevance to the request
- be required to extract and transfer the data securely. (Details of how this will be undertaken will be provided for in each individual PIA).

Stage Two – ERO receives and processes exception reports

The ERO will receive the exception report from each Public Authority whose data they wish to use in the data matching exercise.

The ERO will establish:-

(a) where records do not match, and

(b) individuals who are not yet registered.

(For (a) this may involve software and/or staff time if checks are done manually. For (b), it may involve letters or door to door calls).

The ERO will be required to have secure storage arrangements[4] in place for the data, similar to the security for the register itself or the Council Tax register, since the data it will contain will be similar. The data will be obtained and used only for specified and lawful purposes and will be kept no longer than necessary and destroyed as soon as possible after the end of data sharing on 30 November 2011.

8. 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 that is provided for by the 2009 Act will not involve the transfer of any personal data other than Name, Address and Age or 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. This process takes place on an annual basis (during the 'annual canvass', which usually takes place in the autumn).

Individuals who do not wish to be on the electoral register are still required by law to fill in the annual canvass form accurately. There is no option to opt out from registration for those eligible to vote. Consequently, these provisions do not have any 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, where a household has not provided accurate information.

[4] This should be detailed in the application for the data – matching scheme.

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) by the ERO, 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 agreements stipulated by the Order.

9. Consultation and general communications activity

Consultation formed an intrinsic part of the development of the provisions of the 2009 Act. Informal consultation was carried with a range of stakeholders including:

- The Association of Electoral Administrators (AEA) and the Electoral Commission (EC) (both parties agree that the further steps to bolster the register are needed and beneficial).

- Various Public Authorities, such as Her Majesty's Revenue & Customs (HMRC), Driver and Vehicle Licensing Agency (DVLA), Department of Health, TV Licensing, Land Registry, and Department for Work & Pensions (DWP).

- Third sector organizations, such as Help the Aged, Unlock Democracy, Police State UK, Liberty, and the Citizenship Foundation.

There is ongoing communication between the Cabinet Office and these and other stakeholders with a particular interest in civil liberties, privacy, the use of information and data protection, and that will continue as the policy develops further.

In addition, consultations focusing specifically on data protection and privacy issues have taken place with the ICO.

10. Conclusion

Participating in the data – matching scheme is likely to benefit EROs in a number of ways. It will improve the accuracy and completeness of their electoral register. In improving the accuracy of the electoral register, it will in turn improve public confidence in the register and therefore promote a healthy democratic system. It will certainly enable EROs to test whether access to a particular database will help to improve registration in their area. The purpose of the schemes is to test new data sets that EROs cannot currently access, in order to inform the Government's understanding of their usefulness in enhancing electoral registration.

It is important to reiterate that 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.

Appendix 1

Political Parties and Elections Act 2009 (the 2009 Act)

Sections 35 and 36 of the 2009 Act

Sections 35 and 36 of the 2009 Act provide a power for the Secretary of State to make an Order, which will establish a scheme requiring specified public or local authorities to provide specified registration officers with information for the purpose of fulfilling their registration duties. The provisions allow a single order to include more than one "scheme" (avoiding the need for multiple orders to cover, say, 4 EROs and one public authority). Section 35(10) of the 2009 Act provides for the Orders to be made under the affirmative resolution procedure. Under this procedure, secondary legislation is laid before Parliament in draft or when made, but can only take effect when approved by affirmative resolutions in each House following a debate.

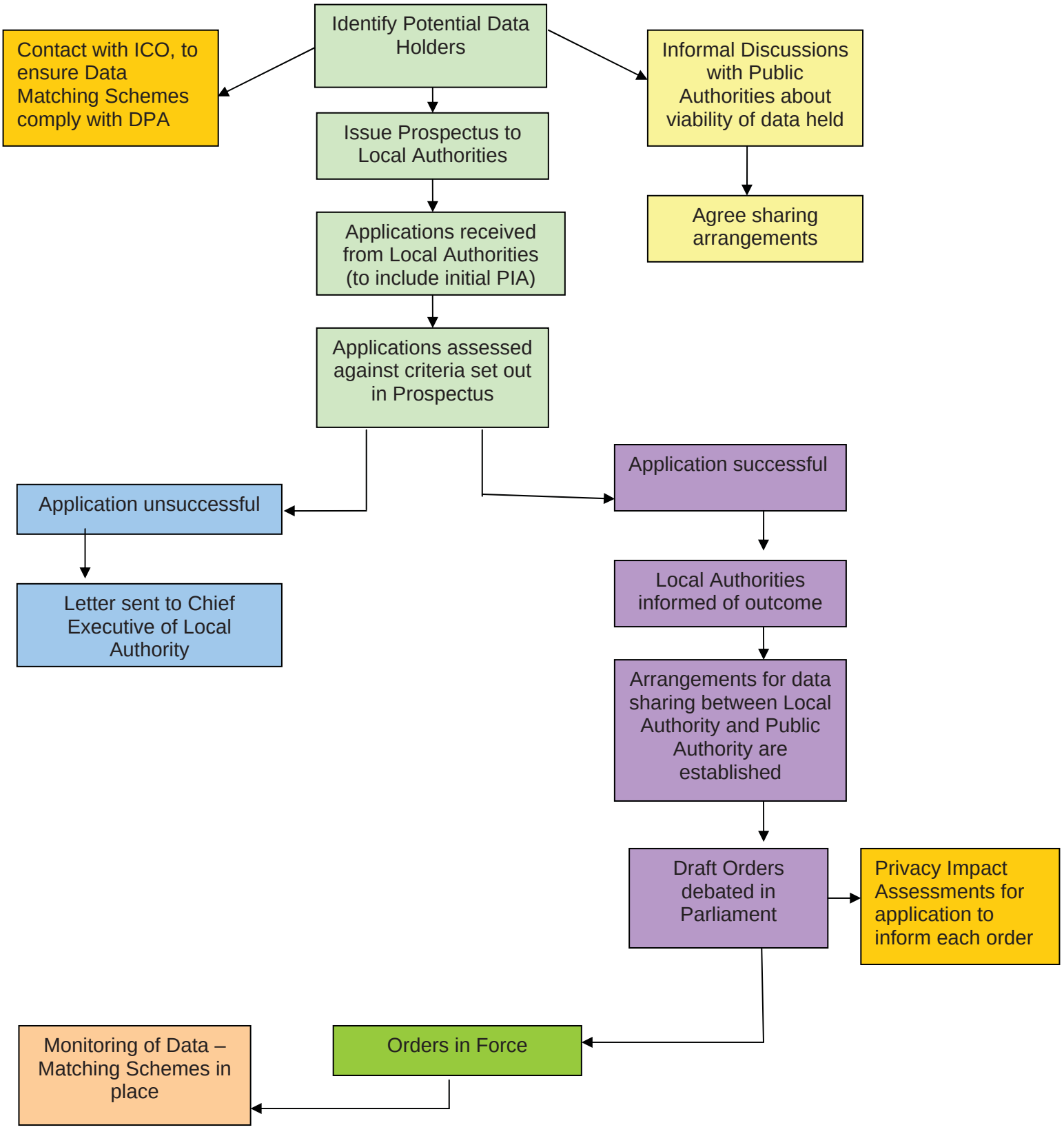
The provisions also set out a number of procedural safeguards on the use of the power. An Order putting a scheme in place can only be made where the scheme has been submitted to the Secretary of State by a registration officer and is being implemented unamended or with amendments agreed by that registration officer. Further, before making an order the Secretary of State is required to consult (a) the Electoral Commission; (b) the Information Commissioner; and (c) any public authority required to provide information under a scheme. The duty to consult the Electoral Commission is modelled on the provisions of the Political Parties, Elections and Referendums Act 2000; the requirement to consult the Information Commissioner is additional.

The provisions expressly provide for the effect of each order to be evaluated by the Electoral Commission which has a statutory duty to evaluate and report on any pilot scheme approved by the Secretary of State. Additionally, Section 36 (4) and (5) of the 2009 Act sets out the criteria for the report. These provisions ensure that lessons are learned from each pilot, and they have been modelled on the Representation of the People's Act 2000 piloting provisions. The provisions also propose the following minimum criteria for the Commission's evaluations:

- the extent to which the scheme has supported the ERO in fulfilling their registration duties;
- whether and how much opposition there was to the scheme;
- how easy it was to administer;
- whether it resulted in cost or time savings; and
- the extent to which the scheme prevented or contributed to the commission of offences under electoral law, or other malpractice.

Appendix 2

Flowchart for Data Matching Schemes



Annex C

It should be noted that this letter relates to a previous version of the Order. With reference to the fourth paragraph, data relating to the nationality of drivers is not held by the Driver and Vehicle Licensing Agency and consequently will not be among the data to be supplied by the Agency. Furthermore, given that the proportion of service personnel without franchise to vote on the grounds of nationality is less than one per cent, the Cabinet Office has decided not to request this information from the MoD.

ico.
Information Commissioner's Office

Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524510 www.ico.gov.uk

Our Ref: DAS/SMcC/AJR

Mr Mark Hughes
Registration Improvements Project Director
Electoral Registration Transformation Programme

22 February 2011

Via e-mail (only)

Dear Mr Hughes,

Thank you for your letter, dated 18 February 2011, constituting formal consultation with the Information Commissioner on the content of the Electoral Data Schemes Order 2011. You mention that you have been working closely with Stephen McCartney from this office during the development of the Draft Statutory Instrument and he has briefed me so that I can provide a full response on behalf of the Commissioner.

The creation of a statutory gateway for the provision of the necessary data by an authority to the registration officer goes a long way to delivering compliance with the requirements of the Data Protection Act 1998. It ensures such data sharing is lawful and is likely to satisfy at least one of the conditions in Schedule 2 of the Data Protection Act. It is also welcome that Clause 6 of the Draft Statutory Instrument does not allow data sharing schemes to proceed unless an agreement is in place that details requirements as to the processing of data, including requirements as to the transfer, storage, destruction and security of data.

One of the main concerns we have about these schemes is that data must be transferred in a manner that is secure. I understand that some of the authorities named in the Statutory Instrument, such as the Department of Work and Pensions, will not simply provide the relevant data in isolation, but will require the registration officer to send them data sets that they will then screen against their own data. They will then return these data sets to the registration officer, along with any additional data they have identified. It is vital that all parties understand that there are inherent risks to transferring large personal data sets between authorities and that they take appropriate technical and organisational measures to ensure that the data is kept securely at all

ico.
Information Commissioner's Office

stages, including during transfers. I am sure that you will understand that should data losses occur, we will investigate the circumstance and, if justified, take appropriate regulatory action against the specific registration officers and/or authorities concerned.

Another concern is over how far it is necessary to share all of the data in each of the data sets. In most of the schemes detailed in the Schedule to the Statutory Instrument the data being provided includes the names, addresses and dates of birth of individuals. However, in some cases, in particular those where data sets are being requested from the Driver and Vehicle Licensing Agency or the Ministry of Defence, the nationality of individuals will also be disclosed. The third data protection principle states that personal data shall be adequate, relevant and not excessive in relation to the purpose or purposes for which they are processed. I am aware that each of the schemes has a slightly different purpose. Some are designed to highlight under-representation on the electoral register by specific groups, some are looking at identifying under-representation on the register more generally. While we do not want to raise an objection to the Statutory Instrument being laid in its current form, we would expect that the evaluation of the schemes will examine which of the data sets were relevant to increasing registration and which were excessive in that they did not significantly contribute to this aim.

Of course, staff from the Information Commissioner's Office will continue to be available to provide help and advice on the evaluation process.

Finally, I would like to thank you for involving the Information Commissioner's Office at a very early stage in the development of the schemes and for our inviting staff to speak about privacy impact assessments at the launch event for the data matching schemes.

Should you have any questions or comments on this response, please do not hesitate to contact me.

Yours sincerely,

David Smith
Deputy Commissioner and Director of Data Protection