



## **Government's proposals on Individual Electoral Registration in Great Britain Response to PCRC Call for Evidence from EURIM (The Information Society Alliance)**

### **Introduction**

EURIM ([www.eurim.org.uk](http://www.eurim.org.uk)) is a cross-party, pan-industry policy research group concerned with the formation and scrutiny of legislation, regulation and government initiatives related to UK/EU competitiveness in the global information society and to the effective use of technology to serve society as a whole. It uses funding from its corporate and associate members to organise working groups of politicians, advisors, officials, industry, professional bodies, trade associations and interest groups. By seeking consensus and focusing on IT governance and security of information, EURIM's Information and Identity Governance Group fosters an understanding of, and highlights good practice in, information management across borders, regulations and cultures.

EURIM welcomes the work of the present and last governments in aiming for an improvement in the accuracy and completeness of the electoral rolls in the UK to increase registration and reduce fraud.

### **Implementation of Individual Electoral Registration – Findings from Overseas Research**

1. We believe that the recent study on the mechanics of electoral registration systems overseas by a EURIM working group on Information Governance has important lessons for the UK regarding their use of technology and approaches towards the two key measures of an electoral register: completeness and accuracy<sup>1</sup>. The report, Implementation of Individual Electoral Registration – Findings from Overseas Research, is available at: [http://www.eurim.org.uk/activities/ig/1103-IVR\\_LessonsFromOverseas.pdf](http://www.eurim.org.uk/activities/ig/1103-IVR_LessonsFromOverseas.pdf).
2. An A4 summary version with conclusions and recommendations is also available ([http://www.eurim.org.uk/activities/ig/1103-IVR\\_LessonsFromOverseas\\_Summary.pdf](http://www.eurim.org.uk/activities/ig/1103-IVR_LessonsFromOverseas_Summary.pdf)), parts of this were referenced in the Standard Note entitled 'Individual Voter Registration' issued by the House of Commons Library (<http://www.parliament.uk/briefing-papers/SN05995>).
3. EURIM's main findings concern:
  - the technical means of holding and transferring personal data between different authorities,
  - how to transfer data securely,
  - how to store data in a way consistent with privacy requirements,
  - how current or emerging technology might help facilitate:
    - i. individuals' access to their electoral registration data;
    - ii. the process of applying to be registered;
    - iii. updating information (e.g. change of address);
    - iv. ensuring information held by an Electoral Registration Officer is accurate.
4. Two distinct trends are discernible in the responses from overseas between those countries which treat the electoral register almost exclusively for electoral purposes ('Commonwealth'

---

<sup>1</sup> Accuracy refers to the registration being that of a true identity exercising a legitimate right to vote. Completeness refers to the register having on it the maximum number of eligible people in the district.

or 'common law' heritage), and those that create a multi-purpose population register, either at national or municipal level ('continental' heritage).

5. All sampled common law and continental countries require proof of identity to register the voter; only the UK does not. However, only 3 out of 7 sample countries require the voter to prove identity at the polling station. This may leave open the possibility of fraudulent voting by means of personation, where an individual is legitimately registered, but his or her vote is cast by an impostor.
6. Compulsory registration does not work unless underpinned by other processes: e.g. in Australia large numbers of voters may remain unregistered.
7. Countries that operate data matching to maintain a population register, to transfer data with other public bodies, or that allow citizens to view or amend their personal data, do so through secured systems.

### **Conclusions and Recommendations**

1. Compared with many countries, the UK's system is overdue for an overhaul. Any system of electoral registration should ensure that all personal data is properly managed and protected, and must be practical, conducive to improvements in registration levels and accuracy, and consistent with UK political tradition and culture.
2. In the UK, no proof of identity is required for registration; the voter asserts his or her own identity and the name and address are checked off by polling station staff against the roll, increasing the risk of impersonation. However, balancing the need for ID verification (by data sharing and matching etc.) with resistance to any kind of central database of personal information presents a significant challenge. This has implications for data retention where verification of identity is used to retrospectively check for fraud.
3. We note that HMG plans to support the roll out of other channels (e.g. telephone or online) for registration, and will explore the scope for integrating electoral registration into other services. When/if online registration is implemented, the use of digital certificates by a registering elector should be the norm.
4. Data matching or data sharing with other public bodies, online or offline, should be done securely, comply with data privacy laws, and be covered by formal agreements.
5. The Government should consider the advantages or otherwise of data matching with private sector databases.
6. For expatriate electors, the Government might consider using the Foreign and Commonwealth Office's consular facilities to encourage and facilitate registration overseas.
7. ISO 27001 should be adopted in as an information security management system standard.
8. Key issues to be addressed include the timetable for change: concerns about technical issues include the funding of a new system with heavy transitional costs e.g. establishing the interface for access to DWP records for the NINO. This is a major change that cannot be accomplished cheaply; central funding should be ring-fenced.

### **Current and Future Activity**

1. The EURIM members who organised the previous exercise are happy to consider undertaking further work in this area. For example, the Government has announced an interest in developing a market for competing service providers in this field, is keen to look at how IT and online processes can support the registration process, and how digital identity assurance might be used to verify an application to join the register. It has been suggested that it is possible to help drive efficiencies by linking programmes to encourage registration with transactions that update other publicly held personal information. The idea is superficially attractive but raises many issues, including of the "function creep" that has been a common problem with ID systems around the world, not just in the UK. It also raises issues of data and

2. EURIM met with Cabinet Office officials on 28th July 2011 to explore whether our members can provide industry assistance with data matching and established identity assurance systems for electoral registration in future. The private sector, not just the credit reference agencies but the financial sector data transfer and trust networks (designed to quantify and pre-define liabilities around the use of eIDs issued by trusted parties to end users and relied upon by other parties) together with the various fixed and mobile communications and online communities and their customer identification services, may be able to assist in improving the quality and integrity of the electoral register. They may also be able to advise on how to build secure and sustainable systems, ensure interoperable frameworks and standards, and promote rationalisation etc.
3. EURIM notes that while the Organisation for Security and Co-operation has recommended that "Consideration should be given to introducing an identification requirement for voters when applying for registration as a safeguard against fraudulent registration", HMG's current intention to remove the requirement for a signature in identity verification is necessary for multi-channel registration (e.g. telephone, online). HMG maintains that the requirement does not add any significant security to an application nor is there the facility to verify the authenticity of the signature. However the legislation retains the option for a signature to be prescribed in regulations. EURIM notes that dropping this requirement will enable registrations to be made through new channels such as online or by telephone, but these need to be supported by appropriate identity assurance, including in future digitally, to verify applications to the electoral register.
4. HMG envisages that *"evidence of a connection between an individual and an address should be established either by an individual responding to a direct invitation by an ERO which has been sent to a known address (for example via the current canvass process), or where an unsolicited application takes place (for example online), by the ERO seeking confirmation of registration by writing to the individual at their address"*. HMG notes that it may be possible to dispense with this stage if verification of address can be carried out by other means.
5. EURIM is considering conducting a survey of its corporate and associate members specifically on Identity Assurance to identify concrete operational industry experiences in this field.