



Privacy Threshold Assessment

Project Details

Project name	Power Platform CRM
Project manager/ Responsible official	Gavin Veitch – Director, Digital Science Platforms / Enterprise Data and Digital (EDD) / Corporate Division
Threshold assessment drafter	Scott Murray – Business Analyst, Digital Science Platforms / Enterprise Data and Digital (EDD) / Corporate Division
Description of the project	<p>The Power Platform CRM project is a new initiative aimed at operationalising and deploying a production version of the CRM solution that was successfully piloted within Geoscience Australia (GA). The pilot addressed critical needs, including managing customer and stakeholder data for business areas like the Land Access Management and Approvals (LAMA) team, which was highlighted in an audit as requiring a fit-for-purpose system.</p> <p>Building on the pilot's success, the project seeks to:</p> <ul style="list-style-type: none"> • Stand up a scalable, secure, and fully operational production environment for the Power Platform CRM. • Migrate the pilot configurations and design decisions into the production environment, ensuring alignment with organisational standards. • Expand the system's functionality to support additional business areas while maintaining compliance with government security and privacy requirements. <p>This project transforms the CRM from a pilot concept into a robust enterprise solution, addressing the gaps identified in the audit and supporting GA's broader operational and engagement needs.</p>
Types of personal information being handled as part of the project	<p>The Power Platform CRM project records personal information related to business and partner contacts to support Geoscience Australia's operations. This includes:</p> <ul style="list-style-type: none"> • First name and surname of the contact. • Business contact details, such as: <ul style="list-style-type: none"> ○ Business phone number. ○ Business email address. ○ Business postal address. ○ Business fax number (if applicable). • Records of interactions, such as: <ul style="list-style-type: none"> ○ Logs of communications with GA staff.

	<ul style="list-style-type: none"> ○ Correspondence logs, including email messages sent to the nominated business contact (excluding attachments containing sensitive or classified content). <p>The system focuses on managing business contact information rather than personal or sensitive information unrelated to organisational needs. This ensures compliance with privacy regulations while enabling effective stakeholder engagement.</p> <p>Personal information is information or an opinion about an identified individual, or an individual who is reasonably identifiable.</p>
<p>What is the purpose of, or legal authority for, handling the personal information?</p>	<p>The Power Platform CRM is implemented to meet GA's operational needs for managing stakeholder and partner engagement, as identified during the pilot phase and subsequent audits.</p> <p>Its primary purpose is to provide a centralised, secure, and compliant system for recording and managing business contact information, supporting efficient communication and decision-making across GA's business areas, including LAMA and others.</p> <p>The legal authority for handling personal information is derived from GA's statutory functions and obligations, which include stakeholder engagement and the provision of advice under relevant legislative frameworks such as the <i>Privacy Act 1988</i> (Cth). This ensures that the collection, use, and storage of personal information comply with legal and regulatory requirements.</p> <p>Data Protection Measures</p> <p>The system architecture, based on Datacom's design, ensures robust data protection through:</p> <ul style="list-style-type: none"> • Role-Based Access Control (RBAC): Only authorised users with defined roles can access specific data. Sensitive records are further restricted to specialised groups, such as the Access Engagement Team. • Data Encryption: All data is encrypted at rest and in transit within Microsoft's secure Azure environment, protecting it from unauthorised access. • Audit Logs: Comprehensive logs track user access and activities, supporting (manual) compliance monitoring and mitigating the risk of unauthorised data handling. • Separation of Environments: The system operates in isolated environments for production, ensuring that live data is not accessible during development or testing.

	<p>Mitigation of Risks Measures implemented to mitigate risk related to the handling of personal information includes:</p> <ul style="list-style-type: none"> • Regular audits and security reviews to identify and address vulnerabilities. • A privacy-centric design, ensuring that data collection is limited to what is strictly necessary for business purposes. <p>Establishing Data Governance Data governance is required to ensure that the records in the system maintain integrity. The business owner is responsible for performing data governance. The infrastructure to support data governance has been built and the practices are being developed.</p> <p>Auditing and Review Process The CRM’s built-in logging and auditing functionality tracks key activities, including user access, data interactions, and configuration changes. These logs will be reviewed manually by authorised administrator roles assigned to the business owner using the Power Platform Admin Center. These manual reviews will be conducted periodically and focus on detecting unauthorised access, identifying workflow misconfigurations, and monitoring privileged user activities to mitigate risks.</p> <p>While advanced real-time monitoring is not currently feasible, this limitation can be mitigated through granular logging at the table and column level, complemented by regular manual audits to ensure compliance and proactively address risks.</p> <p>Multi-Factor Authentication (MFA) As strongly recommended by the ISM, users are required to complete an MFA step when logging on to Power Platform. This step is required of all users of Power Platform regardless of which feature they are using.</p> <p>Data Hosting and Oversight Per advice from GA legal counsel, hosting data on the IRAP-certified Microsoft Azure platform (hosted in Microsoft Azure’s Australia East and Australia Southeast data center) does not constitute a disclosure of personal information outside of GA. This is because GA retains effective oversight and control of its data, consistent with privacy regulator guidance and GA’s established practices.</p> <p>The CRM aligns with GA’s commitment to safeguarding personal information while enabling critical business processes efficiently and securely.</p>
Stakeholders	<p>Internal Stakeholders</p> <ol style="list-style-type: none"> 1. GA Business Areas (Power Platform CRM Users): <ul style="list-style-type: none"> ○ Land Access Management and Approvals (LAMA): Key users managing potentially sensitive stakeholder data to which access

is restricted using Role Based Access Control (RBAC).

- Space Division: Using the CRM for managing stakeholder interactions related to Digital Earth Australia projects.
 - Place and Communities Division: Leveraging the CRM for geospatial data services and stakeholder management.
 - Mineral, Energy and Groundwater Division: Supporting stakeholder engagement and landholder negotiations.
 - Corporate Division: Ensuring external stakeholder coordination and engagement is tracked effectively.
2. GA Cyber Security Team: Evaluating the Detailed Design (DD) System Security Plan (SSP) and Security Risk Management Plan (SRMP) and provide feedback to DSP and Datacom to be addressed in the documentation to ensure compliance with security policies and mitigate risks, supporting the Authority to Operate (ATO) Process.
 3. GA ICT Design Authority: Responsible for reviewing and approving the design of the Power Platform CRM (including granting the ATO if appropriate), ensuring alignment with enterprise standards.
 4. GA Privacy Officer: Oversee compliance with the Privacy Act 1988 and providing guidance on personal information handling.
 5. GA Enterprise Digital Delivery (EDD) Teams:
 - Cloud Platforms Team: Supporting infrastructure readiness and integration with GA's cloud systems. Providing ongoing support and maintenance for GA Cloud Platforms (including the Power Platform CRM, once deployed). Ongoing maintenance, operation, expansion/update and governance of the MS Azure and Power Platform platforms.
 - Digital Experience Team: Ensuring ongoing maintenance and operational support for the CRM, and day-to-day CRM activities, including user onboarding/offboarding, customising Power Apps, troubleshooting user issues, and ensuring the smooth operation of the CRM. Also supports Power Automate flows and process automation related to the CRM.
 6. Geoscience Australia Directors of Information Operations (DIOs): Representing divisional

priorities and ensuring CRM alignment with their respective operational needs.

External Stakeholders

1. Datacom:
 - Primary vendor responsible for developing the CRM pilot and supporting its transition to a production environment.
 - Responsible for developing the Power Platform CRM Detailed Design with support from GA resources.
2. Microsoft:
 - Provider of the Power Platform and Azure cloud infrastructure.
 - Ensuring technical reliability, security compliance, and operational support for the CRM environment.
3. Stakeholder and Partner Organisations:
 - Businesses and agencies engaged with GA, whose interactions and data will be recorded and managed within the CRM.
4. National Archives of Australia (NAA):
 - Oversight of record management compliance for CRM data, ensuring alignment with NAA guidelines for metadata and records handling.
5. Australian Government Regulatory Bodies:
 - Ensuring that the CRM meets legal and regulatory requirements, particularly those related to privacy and data security (e.g., Australian Privacy Act 1988).
6. Third-Party Service Providers:
 - Vendors providing integrations or ancillary services connected to the CRM (e.g., email tracking, reporting tools).

Part 1: Handling personal information

	Yes	No	Potentially
Will the project involve new or changed ways of handling personal information?	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Part 2: Determining potential for a high privacy risk

Consider the following questions and record each answer as 'yes', 'no' or 'potentially'. The purpose of these questions is to help you screen for factors which point to the potential for a high privacy risk project. It's important to note that these questions are non-exhaustive, and you should

also consider whether there are any other relevant factors that may indicate that your project is a high privacy risk project.

Will the project involve:	Yes	No	Potentially
<p>Handling large amounts of personal information?</p> <p><i>Consider the amount of personal information and the number of individuals that will be impacted by your project. Even if you consider that each individual will only have a small chance of suffering a negative impact, handling personal information on a large scale can increase the privacy risk associated with your project. You should also consider whether your project will result in significant increases in the volume of personal information being handled through new or existing channels.</i></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Handling sensitive information?</p> <p><i>Sensitive information includes, but is not limited to, information about an individual's racial or ethnic origin, political opinions, religious beliefs or affiliations, criminal records, sexual preferences or practices, biometric information, health information and genetic information.</i></p> <p><i>The privacy risk associated with your project can increase if sensitive information is involved given the potential for adverse consequences for an individual, or those associated with the individual, if it is mishandled (for example, discrimination, mistreatment, humiliation or embarrassment).</i></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Sensitivities based on the context in which the project will operate?</p> <p><i>Consider the context and circumstances surrounding the project. Are there prior concerns over this type of handling or activity? Is the project likely to have community support? Is the handling of personal information novel in any way? What is the current state of technology in this area and has there been any previously identified security or technology flaws? Are there any current issues of public concern that you should factor in? What is the nature of your relationship with individuals that may be impacted by the project? How much control will they have over the handling of their personal information? Would they expect you to use their personal information in this way?</i></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Handling personal information of individuals who are known to be vulnerable?</p> <p><i>Consider whether the activity may have greater sensitivities or disproportionate impacts on vulnerable populations and certain groups of individuals. This could include children and seniors, people with impaired intellectual or physical functioning, people who are not native speakers of the local language, people with low levels of literacy or education, people from a low socio-economic background, people experiencing financial hardship, people who are Aboriginal or Torres Strait Islanders.</i></p> <p><i>An individual's circumstances, or the increased power imbalance between the individual and an entity, may mean, for example, they are unable to easily consent to, or oppose, the handling of their personal information, understand its implications, or exercise control over their personal information.</i></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Will the project involve:	Yes	No	Potentially
<p>Handling personal information in a way that could have a significant impact on the individuals concerned?</p> <p><i>Consider the potential consequences for the individuals concerned. For example, negative impacts on physical and mental wellbeing, reduced access to public services, discrimination, financial loss or identity theft.</i></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Disclosing personal information outside of your entity?</p> <p><i>Consider whether your project will involve sharing personal information with another entity, organisation or to any individuals other than the individual to whom the information relates. This might include the use of contractors or sub-contractors. Also consider whether your project will require the disclosure of personal information overseas.</i></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Using or disclosing personal information for profiling or behavioural predictions?</p> <p><i>This includes valuation or scoring, profiling and predicting (including in relation to economic situation, health, personal preferences or interests, reliability or behaviour, location or movements).</i></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Using personal information for automated decision-making?</p> <p><i>This might include the use of artificial intelligence technologies or data analytics techniques on personal information to produce insights for policy-making or improved service delivery. It might also include using automated decision-making to make decisions that affect the rights, entitlements and opportunities of an individual.</i></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Systematic monitoring or tracking of individuals?</p> <p><i>For example, the introduction or enhancement of a surveillance system, the monitoring of communications, tracking an individual's geolocation or behaviour.</i></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Collecting personal information without notification to, or consent of, the individual?</p> <p><i>This might include collecting personal information about an individual from a third party without the individual's knowledge or consent. It might also include collecting personal information compulsorily under an existing, or proposed, legislative authority.</i></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
<p>Data matching (linking unconnected personal information)?</p> <p><i>For example, a new data matching program combining, comparing or matching personal information obtained from multiple sources.</i></p>	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Will the project involve:

Yes

No

Potentially

Developing legislation to modify the operation of one or more APPs or which seeks to rely on the required or authorised by law exception to the APPs?

This might include legislation or delegated legislation that seeks to modify the operation of one or more APPs in certain circumstances. It might also include legislation that seeks to rely on the required or authorised an exception to the APPs (such as legislation authorising the use or disclosure of personal information).

Decision & declaration

If you have answered 'Yes' or 'Potentially' to any of the questions in Part 2, a PIA should be completed. If you are uncertain as to whether you have considered all relevant risks, you are strongly encouraged to seek support from your entity's privacy officer to ensure your assessment is thorough and complete. If still unsure, err on the side of caution and conduct a PIA.

Based on your answers above, is a PIA required?

Yes

Yes, there are (or potentially are) high privacy risk elements to this project.

No

No, a PIA is not necessary. This project does not carry any high privacy risks.

Project Manager/Responsible Official Sign-off

Gavin Veitch – Director, DSP / EDD / Corporate

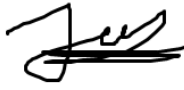
07/02/2025

	7/2/2025
---	----------

Privacy Officer Sign-off

Position: Yifu Jiang, Senior Legal Counsel

Date

	7/02/2025
---	-----------