

# Privacy Impact Assessment Report Citizen Account

**Produced By: Cameron Walker / Carol Peters**

**Date: 3<sup>rd</sup> November 2008**

## **1. Project Description**

Customer First is a Scottish Government sponsored programme developed in partnership with Scottish local authorities and managed, with the support of SOLACE, under the direction of the Improvement Service.

The infrastructure that will support Customer First (The National Infrastructure) consists of a number of national business applications. This assessment focuses on the first application, the Citizen Account which is aimed at making citizen interaction with the public sector an easier and more joined-up experience.

## **2. Issues Register**

9 issues are outstanding. Risk Levels are identified as 1 x critical, 5 x High, 1 x medium and 2 x low. Most are associated with a lack of policy or procedure. The critical priority is due to a lack of a defined governance model for the Customer First management of the National Infrastructure in general.

## **3. Business Case for Intrusion & Implications**

Customers choose whether or not to register and for what services. The impact on privacy is nominal. In addition, the Citizen Account processes only the basic details necessary for the purposes of registration and generally widely available in the public domain eg., name, address.

The following legislative powers were identified as support for processing:

1. Person data is captured under the legal powers given to the Registrar General (the data controller) under the [Local Electoral Administration and Registration Services \(Scotland\) Act 2006](#) (LEARS Act).
2. Application data and address data is processed under the legal powers given to Scottish Local Authorities by the Powers: S69 of the Local Government (Scotland) Act 1973
3. Future extension of the Citizen's Account to the wider public sector would be underpinned by the Community Planning duties defined in the Local Government in Scotland Act 2003.
4. Privacy was considered in discussion with the ICO and OSSE and it was agreed that the Citizen's Account (in its current form) would comply with the Human Rights Act.

## **4. Alternatives Considered & Rationale behind Decision**

The major objectives of this project are: (i) to provide citizens with secure/authenticated access to a range of online public services; (ii) to provide customer services staff with accurate customer data to help them deliver efficient/joined-up services; and (iii) to allow citizens secure access to their own data and to be able to manage/notify changes to that data.

The only other viable alternative would be for each authority to provide the same locally on their own website. Whilst this would allow citizens to access public services online, it doesn't simplify interaction with local government services or facilitate notification of a change of personal details across other local authorities or public services.

## **5. Description of Privacy Design Features**

The data captured at application time is the minimum required to validate the person and his/her address and, with the exception of the Date of Birth, is freely available from other public domain sources. As customers choose whether or not to register, and for what services, the impact on privacy is nominal.

Customer accounts are only set up with the informed consent of the citizen to the data sharing involved. Citizens can remove (or add) consent at any time. The consent model allows for flexible development of consents in relation to either services or service providers. Security is comparable with the current standards deployed within the Financial Sector, and is capable of being configured to comply with the current UK Government Protective Marking Scheme.

All security measures will be considered and defined in accordance with best practice and ISO27002. A third party has been contracted to provide a 24 Hour monitoring, reporting and management service for the security infrastructure.

## **6. Analysis of public acceptability of scheme & applications**

A restricted pilot by members of the public will be held prior to going live, to determine public perceptions of the new system and its security and how it improves their interaction with public services.

## **7. Conclusion**

No legal or ethical restrictions to processing personal data on the Citizens account were identified and all Data Protection Act obligations have been met or are planned. Pending completion of information security policies and standards, there are no reasons why the system cannot become operational.