Privacy Impact Assessment: Threshold check

Facial Recognition System

30 January 2020

Internal Affairs
Te Tari Taiwhenua

New Zealand Government

Contents

Introduction and overview of approach

Include a brief description of the proposed project or initiative.

DIA's current Passport Facial Recognition System (ABIS) is being replaced with a new facial recognition solution that will be delivered 'as a Service', Facial Recognition as a Service (FRaaS). The system will be integrated with the passport system to continue supporting process automation and fraud detection, with the goal of increasing productivity of passport issuances whilst maintaining the current integrity of the New Zealand passport.

Describe any existing systems or processes, and the main changes that are proposed:

The new FRaaS (highlighted in green in Figure 1) will replace ABIS (highlighted in grey) and will be delivered as a Managed Service by DXC Technology, hosted and managed within New Zealand. The Service will be hosted in 9(2)(k) data centres. The FRaaS Security monitoring and logging data only (which does not contain any personal identifiable information) will be transferred offshore to Australia as part of the security management and monitoring of the FRS.

9(2)(k)

a) **Describe the purpose of the change, including any projected benefits to your business or to the individuals affected**

The new service will include new hardware and software that will increase performance and accuracy of the biometric matching.

The business outcome for Facial Recognition Service (FRS) project is to deliver a fit for purpose and supported Facial Recognition Solution that will increase productivity, reduce cost and extend the capability across and beyond SDO branch.

b) **Identify the main stakeholders or entities involved, and their role in the initiative.**
The main stakeholder is the Deputy Director Service Delivery & Operations; who is responsible for ensuring that the value (high trust) and integrity is maintained in the New Zealand passports. Benefits to the wider public resulting from the power of the New Zealand passport include visa free travel to a large number of countries. https://www.passportindex.org/byRank.php

Describe the personal information that the initiative will involve. Note: "Personal information" is any information about an identifiable living person. However, a person doesn't have to be named in the information to be identifiable. You only need to complete a Threshold Assessment if your proposal involves personal information.

The description should cover:

a) **What is the source of the information? (e.g. collected from the individual, re-use of existing information)**
b) **What is the purpose of the information for the initiative?**

The Facial Recognition Service will hold biometric templates of all youth and adults from the age of 11 who have applied for a NZ passport. The templates are derived from images (photographs) that are submitted with a passport application. The conversion process uses an algorithm from a biometric vendor to create a unique biometric template for every image converted. This process creates a database of approximately 4.5 million templates against which biometric matches and searches can take place.

The following data, sourced from the Passports Systems, will be sent to the Facial Recognition Services, to be associated with each main gallery image to be enrolled and saved against the corresponding template:

Transaction data:

- Image ID

Biographic data

- Identified gender
- Age at time of capture (calculated from application received date and date of birth)
- Place of birth
- Country of birth
- Image capture date (date application is received)

Raw data:

- Image

FRaaS data is stored in relational database and logically partitioned by participating agency. There are multiple databases to serve the logical components:

- Image blob database - dedicated image storage that contains all facial images submitted by an agency during the enrolment process.
- Biometric database - contains all extracted biometric templates
- Service Bus Database - System internal database that controls the operations of the service
- Reporting database - contains all report definitions for standard FRaaS reporting capabilities

Service calls to the FRaaS API will be authenticated using mutual TLS and each participating agency will only be granted access and connectivity to a FRaaS Instance where they have a valid and associated Agency ID. After client certificate authentication is performed, a match will be performed to ensure that the agency ID being supplied matches an attribute of the client certificate.

Participating agency internet proxy IP address will be whitelisted in Neoface Reveal web based Investigation Service. This means only staff using DIA device can access this service. And DIA will further limit users belonging to a certain AD group having access to the service.

Participating agency staff can access the web-based application after successfully providing credentials issued to each named user. Password complexity, expiry and user authentication will be managed by the FRaaS Platform administrators at the direction and approval of the DXC Account Security Officer and authorized participating agency representatives. End-user authentication will be performed against the internal role and user membership in the FRaaS database.

The FRaaS web-client application provides a role-based security model. The FRaaS has a predefined set of functions and permissions that can be assigned to individuals or groups of users. FRaaS will provide a role with associated permissions appropriate to the consumption of Investigation Services and can be assigned to named users from the participating agency.

FRaaS web-service calls to the API endpoint for each instance will perform authorisation to ensure that each participating agency can only execute transactions against galleries that are maintained for the authenticated Agency ID.

Web-service calls that are not authorised will be recorded in the FRaaS Platform audit logs and investigated to determine the root cause of the authorization failure.

The purpose of the provided biographic and biometric data and biometric matching and is to ensure; people only hold one passport, speed and accuracy of entitlement determination and detecting fraudulent attempts to obtain a passport. This is achieved through the following services:

- Identification Service

Provides functions to support one-to-many searches using facial characteristics against a biometric enrolment database.

- Verification Service

Provides functions to enable the performing of one-to-one comparisons searches using facial characteristics.

- Investigation Service

Provides functions to enable investigators to investigate identity fraud and perform forensic analysis of facial images.

Privacy risk assessment

Some types of initiatives are more likely to create privacy risks. If the initiative involves one or more of these risk areas, it's likely that a Privacy Impact Assessment will be valuable.

Use the following checklist to identify and record whether your proposal raises certain privacy risks. Delete any that do not apply.

Does the initiative involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
Information management generally			
A substantial change to an existing policy, process or system that involves personal information	✓		This is an entirely new system (even though it is performing the same functions as a previous system)
Any practice or activity that is listed on a risk register kept by your organisation	✓		The FRS will be integrated with the Passports System. As part of the FRS Certification and Accreditation process risks are identified and controls applied. Any Residual Risks are included in the certificate for acceptance by the Business Owner and DCE. A Security Risk Assessment has been performed for FRS.
Collection			
A new collection of personal information		✓	
A new way of collecting personal information		✓	
Storage, security and retention			

Does the initiative involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
A change in the way personal information is stored or secured	✓		In the current FR system, ABIS, the biometric template is stored with a small amount of biographic information for 'binning' purposes (filtering). This is limited to Gender, Date of Birth, Place of Birth and Country of Birth. The images are not stored in ABIS. In the new FRaaS, both images, biometric templates and biographic data will be stored in separate databases and logically partitioned by participating agencies. The DIA data stored in FRaaS are: Image ID, Identified gender, Age at time of capture (calculated from application received date and date of birth), Place of birth, Country of birth, Image capture date (date application is received) and the image.
A change to how sensitive information is managed	✓		In the current FR system ABIS is hosted in DIA DCSG data centre and information is managed by DIA business system and Datacom. In the new FRaaS solution, the information will be managed by DXC as part of the managed service.
Transferring personal information offshore; using a third-party contractor or Cloud storage		✓	
A decision to keep personal information for longer than you have previously		✓	
Use or disclosure			
A new use or disclosure of personal information that is already held		✓	
Sharing or matching personal information held by different organisations or currently held in different datasets		✓	
Individuals' access to their information			

Does the initiative involve any of the following?	Yes (tick)	No (tick)	If yes, explain your response
A change in policy that results in people having less access to information that you hold about them		✓	
Identifying individuals			
Establishing a new way of identifying individuals		✓	
New intrusions on individuals' property, person or activities			
Introducing a new system for searching individuals' property, persons or premises		✓	
Surveillance, tracking or monitoring of movements, behaviour or communications		✓	
Changes to your premises that will involve private spaces where clients or customers may disclose their personal information		✓	
New regulatory requirements that could lead to compliance action against individuals on the basis of information about them		✓	
List anything else that may impact on privacy, such as bodily searches, or intrusions into physical space		✓	

Initial risk assessment

If you answered "Yes" to any of the questions above, use the table below to give a rating: **Low (L)**, **Medium (M)**, or **High (H)** – for each of the aspects of the project set out in the first column. For risks that you've identified as Medium or High, indicate (in the right-hand column) how the project plans to lessen the risk (if this is known).

If you answered "No" to all the questions in the privacy risk assessment above, move on to the Summary section below.

Privacy Principle affected	Rating (Low, Medium, High)	Describe any medium and high risks and how they will be mitigated
Level of information handling L – Minimal personal information will be handled M – A moderate amount of personal information (or information that could become personal information) will be handled H – A significant amount of personal information (or information that could become personal information) will be handled	High	This system will hold biometric data, images and biographic data for approximately 4.5m individuals. A risk assessment has been carried out and appropriate controls will be implemented e.g. separation of biometric and biographic data, design and implementation assurance and testing of the system, strict controls on physical and logical access. This will be documented and recorded in the FRaaS Security Certificate.
Sensitivity of the information (eg health, financial, race) L – The information will not be sensitive M – The information may be considered to be sensitive H – The information will be highly sensitive	High	Two reasons: 1. Volume – the aggregate is enormous. 2. Value – if biometric id is compromised it cannot be repaired.
Significance of the changes L – Only minor change to existing functions/activities M – Substantial change to existing functions/activities; or a new initiative H – Major overhaul of existing functions/activities; or a new initiative that's significantly different	Medium	This is a new system and Investigation services tool.

Interaction with others L – No interaction with other agencies M – Interaction with one or two other agencies H – Extensive cross-agency (that is, government) interaction or cross-sectional (non-government and government) interaction	Low	
Public impact L – Minimal impact on the organisation and clients M – Some impact on clients is likely due to changes to the handling of personal information; or the changes may raise public concern H – High impact on clients and the wider public, and concerns over aspects of project; or negative media is likely	Low	

Summary of privacy impact

Complete the table below based on the assessment outcome so far.

The privacy impact for this initiative has been assessed as:	Tick
Low – There is little or no personal information involved; or the use of personal information is uncontroversial; or the risk of harm eventuating is negligible; or the change is minor and something that the individuals concerned would expect; or risks are fully mitigated	
Medium – Some personal information is involved, but any risks can be mitigated satisfactorily	✓
High – Sensitive personal information is involved, and several medium to high risks have been identified	
Reduced risk – The project will lessen existing privacy risks	

Recommendation

A full privacy impact assessment is not required for FRS, providing no significant risks are identified during the completion of security and cloud risk assessments for the system.

Should the selected provider not be able to answer or address risks arising from the security and cloud risk assessments, a targeted PIA may be required.

Authorisation

The Business Owner is ultimately responsible for ensuring that the Privacy Impact Assessment has the appropriate scope, and that the recommendations are actioned. The Principal Advisor Privacy should be consulted before the document is finalised to ensure that the Threshold Check addresses the necessary privacy considerations.

Authorised by	Signature	Date
Business Owner(s) Russell Burnard General Manager Operations Service Delivery & Operations Branch		26/2/2020
Privacy Reviewer Kevin Linnane Principal Advisor Privacy Organisational Capability and Services		20 February 2020

Forward a copy of the final signed document to [*privacy@dia.govt.nz*](mailto:privacy@dia.govt.nz)*.*