Privacy Impact Assessment

Promadis

Prepared for the ACT City and Environment Directorate

24 November 2025

1 Overview

Background

1.1 The City and Environment Directorate (**CED**), operates an IT system for the Registrar-General which facilitates the registration of life events as well as the change to registered details. The system is known as 'Promadis' (**Promadis**).

1.2 Promadis was first implemented by the ACT Registrar-General in 2002 to be 'the register of registrable events' that the Registrar-General must maintain under section 39 of the *Births, Deaths and Marriages Registration Act 1997* (**BDMR Act**). Initially Promadis was implemented as a database and was purpose built to integrate with the Registry's functions with the aim of increasing productivity.

1.3 The Head of Access Canberra is appointed as the Registrar-General[1] and is responsible for the registration of life events such as births, deaths, marriages and relationships in the ACT. Up until now, the applications for registration of a life event or changes to a registration have been paper-based applications, which are not always convenient for the community or the BDM Team who process these applications

1.4 CED is now seeking to implement an online channel for applicants or Industry informants (i.e. celebrants, hospitals, funeral director etc) to register a life event or apply to change a registration. This will be facilitated through the introduction of 10 new service portals which will enable submission, processing and case management of applications submitted through Access Canberra, as well as the introduction of four new industry portals (**Project**).

1.5 Additionally, Promadis will provide the Registrar-General and the Births, Deaths, and Marriages (**BDM**) team (delegates of the Registrar-General) with the ability to manage registering, searching, viewing, correcting, altering and validating life events online and remove manual handling of applications and supporting documents.

1.6 This privacy impact assessment (**PIA**) was undertaken to assess how the Registrar-General's privacy obligations will be impacted by the Project and made the below recommendations to mitigate any privacy compliance risks identified.

New Process Flow

1.7 The Promadis system is hosted on the Promadis BDM Database and application server.[2] The system will be accessed by the public through 'apply now' links on the Access Canberra website (for each BDM service). The online service portals are hosted on a web-based server that uses the domain name www.rgoonline.act.gov.au, with a unique URL extension for each service portal.

1.8 Customers will not be required to create any account in order to access the portals and submit an application however, all customers will be required to verify their identity through the Document Verification Service (**DVS**). All customers lodging an application will also be required to scan and upload a copy of the identity document they used for DVS verification as an additional authentication step.

---

[1] As appointed by the Acting Director-General of the Justice and Community Safety Directorate in accordance with section 4 of the *Registrar-General Act 1993* (ACT) on 26 June 2025 by Notifiable Instrument NI2025 – 354.

[2] Page 5 – Promadis current state doc 4

1.9 Applicants will complete the application for their desired service online and then submit the application. The portals will also enable applicants to upload documents supporting their application.

1.10 If the application requires input from a third party other than the applicant, i.e. the other parent on a birth certificate, the Promadis system will enable input of the third party name and contact details which the system will use to communicate with the third party and enable them to complete their section/s of the application.

1.11 Once complete and submitted, staff from the BDM team within Access Canberra will process the application.

1.12 Industry partners will not be required to verify their identity as they will undertake actions on behalf of their employer/business, however, will be required to create an account which they will log into to conduct their business.

2 Overall findings

2.1 This Project does not involve any new collection of personal or health information. Rather, it is implementing a new way of handling personal and health information which is intended to remove the need for manual handling of personal information thereby improving the quality of personal information collected and held by the Registrar-General.

2.2 The PIA focused largely on the practices, processes and procedures put in place to ensure compliance with privacy obligations as well as data quality and security matters.

2.3 The PIA process did not identify any high risks issues. The PIA found that many of the privacy processes and procedures the Registrar-General has in place were mature and robust from a privacy perspective, and in particular:

(a) the agreement the Territory has in place with the third-party ICT service provider for the delivery of the Promadis system, contained sufficiently robust obligations on the third-party contracted service provider with respect to the handling of personal and health information as well as in relation to data security;

(b) transparency notices required some work to ensure the Registrar-General was providing clear and accessible messaging to the public about how it handles and protects the personal and health information it collects and holds and to ensure that the information it does make available is up to date; and

(c) the Promadis Security Plan in place considers matters such as (but not limited to) system governance, awareness and training, identification and authentication, access control, auditing, incident response, contingency planning, and Essential Eight compliance.

3 Summary of recommendations

3.1 The recommendations made in this PIA aim to ensure current processes and procedures are reviewed and remain compliant with the implementation of the Project and specifically in relation to transparency, further steps are taken to provide clear and accessible information to the public.

3.2 All recommendations in the PIA have been accepted by the Registrar-General.

3.3 The recommendations made in the PIA are summarised as follows:

(a) once the solution is implemented, to ensure privacy compliance issues are managed in an ongoing and proactive way, we recommend the Registrar-General periodically review the new capabilities implemented to ensure they are operating as intended and continue to comply with their obligations under the TPPs and HPPs (**Recommendation 1**);

(b) the Registrar-General develop a privacy policy in accordance with their obligations under TPP 1.3 which contains all information required to be included in accordance with the Registrar-General's obligations under TPP 1.4 (**Recommendation 2**);

(c) if the Registrar-General uses or intends to use Aboriginal and Torres Strait Islander status information collected under section 47 of the BDMR Act, for any purpose other than to pass on to the ABS, we recommend the Registrar-General consider amending the BDMR Regulation to include it as a prescribed particular where relevant (**Recommendation 3**);

(d) the Registrar-General review and confirm that the information that is required to be entered into Promadis by Industry Partners, is limited to that which the Industry Partner is required to provide under the BDMR Act (**Recommendation 4**);

(e) to ensure compliance with TPP 5, we recommend a collection notice is developed in respect of the personal and health information collected via Promadis and provided to individuals as part of the Project. If one (or more) collection notices already exist, then we recommend the Registrar-General review the collection notice(s) to ensure it remains relevant and up to date in light of the changes brought about with the implementation of the Promadis portals (**Recommendation 5**);

(f) we recommend the Registrar-General finalise the DVS collection notice, updating it to identify the Registrar-General as the public sector entity that is collecting and handling personal and health information. We further recommend that the finalised notice is made available to applicants as part of the Project (**Recommendation 6**);

(g) we recommend that the collection notice(s) include the following information as it relates to personal health information (**Recommendation 7**):

(i) the purpose of collecting the personal health information;

(ii) if the collection of the personal health information is required or authorised by law, the law that does so require or authorise; and

(iii) the identity of the persons or agencies that the personal health information is usually disclosed to;

(h) to ensure the Registrar-General is receiving accurate and complete information, we recommend that each individual who submits an application is required to make a declaration that the information and documents they are providing are accurate and complete (**Recommendation 8**); and

(i) when developing its Data Management Plan, we recommend that the Registrar-General (**Recommendation 9**):

(i) take into account its obligations under HPP 4.2; and

(ii) ensure all information collected in accordance with section 47 of the BDMR Act is identifiable and is stored separately to the register as required under subsection 47(2) of the BDMR Act.

4 Community Expectations

4.1 The lawful collection, use or disclosure of personal information may ensure that a particular activity complies with the Privacy Act, and even with generally accepted privacy principles. However, that does not mean it will necessarily meet community expectations.

4.2 The former Australian Privacy Commissioner Malcolm Crompton has noted that:

> *Consumers everywhere eventually reach a level of concern where they no longer accept a situation of low security and regular loss of privacy through inappropriate use and sharing of information, even if legal.*[3]

4.3 Furthermore, community expectations about what constitutes an invasion of privacy are not necessarily reflected in the law, with some surveys of lodged privacy complaints suggesting that many complainants' expectations about how the law is supposed to protect their privacy are not being met by privacy laws, including the Privacy Act, in practice.

4.4 Reliable indicators of community expectations are notoriously difficult to produce however, some assumptions may be drawn from the findings of OAIC's *Australian Community Attitudes to Privacy Survey 2023* which provides valuable insights into community expectations generally. Relevant findings from the most recent survey include:

(a) 62% see the protection of their personal information as a major concern in their life[4];

(b) 61% of Australians trust that Government agencies will use and share their personal information only for the purposes they say they will[5]; and

(c) 74% of Australians feel data breaches are one of the biggest privacy risks they face today.

4.5 Transparency is an important aspect of building trust in the community. Trust that personal information is being used in ways which are expected and trust that there is integrity in the outcomes which impact people's lives. The Registrar-General plays an important role in the lives of many, registering our most important life events. As such, where the Registrar-General uses the processes for gathering information to register life events for the purposes of collecting personal information for other purposes (such as for passing onto the ABS), this needs to be clearly communicated.

4.6 Where such collections are not mandatory, this is also an important factor that should be brought to the attention of all applicants, up front, before they commence completing any application form. In this regard, we refer to **Recommendations 2, 5, 6** and **7**.

4.7 Provided the recommendations in this PIA are implemented, we do not consider the expansion of Promadis system capabilities to raise any significant issues from a community expectations perspective. We consider that due to lessening the manual handling of application it is likely to facilitate increased efficiency in processing of applications as well as increased accuracy.

---

[3] Information Integrity Solutions, *The trust cluster: dealing effectively with security, privacy, identity and authentication at the heart of connected government* dated 2005.

[4] Main findings

[5] Figure 32: Trust in aspects of personal information handling by industry sector