Privacy Impact Assessment

On The use of RSA Driving Licence Data to invite PPSN holders to use this data to register for a Public Services Card

An Individual's right to privacy is protected under Irish legislation by the Data Protection Acts 1988 and 2003 and within article 8 of the European Human Rights Act. A Privacy Impact (PIA) Assessment involves evaluation of the privacy implications of projects and assessment of their compliance with relevant legislation. Where potential risks are identified, it should be possible, in consultation with stakeholders, to identify controls and safeguards to mitigate or reduce these risks without impacting on the realisation of the benefits of the initiative or project under assessment.

1. Initial Assessment

Background

The RSA is listed as a specified body under Section 262 of the Social Welfare Act 2005 for the use of the Public Service Identity (PSI) dataset, which includes the Personal Public Service (PPS) Number, in a transaction with an individual.

Since October 2013, all applications for a driving licence have included an in-person interview where a photograph is taken of the applicant and their identity is authenticated. This authentication involves the partial update of (PSI) data during the transaction but does not take details of the birth surname of the applicant's mother nor does it include a full verification of their date of birth.

The DSP is responsible for providing a range of identity management functions and services internally to the Department of Social Protection and to other public bodies. It issues and manages the Personal Public Services (PPS) Number and provides related data matching services to over 100 public bodies as specified for in legislation. As Data Controller, the DSP is obligated to ensure as far as is possible that the data it hold is accurate, complete and up to date.

Subsection (5) of Section 262 provides that, where a specified body collects from a person any of his/her PSI data, that information shall also be collected for the purpose of maintaining the person's public service identity.

The (DSP) is proposing to request from the RSA, PSI data collected via the drivers licence application process and to write to individuals who have renewed their driving licence since March 2014, inviting them to register for a Public Services Card (PSC) by providing their consent to use the photograph taken during their transaction with the Road Safety Authority (RSA), and answering some additional security questions.

Privacy Issues

The information collected by the RSA was for the purpose of providing a driving license.

This project proposes to use that information for a different purpose - to maintain the individual's PSI and to complete the registration process for a PSC.

CIS will be using data provided by the RSA to trigger this invitation to register. The individual may not have **knowingly** provided their consent for the information associated with the driving licence transaction to be shared with the DSP.

The data that will be shared will be PSI data[1]. This is the normal data legally held and shared with specified public bodies by the DSP and will be transferred using Secure File Transfer Protocols and will be subject to security measures to defend and prevent any breaches of security as deployed by both the RSA and the DSP.The provision of secure computing systems is a key principle for the operations of DSP's Information Systems Division (ISD). The Department recognises that specific ICT measures are an important part of an overall strategy to protect strategic systems from failure. The security of the Department's ICT infrastructure is addressed at many levels and detailed in the ICT strategy.

ISD works in association with Business Information Security Unit (which has overall responsibility for information security policy) and Facilities Management Unit (which is responsible for physical access to buildings including the data centres), to ensure the security of the Department's systems

Risk Assessment

What are the privacy risks?

1. The primary risk identified is the intrusion of person by sending a letter triggered by the driving licence data set.
2. Possible breach of DP Act as consent may not have been knowingly given by the individual when applying for a driving licence to share this information with the DSP.

[1] Section 262 of the Social Welfare Consolidation Act 2005, provides that "public service identity", in relation to a person, means the person's personal public service number and his/her; surname; forename; date of birth; place of birth; sex; all former surnames (if any); all former surnames (if any) of his or her mother; address; nationality; date of death; certificate of death, where relevant; a photograph of the person, other than in the case of a deceased person; the person's signature, other than in the case of a deceased person; any other information as may be required for authentication purposes that is uniquely linked to or is capable of identifying that person; any other information that may be prescribed which, in the opinion of the Minister, is relevant to and necessary for the allocation of a personal public service number.

How are those risks identified?

Change of purpose - the original data provided by the individual is being used to extend an invitation to them to update their PSI data with DSP and to register for a PSC, not to renew a driving license.

Asses the risk

The element of the project giving rise to the risk is the decision to use RSA data shared with the DSP to determine the suitability of the individual for remote registration by data matching against the PSI data already held by the DSP. This derived data will then be used to write to the client inviting them to provide consent to proceed to use data (photograph taken at an in-person interview with the RSA) to produce a PSC.

The **purpose** of this element is to identify clients that are suitable for this method of registration.

The **benefits** of this element are to provide accurate details of the holders of PPS Numbers so as to ensure that a PSC registration can be completed. Individuals will **benefit** by using the information already provided to the RSA to register for a PSC and thereby save on duplication of effort.

This will **benefit** the individual by saving them from having to attend in person at a SAFE station at a later date and therefore enable the efficient and effective delivery of public services.

This element will benefit the DSP and the client through saving time and financial resources.

The only **alternative** is to allow the client to attend in person to register for a PSC as and when they are invited to attend or as and when they need a PSC to access public services.

The potential impact on privacy to the individual is the change of purpose of the driving license renewal data and the uninvited letter of invitation to register for a PSC.

The likelihood of an individual taking exception to the invitation is slight as they did provide their PPS Number and PSI data for the transaction with the RSA to renew their driving license and the RSA provided on-line forms for this renewal advise that this information may be shared through the following -

Public Service Identity data collected on this form/provided by you may be used to maintain/authenticate your Public Service Identity, under Section 262(5) of the Social Welfare Consolidation Act2005 (as amended). Only your Public Service Identity data may be shared with other public bodies under this provision.

How are privacy risks resolved?

The risk is acceptable as the benefits to the individual outweigh risks related to an intrusion to their personal privacy and the legal basis for sharing this data should and may have already been clear to the individual when they renewed their driving license.

The risk will be partially avoided by the inclusion of a consent box on the letter asking the individual for their permission to use the RSA data.

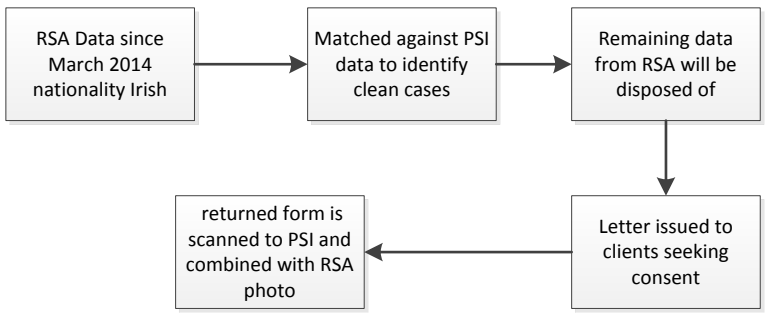
The only data that will be shared by the RSA with the DSP will be PSI data. This is data which the DSP already holds for each holder of a PPS Number. The DSP has an obligation to ensure that this data is up to date accurate and complete. The act of writing to the individual will provide the individual with an opportunity to ensure that their PSI data is correct and complete.

PIA Decision

The level of risk is considered justified taking into account the increasing benefits that will accrue to the individual by having a PSC and the future need for a PSC to engage fully with public services

3. Planning

Information flows



Project Team

DSP CIS - Linda O'Connor, John Maguire, Geraldine McGourty, Monaghan PSC Back Office

DSP IS Services - Conor Ryan, Denise Murphy

Stakeholders

RSA, RSA Clients, CIS – Card Management, CIS Control

4. Consult and gather information

Internal and External Consultation

CIS senior management, IS Services, Legislation, BISU and RSA.

The project was discussed, planned and considered in depth by the management team in CIS and presented at ASec level. The project was discussed with PO in BISU and advice sought from our legal advisor. The process was discussed in depth with the IS Services team. This project builds on on-going discussions that have been held with the RSA since 2011 where PSC related data sharing proposals have been considered.

The concern highlighted by the legal advice was that the trigger of writing to the clients is derived from RSA renewal data without the **explicit** consent of the individual, even though the legal basis for data sharing may be clear.

A data sharing Memorandum of Agreement (MOA) was agreed with the RSA and is now in place between the DSP and the Department of Transport, Tourism and Sport (DTTaS) who is the data processor for the RSA.

The methods used to transfer and process the data are similar to the method in place to transfer and process Passport Office data in an earlier similar project. Secure File Transfer Protocol (SFTP) is deployed to ensure security of transfer of data. These methods were discussed and planned in detail with the IS services support team to CIS. Test files have been exchanged to ensure that all security protocols and procedures are fit for purpose.

Other Information

This is very similar to a project that was conducted using information provided by the Passport Office to invite customers of the Department who were the holders of a passport to use this information to register for a PSC. Consultations with the ODPC for that project resulted in the inclusion of a consent box to allow the data to be used. The use of that consent box will be included in this current project which differs only in that the customers of the RSA may not be scheme clients of the DSP, although

they are holders of a PPS Number which is issued and maintained by Client Identity Services in the DSP. Public reaction to the data sharing in the original Passport Office project was positive.

Confidentiality Concerns

The MOA between the DSP and DTTaS acting as data processor for the RSA addresses these concerns.

5. Compliance review

Legal Issues

Legislative Basis for Sharing Data in Social Welfare Legislation

The Social Welfare Consolidation Act 2005 provides a legislative basis for the transfer of data as under section 262 of the SWCA 2005 (as amended) which provides for the use, maintenance and sharing of the Public Service Identity (PSI) dataset which includes, inter alia, a person's photograph. It should be noted that Section 262 provides that PSI data can only be used by public bodies specified in Schedule 5 to the Act. Both the DSP and the RSA are Specified Bodies.

The legal basis for the processing of the data is the DP Acts 1988 & 2003 which provide that:

"2A (1) Personal data shall not be processed by a data controller unless section 2 of this Act (as amended by the Act of 2003) is complied with by the data controller and at least one of the following conditions is met:

(a) the data subject has given his or her consent to the processing .....and the giving of such consent is not prohibited by law….

(c) the processing is necessary …

(h) *"made at the request or with the consent of the data subject or to a person acting on his behalf"*

(iii) for the performance of a function of the Government or a Minister of the Government,

(iv) for the performance of any other function of a public nature performed in the public interest by a person. "

6. Analysis and solutions

The legal basis for the data sharing is highlighted in section 265 (1) of the Social Welfare Consolidated act 2005, where by the transaction is the proposed registration for a PSC.

The consent of the individual for the data sharing, as required under section 2A (a) of the DPA, can be implied for a percentage of cases through the on line form notification provided by the RSA, and where not explicit, it will be sought through the communication seeking consent from the individual to proceed. The implicit necessity of the processing of the data as required under the DPA 2 A(b) can be taken by the roll out of new public services that require a PSC to engage with.

Risk Assessment

The element of the project giving rise to the risk is the decision to use RSA data to determine the suitability of the individual for remote registration by data matching against the PSI data already held by the DSP. This derived data will then be used to write to the client inviting them to provide consent to proceed to use data (photograph taken at an in person interview with the RSA) to produce a PSC.

The **purpose** of this element is to identify clients that are suitable for this method of registration.

The **benefits** of this element are to provide accurate details of the holders of PPS Numbers so as ensure that a PSC registration can be completed remotely.

Individuals will **benefit** by using the information already provided to the RSA to register for a PSC.

This will **benefit** the individual by saving them from having to attend in person at a SAFE station at a later date and therefore enable the efficient and effective delivery of public services.

The full engagement and consent of the individual will allow for the accurate and complete update of the PSI data held in CIS as required under the Data Protection Acts.

This element will benefit the DSP and the client through saving time and financial resources.

The only **alternative** is to allow the client to attend in person to register for a PSC as and when they are invited to attend or as and when they need a PSC to access public services.

The potential impact on privacy to the individual is the change of purpose of the driving license renewal data and the uninvited letter of invitation to register for a PSC.

The likelihood of an individual taking exception to the invitation is slight as they did provide their PPS Number and PSI data for the transaction with the RSA to renew their driving license and the RSA provided on-line forms for this renewal advise that this information may be shared-

Public Service Identity data collected on this form/provided by you may be used to maintain/authenticate your Public Service Identity, under Section 262(5) of the Social Welfare Consolidation Act 2005 (as amended). Only your Public Service Identity data may be shared with other public bodies under this provision.

The level of risk is considered justified taking into account the increasing benefits that will accrue to the individual by having a PSC and the future need for a PSC to engage fully with public services.

Solutions

A consent box will be included in the letter that will issue seeking explicit consent to use the data.

Any records that are not suitable for use will be deleted and this process will be validated.

The remaining data will be held for as long as is strictly necessary and not beyond 18 months.

The RSA data will be stored on a BOMi database with access limited to a limited number of key DSP personnel. The process business rules will require that all records over 18 months from date of receipt and records deemed as unsuitable will be deleted. The date of deletion and the number of deleted records will be maintained. The deletions will be run as the stored procedure on the database; only a limited number of officers with access to execute procedures in this environment will be able to do so. The deleted records will be capable of restoration for three months after deletion. Once the three months have elapsed they will be permanently deleted.

Privacy Design Features

The project will be subject to the governance and business information security protocols of the DSP that are applicable to all PPS number and PSI data sources.

In addition;

RSA data that does not suitably match the PSI data held by DSP will be discarded.

Consent will be sought from each individual prior to utilising the RSA photograph

Clients who do not respond to the communication with consent will have their RSA sourced data deleted within 18 months of initial communication

7. Implement and review

This project will be implemented from June 2017 and reviewed in June 2018, or sooner depending on responses received from clients.