

Document 3 (pages 43 - 88) deleted under section 42(1) of the ***Freedom of Information Act 1982*** (Cth).

Document 4 (pages 89 - 98) deleted under section 42(1) of the ***Freedom of Information Act 1982*** (Cth).



Privacy Threshold Assessment

Apprenticeship, Vet Student Loan, Vet FEE_HELP Data Matching

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes	Using existing DEWR Apprenticeship, Vet Student Loans (VSL) and Vet FEE_HELP (VFH) data holdings to: • Identify instances of multiple Government funds, over the same periods of time, where the entity may be ineligible. • Identify presence of potential fraud, such as identity theft or unknowing participants. • Assessment to ensure compliance with citizenship and other relevant eligibility criteria. • Support a more holistic departmental approach to identifying Compliance and/or fraud risks and entities present across multiple programs.
Key implementation date/s	Phase 1 – Identify the individuals present in apprenticeship, VSL and VFH systems [Completion Date: Mid 2023]. Phase 2 – Import the relevant information into suitable analytical environment (Skills iBase Database (SID)) [Completion Date: Mid 2023]. Phase 3 – Assessment of information and referral to relevant compliance teams for appropriate treatments [Completion Date: Ongoing].
Key internal and external stakeholders	Compliance Intelligence Team, Skills Compliance Delivery Team, Technology and Services Division (DEWR IT security/oversight), VA Worldwide (external vendor support of i2 iBase/SID) Assurance Coordination Branch, VET Student Loans Branch, VET-Fee-Help Redress, VET Information Systems Branch.

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information¹? - If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.						Yes
Type of information	Collect	Use	Disclose	Store	Destroy ²	De-identify
Names	☐	☒	☐	☒	☐	☐
Signatures	☐	☒	☐	☒	☐	☐
Addresses	☐	☒	☐	☒	☐	☐
Email addresses	☐	☒	☐	☒	☐	☐
Telephone numbers	☐	☒	☐	☒	☐	☐
Dates of birth	☐	☒	☐	☒	☐	☐
Sex or gender	☐	☒	☐	☒	☐	☐
Opinions or feedback	☐	☒	☐	☒	☐	☐
Commentary	☐	☒	☐	☒	☐	☐
CRNs or JSIDs	☐	☒	☐	☒	☐	☐
USIs or CHESSNs	☐	☒	☐	☒	☐	☐
Tax file numbers	☐	☒	☐	☒	☐	☐
Financial information	☐	☒	☐	☒	☐	☐
Bank account details	☐	☒	☐	☒	☐	☐
Identity documents	☐	☒	☐	☒	☐	☐
Racial or ethnic origin	☐	☒	☐	☒	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☒	☐	☒	☐	☐
Health information	☐	☒	☐	☒	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐

¹ 'Personal information' is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

If not listed above, specify other type/s of personal information handled in the project or initiative:

How will personal information be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative?

You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.

This initiative seeks to use the existing personal information holdings collected by the department in the course of administering departmental programs, specifically: apprenticeship wage subsidies and incentives, VSL and VFH Loans, VFH redress and general data on participants in these programs.

The information is currently collected and stored in secure server databases, with access reserved for appropriate users with sufficient programming skills and appropriate business cases to access.

The identification of individuals and information related payments will be extracted from the Apprenticeships, VSL and VFH databases. The information will then be imported and stored in SID on a secure internal DEWR server and compliant with internal security policy that is managed by the department's database administrators (DBA).

Access to the information in SID will be assessed by the SID administrators through Access Control AD groups and SID controls. The SID administrators resource group and membership is managed by the department's Skills Program Compliance, Compliance Intelligence Team. Appropriate level of access will be provided to Skills Program Compliance users based on their Compliance roles and in line with the needs-to-know principle. Additional information and assessment on safeguarding and risk mitigating protocols in relation to SID are also available in the SID Privacy Impact Assessment that addresses these issues.

This will enable the following Intelligence activities for compliance purposes³:

- Identification of entities receiving potentially non-compliant and ineligible government payments over the same overlapping periods.
- Identify the presence of unknowing individuals with details being misused and the risk of potential identity fraud.
- Support validation that the apprentice/trainee/VSL identity details held by the department are correct and accurate, with benefits including using most contemporary information for contacts where appropriate.
- Identify and assess potential non-compliance with citizenship/other eligibility criteria.

³ Compliance means conforming to a relevant rule, such as a specification, policy, regulation, standard or law.

A compliance breach occurs when there is a failure to comply with a legislative obligation, that may be established in Rules, Policies, Procedures or Guidelines.

Breaches can occur, for example, through human error, technical issues, misinterpretation of the obligations, or through a deliberate act.

A compliance activity is an activity that will attempt to identify and resolve a relevant compliance breach.

This may include raising of a debt, issuing a infringement notice, education, notification to DEWR Fraud Team or relevant external agency.

- Provide a more holistic departmental approach to using data holdings and having consideration for those entities that are present across multiple programs for intelligence and compliance.

How many individuals' personal or sensitive information will be handled in the project or initiative?

Approximately 1.5 million information records.

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?

Yes

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.

- ☐ The nature or type of the personal information being handled is new or different.
- ☐ The scope of the personal information being handled is new or different.
- ☐ The personal information is being handled in a new or different context.
- ☒ The purpose for which the personal information is being handled is new or different.
- ☒ The risk of handling the personal information is new or different.

If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).

This project will use personal information to identify entities present in departmental administrative data holdings across multiple programs using the existing processes and secured through appropriate security settings built into the SID secure database.

This project will also lessen or mitigate potential privacy risks involved in the manual handling of bulk personal information by securing the access to and linkage of data inside the SID secure database. This will provide additional assurances and a strong level of handling maturity - such as appropriate role and user group access and auditing capability, instead of personal data being shared via less secure and alternative methods including electronic mail, SharePoint sites or handled in decentralised excel spreadsheets.

If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).

You should provide the name of the same or similar project or initiative where the practice(s) have been assessed previously and reflect on whether the controls are current and working, or will be working, well in this project or initiative.

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals?

Yes

To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	
☒	Handling large amounts of personal information.
☒	Handling sensitive information ⁴ .
☐	Handling personal information in a way that is likely to raise public concern or unlikely to have community support.
☒	Handling the personal information of individuals who are vulnerable. ⁵
☒	Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.
☐	Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.
☒	Using or disclosing personal information for profiling or behavioural predictions.
☐	Using personal information for automated decision-making.
☐	Collecting personal information through systematic monitoring or tracking of individuals.
☒	Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
☒	Using information for data matching or linking unconnected personal information.
☐	Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
☒	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	

⁴ Sensitive information is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practice or criminal record, as well as health information about an individual or genetic or biometric information about an individual.

⁵ May include children, 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.

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

Outcome	A PIA is required as there are or potentially are high privacy risk elements
---------	--

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by: s 22(1) , s 22(1) , Skills Programs Compliance Branch

Date: 12/04/2023

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officers](#).



Threshold Assessment

QARMB iBase server implementation

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes	The Quality, Assurance and Risk Management Branch (QARMB) is responsible for assurance coordination and risk management for the department's employment services programs. QARMB will be implementing iBase, a digital asset management software, to analyse, report on and store its assurance intelligence in relation to employment service providers. TSD will be providing support through creating an instance to host the iBase database.
Key implementation date/s	1/7/2023
Key internal and external stakeholders	The Quality, Assurance and Risk Management Branch, participants of the department's employment services programs, employment services providers.

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information¹? - If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.						Yes	
Type of information	Collect	Use	Disclose	Store	Destroy ²		
Names	☐	☒	☐	☒	☐	☐	
Signatures	☐	☒	☐	☒	☐	☐	

¹ 'Personal information' is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Addresses	☐	☒	☐	☒	☐	☐
Email addresses	☐	☒	☐	☒	☐	☐
Telephone numbers	☐	☒	☐	☒	☐	☐
Dates of birth	☐	☒	☐	☒	☐	☐
Sex or gender	☐	☒	☐	☒	☐	☐
Opinions or feedback	☐	☒	☐	☒	☐	☐
Commentary	☐	☒	☐	☒	☐	☐
CRNs or JSIDs	☐	☒	☐	☒	☐	☐
USIs or CHESSNs	☐	☐	☐	☐	☐	☐
Tax file numbers	☐	☐	☐	☐	☐	☐
Financial information	☐	☐	☐	☐	☐	☐
Bank account details	☐	☐	☐	☐	☐	☐
Identity documents	☐	☐	☐	☐	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☐	☐	☐	☐	☐
Health information	☐	☐	☐	☐	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
N/a						
How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative? <i>You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.</i>						
Collection - No information will be collected from individuals through this initiative. Existing personal Information in relation to program participants previously collected by the Employment Services Program areas and provided to the Digital Assurance team will be deposited into iBase for internal use only.						

Use – iBase will be an integrated IT environment where program areas can plan and record each stage of their quality and assurance lifecycle. This includes the initial planning of an activity, recording of key assurance information, tracking the activity progress, drafting and implementing recommendations, and accessing to record and report results.

Benefits will include:

- a consolidated environment for all programs
- a record of first line and second line assurance activities
- the Branch will have oversight of all assurance activities, and
- improve the consistent reporting of assurance to governance committees through using a single source of data for reporting.

Personal information in relation to program participants, which has already been collected through approved means, will be deposited into iBase for provider quality and assurance reporting purposes. The iBase software will use the collated counts of the various types of information to produce de-identified assurance reports for internal use only. Please note QARMB *will not be reporting personal information either internally or externally*. Our reporting consists of transactional reviews for compliance with relevant Department policies and Deeds such as the Workforce Australia Services Deed of Standing Offer 2022-2028; Workforce Australia – Transition to Work Deed 2022-2027; ParentsNext Deed 2018-2024

Disclosure – Personal information stored on iBase will not be disclosed to third parties, including the i2 Group, the software developer of iBase. If the de-identified reports produced through iBase indicate provider fraud, this report will be provided internally to the relevant team for investigation and action (which may then involve informing other government agencies, where required by law).

Storage – Personal information already held by the department will be stored on the Department's current iBase server, in accordance with the Department's current record keeping policy. Departmental staff who administer or report on assurance activities for employment services programs will have access to this iBase assurance system (QuARTS).

Destruction – We will comply with the requirement for destroying any personal information in line with the Department's current processes. **De-identification** – Personal information will be held in iBase. However, QARMB will not be reporting any personal information either internally or externally. Our reporting consists of transactional reviews for provider compliance, i.e. de-identified number or counts only, related to compliance with relevant Department policies and Deeds such as the Workforce Australia Services Deed of Standing Offer 2022-2028; Workforce Australia – Transition to Work Deed 2022-2027; ParentsNext Deed 2018-2024.

How many individuals' personal or sensitive information will be handled in the project or initiative?

Any persons linked to an assurance activity conducted by QARMB. This

	could be up to and including the whole ES caseload – currently at 645K people at 31/3/2023
--	--

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way? If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.	Yes
☐ The <u>nature or type</u> of the personal information being handled is new or different.	
☐ The <u>scope</u> of the personal information being handled is new or different.	
☐ The personal information is being handled in a new or different <u>context</u> .	
☐ The <u>purpose</u> for which the personal information is being handled is new or different.	
☒ The <u>risk</u> of handling the personal information is new or different.	
If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).	
If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).	
You should provide the name of the same or similar project or initiative <u>where the practice(s) have been assessed previously</u> and reflect on whether the controls are current and working, or will be working, well in this project or initiative.	

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals? To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	No
☒ Handling large amounts of personal information.	

☐	Handling sensitive information ³ .
☐	Handling personal information in a way that is likely to raise public concern or unlikely to have community support.
☒	Handling the personal information of individuals who are vulnerable. ⁴
☐	Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.
☐	Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.
☐	Using or disclosing personal information for profiling or behavioural predictions.
☐	Using personal information for automated decision-making.
☐	Collecting personal information through systematic monitoring or tracking of individuals.
☐	Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
☒	Using information for data matching or linking unconnected personal information.
☐	Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
☐	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
QARMB's use of iBase is for provider assurance activities, not for assurance work in relation to individual participants. It will consolidate the storage of personal information for these purposes in a secure setting, where this information is otherwise currently held by different departmental teams in documents stored in various locations. The reports generated through iBase by QARMB will be limited to counts and numbers of various datapoints relating to provider performance and assurance evaluation. No personal information handled through iBase will be disclosed externally.	

³ Sensitive information is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practice or criminal record, as well as health information about an individual or genetic or biometric information about an individual.

⁴ May include children, 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.

Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

Outcome	A PIA is not required as there are no high privacy risk elements or no new or changed ways of handling personal information
---------	---

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by: s 22(1)

s 22(1)

<Approved by email>

Date: 23/05/2023

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).



Privacy Threshold Assessment

Use of iBase by the Fraud Prevention and Investigations Team(s) in the Department of Employment and Workplace Relations and Department of Education.

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes	Use of iBase database by Department of Employment and Workplace Relations (DEWR) and the Department of Education (EDU) to: • Store information including fraud information reports, referrals, and investigations cases. • Perform probity checks. A case management system to manage the conduct of investigations is a requirement of the Australian Government Investigation Standards (AGIS). iBase is the case management system used to meet that requirement. There is no proposed end date for the use of iBase as the department's investigative case management system. This project is specific to the Fraud Prevention and Investigations Team database within the iBase environment and does not consider other instances of iBase that may be used across the department. All references to iBase in this document refer to the Fraud Team iBase database, and not the software itself.
Key implementation date/s	Provisional approval in place and system is currently in use.

Key internal and external stakeholders	Fraud Prevention and Investigations Team (Fraud Team), Enterprise Risk, Assurance and Investigations Branch, Legal and Assurance Division, DEWR
	Fraud Prevention and Investigation Team, Parliamentary, Audit and Risk Branch, People, Parliamentary and Comms Division, Corporate and Enabling Services, Department of Education
	SQL, SAS and Data Management Team, Infrastructure, Platforms and Projects, Technology and Services Division, DEWR Corporate and Enabling Services, DEWR
	Corporate Applications Team, Digital Workplace, Technology and Services Division, DEWR Corporate and Enabling Services, DEWR

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information¹? - If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.						Yes	
Type of information	Collect	Use	Disclose	Store	Destroy ²		
Names	☐	☒	☒	☒	☐	☐	
Signatures	☐	☒	☒	☒	☐	☐	
Addresses	☐	☒	☒	☒	☐	☐	
Email addresses	☐	☒	☒	☒	☐	☐	
Telephone numbers	☐	☒	☒	☒	☐	☐	
Dates of birth	☐	☒	☒	☒	☐	☐	
Sex or gender	☐	☒	☒	☒	☐	☐	
Opinions or feedback	☐	☒	☒	☒	☐	☐	
Commentary	☐	☒	☒	☒	☐	☐	
CRNs or JSIDs	☐	☒	☒	☒	☐	☐	
USIs or CHESSNs	☐	☒	☒	☒	☐	☐	
Tax file numbers	☐	☒	☐	☒	☐	☒	

¹ 'Personal information' is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Financial information	☐	☒	☒	☒	☐	☐
Bank account details	☐	☒	☒	☒	☐	☐
Identity documents	☐	☒	☒	☒	☐	☐
Racial or ethnic origin	☐	☒	☒	☒	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☒	☒	☒	☐	☐
Health information	☐	☒	☒	☒	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
The Fraud Team is very unlikely to use or store other types of personal or sensitive information unless it is relevant to a criminal investigation. For example, personal and sensitive information such as relationship status and involvement in family and domestic violence.						
How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative?						
<i>You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.</i>						
Personal and sensitive information of individuals will be stored in iBase when the Fraud Teams in DEWR and EDU receive tip-offs or referrals and conduct investigations into instances of potential fraud and corruption. Information collected as part of the referral assessment and investigation processes (that occur independently of iBase) will be stored in and retrieved from iBase.						
As information is added to the database over time, links may be created between people or organisations that reoccur in the database to reveal patterns of behaviour or conduct.						
iBase will be used as a source to respond to probity check requests; business areas within DEWR and EDU can request if a person or organisation is known to the Fraud Team and if there are any concerns regarding connections to known fraudulent behaviour. Each request is considered on a case by case basis and released in line with relevant legislation and personal information management requirements.						

The Fraud Team's iBase database is located at s 47E(d)

. The information stored in iBase is held on an internal server managed by the SQL, SAS and Data Management Team. The internal DEWR server is compliant with the [Information Management Policy](#), and adheres to the [Information Security Handbook](#) and procedures in place by DEWR's database administrators (DBA).

Members of the DEWR Fraud Team, EDU Fraud Team, and DBAs from the SQL, SAS and Data Management Team and Corporate Applications Team have access to the information stored in iBase. All members of the Fraud Teams with access to iBase have or are in the process of gaining NV1 clearances. While the team is in the process of implementing access control to reduce the ability of DEWR and EDU to access each other's cases, at this stage administrative controls are that staff are instructed only to access information on a need-to-know basis. Audit logs for both users and DBAs are available to record actions in relation to iBase and are reviewed periodically.

Disclosure to third parties will occur in accordance with appropriate legislation or criminal proceedings on a case-by-case basis. The nature of sharing will vary depending on each case but most typically by email or by File Transfer.

How many individuals' personal or sensitive information will be handled in the project or initiative?

As many as required to perform fraud investigations, likely in the 1000s over the expected life (indefinitely) of the database.

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.

No

- | | |
|--------------------------|---|
| ☐ | The <u>nature or type</u> of the personal information being handled is new or different. |
| ☐ | The <u>scope</u> of the personal information being handled is new or different. |
| ☐ | The personal information is being handled in a new or different <u>context</u> . |
| ☐ | The <u>purpose</u> for which the personal information is being handled is new or different. |
| ☐ | The <u>risk</u> of handling the personal information is new or different. |

If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).

If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).

You should provide the name of the same or similar project or initiative where the practice(s) have been assessed previously and reflect on whether the controls are current and working, or will be working, well in this project or initiative.

iBase has been used by the Fraud Team since at least 2007 in its current form.

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals?

Yes

To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:

- ☒ Handling large amounts of personal information.
- ☒ Handling sensitive information³.
- ☐ Handling personal information in a way that is likely to raise public concern or unlikely to have community support.
- ☒ Handling the personal information of individuals who are vulnerable.⁴
- ☒ Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.
- ☒ Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.
- ☐ Using or disclosing personal information for profiling or behavioural predictions.
- ☐ Using personal information for automated decision-making.
- ☐ Collecting personal information through systematic monitoring or tracking of individuals.
- ☒ Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
- ☒ Using information for data matching or linking unconnected personal information.
- ☐ Developing legislation to modify the operation of the *Privacy Act 1988* or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
- ☒ Handling personal information for activities of a long term or permanent duration.

If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.

³ Sensitive information is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practice or criminal record, as well as health information about an individual or genetic or biometric information about an individual.

⁴ May include children, 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.

Information related to criminal investigations into individuals, if subject to unauthorised access and release, could significantly damage reputation and wellbeing.	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

Outcome	Choose an item.
I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.	

Approved by: s 22(1) , s 22(1) and s 22(1)

Date: 29/06/2023

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).



Threshold Assessment

ASIC Data - Beneficial Ownership Project

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 20017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes	The project involves the use of publicly available data obtained from the Australian Securities and Investments Commission (ASIC) to support Department of Employment and Workplace Relations (the department) compliance efforts in relation to skills programs and enable the identification of beneficial ownership and potentially undeclared business interests and organisational affiliations. This PTA will be solely focusing on the new and changed way of handling personal information – the use of data already shared by ASIC with the department.
Key implementation date/s	Mid 2023 – Ongoing
Key internal and external stakeholders	Employment Assurance Insights ASIC (External) Compliance Intelligence team

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information¹? - If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.	Yes
---	-----

¹ 'Personal information' is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

Type of information	Collect	Use	Disclose	Store	Destroy ²	De-identify
Names	☐	☒	☐	☒	☐	☐
Signatures	☐	☐	☐	☐	☐	☐
Addresses	☐	☒	☐	☒	☐	☐
Email addresses	☐	☒	☐	☒	☐	☐
Telephone numbers	☐	☐	☐	☐	☐	☐
Dates of birth	☐	☒	☐	☒	☐	☐
Sex or gender	☐	☒	☐	☒	☐	☐
Opinions or feedback	☐	☐	☐	☐	☐	☐
Commentary	☐	☐	☐	☐	☐	☐
CRNs or JSIDs	☐	☐	☐	☐	☐	☐
USIs or CHESSNs	☐	☐	☐	☐	☐	☐
Tax file numbers	☐	☐	☐	☐	☐	☐
Financial information	☐	☐	☐	☐	☐	☐
Bank account details	☐	☐	☐	☐	☐	☐
Identity documents	☐	☐	☐	☐	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☐	☐	☐	☐	☐
Health information	☐	☐	☐	☐	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
• ABN • Business Name • Business Links						
How will personal information will be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative?						

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.

The ASIC data extracts will be used for matching purposes. These extracts will be matched against SID extracted data. Only matched data will then be ingested into SID.

The data will be stored in a secure departmental SQL server. It will only be accessible by certain authorised members of the Compliance Intelligence team.

How many individuals' personal or sensitive information will be handled in the project or initiative?

>1,000,000

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?

Yes

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.

- ☐ The nature or type of the personal information being handled is new or different.
- ☐ The scope of the personal information being handled is new or different.
- ☒ The personal information is being handled in a new or different context.
- ☐ The purpose for which the personal information is being handled is new or different.
- ☒ The risk of handling the personal information is new or different.

If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).

If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).

You should provide the name of the same or similar project or initiative where the practice(s) have been assessed previously and reflect on whether the controls are current and working, or will be working, well in this project or initiative.

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals?

No

To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:

- ☒ Handling large amounts of personal information.

☐	Handling sensitive information ³ .
☐	Handling personal information in a way that is likely to raise public concern or unlikely to have community support.
☐	Handling the personal information of individuals who are vulnerable. ⁴
☒	Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft.
☐	Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers.
☐	Using or disclosing personal information for profiling or behavioural predictions.
☐	Using personal information for automated decision-making.
☐	Collecting personal information through systematic monitoring or tracking of individuals.
☐	Collecting personal information without individuals' consent or without telling individuals their personal information is being collected.
☐	Using information for data matching or linking unconnected personal information.
☐	Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles.
☒	Handling personal information for activities of a long term or permanent duration.
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
The information related to individuals and used as part of this project is already publicly available and may be obtained by any member of the public.	
There are minimal additional impacts or privacy risks identified with procedure proposed in the current arrangement with ASIC. Clause 13 of the arrangement specifies that the ASIC data should have limited access for authorised personnel and adhere to the 'need to know' principle.	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	

³ Sensitive information is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practice or criminal record, as well as health information about an individual or genetic or biometric information about an individual.

⁴ May include children, 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.

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

Outcome	A PIA is not required as there are no high privacy risk elements or no new or changed ways of handling personal information
---------	---

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by: s 22(1)

s 22(1)

Date: 27/07/2023

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officers](#)



Threshold Assessment

Open-Source Data Sets

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes	The project involves the use of open-source public registers to support Department of Employment and Workplace Relations (the department) compliance efforts in relation to skills programs and better enable the identification of undeclared interests, organisational affiliations, and relationships. This PTA will consider the collection and use of personal information that may potentially be obtained from these registers, noting that this project will primarily focus on organisations rather than individuals, with no sensitive information to be handled.
Key implementation date/s	Mid 2023 – Ongoing
Key internal and external stakeholders	Employment Assurance Insights Team Compliance Intelligence Team

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information¹? - If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.						Yes	
Type of information	Collect	Use	Disclose	Store	Destroy ²		
Names	☒	☒	☐	☒	☐	☐	

¹ 'Personal information' is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Signatures	☐	☐	☐	☐	☐	☐
Addresses	☒	☒	☐	☒	☐	☐
Email addresses	☒	☒	☐	☒	☐	☐
Telephone numbers	☒	☒	☐	☒	☐	☐
Dates of birth	☒	☒	☐	☒	☐	☐
Sex or gender	☒	☒	☐	☒	☐	☐
Opinions or feedback	☐	☐	☐	☐	☐	☐
Commentary	☐	☐	☐	☐	☐	☐
CRNs or JSIDs	☐	☐	☐	☐	☐	☐
USIs or CHESSNs	☐	☐	☐	☐	☐	☐
Tax file numbers	☐	☐	☐	☐	☐	☐
Financial information	☐	☐	☐	☐	☐	☐
Bank account details	☐	☐	☐	☐	☐	☐
Identity documents	☐	☐	☐	☐	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☐	☐	☐	☐	☐
Health information	☐	☐	☐	☐	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
• ABN • Business Name • Business Links • Other identifiers within the Public Registers						
How will personal information be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative?						

You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.

The Compliance Intelligence team will regularly obtain data from public Federal and State government open-source registers. These are publicly available holdings for general use. The primary source of these holdings are lists and registers held on data.gov.au. The site is the central source of all Australian Government data holdings and already heavily utilised by the department and across the Commonwealth. Furthermore, anyone can easily access the anonymised public data published by federal, state and local government agencies.

Examples of the data this project will use includes:

- Childcare Service Provider List
- Workforce Australia Provider List
- Group Training Organisation (GTO) Register
- Commonwealth Register of Institutions and Courses for Overseas Students (CRICOS)
- Office of the Registrar of Indigenous Corporations Register
- The Australian Charities and Not-for-profits Commission Register
- Australian Government Grant Award List
- AusTender Lists
- NDIS Provider List
- National Register of Higher Education Providers
- Registered Training Organisation (RTO) Register
- Australian Skills Quality Authority Lists
- Vet Student Loan (VSL) Provider List

Where lists and registers cannot be primarily sourced from data.gov.au, the project will obtain the data directly from the specific departmental or agency sites themselves. This can include but is not limited to:

- <https://www.australianapprenticeships.gov.au/>
- <https://www.education.gov.au/>
- <https://www.oric.gov.au/>
- <https://www.acnc.gov.au/>
- <https://www.ndis.gov.au/>

All data used in the project will rely on the information being readily available to the public, through the existing webpages and links developed for this purpose. The data being sought for this project will also be focused on the organisations, rather than individuals and no sensitive information will be handled.

The public information will be loaded and stored in approved departmental data environments (SQL with potential for Databricks) and the outputs then loaded into SID and Power BI reports. The data environments are also resource group controlled and only development programmers will have direct access to this data. Approved operational compliance staff will be able to view the

outputs via SID and Power Bi reports. A Privacy Impact Assessment (PIA) has been completed on the use of SID, it's safety protocols and procedures, and particularly relevant to this project the use of open-source data within its environment. Including for the purposes of data matching activities with existing and future information held in SID.

How many individuals' personal or sensitive information will be handled in the project or initiative?

Less than 50,000

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.

Yes

- | | |
|-------------------------------------|---|
| ☐ | The <u>nature or type</u> of the personal information being handled is new or different. |
| ☐ | The <u>scope</u> of the personal information being handled is new or different. |
| ☒ | The personal information is being handled in a new or different <u>context</u> . |
| ☒ | The <u>purpose</u> for which the personal information is being handled is new or different. |
| ☒ | The <u>risk</u> of handling the personal information is new or different. |

If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).

The use of open-source registers is a logical source of relevant and useful information for the intelligence team and forms a critical component of sourcing information that is already accessible and available to the general public and Commonwealth departments and agencies. The public would also have formed an expectation that this data is already in use and fully operationalised in government for compliance, integrity and counter-fraud work. By coordinating a regular collection of the open-source information and centralising these should result in an increase the speed and efficiency of operational compliance staff undertaking checks or identifying linkages across open-source holdings.

In any of these cases where there are instances that may require further investigation or disclosure to enforcement agencies or otherwise, departmental staff will be required to seek the source supporting information directly or alternatively direct the recipients to the sources for additional information. This would include instances of possible fraud or criminality being identified.

If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).

You should provide the name of the same or similar project or initiative where the practice(s) have been assessed previously and reflect on whether the controls are current and working, or will be working, well in this project or initiative.

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals? To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:	No
☒ Handling large amounts of personal information. ☐ Handling sensitive information³. ☐ Handling personal information in a way that is likely to raise public concern or unlikely to have community support. ☐ Handling the personal information of individuals who are vulnerable.⁴ ☒ Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft. ☐ Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers. ☐ Using or disclosing personal information for profiling or behavioural predictions. ☐ Using personal information for automated decision-making. ☐ Collecting personal information through systematic monitoring or tracking of individuals. ☒ Collecting personal information without individuals' consent or without telling individuals their personal information is being collected. ☒ Using information for data matching or linking unconnected personal information. ☐ Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles. ☒ Handling personal information for activities of a long term or permanent duration.	
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	

³ Sensitive information is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practice or criminal record, as well as health information about an individual or genetic or biometric information about an individual.

⁴ May include children, 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.

If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:

The information to be used in this project is already available to the public through general searches, with all webpages easily accessible. Data sets for the purposes of this project are exclusively open-source registers and analysis will focus primarily on the organisations rather than individuals.

The Compliance Intelligence team closely adheres to departmental privacy and security protocols in protecting the use of information. Furthermore, any information that could be used for an adverse action against a participant of a departmental program will direct staff responsible for these actions to return to the source of the data.

This is an intelligence project. As a result, the privacy impact on individuals and organisations that could be captured by the program has no additional risk compared to the base level that exists for the information already being openly available and regularly updated by the relevant official Commonwealth data custodians.

Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?

Yes

If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

Outcome

A PIA is not required as there are no high privacy risk elements or no new or changed ways of handling personal information

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by:

s 22(1)

s 22(1), s 22(1)

, Skills Programs Compliance Branch

Date: 29/08/2023

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).



Threshold Assessment

Australian Business Register Data Set

Complete this assessment to determine whether a Privacy Impact Assessment (PIA) is required for a project or initiative under the [Privacy \(Australian Government Agencies – Governance\) APP Code 2017](#) (Privacy Code).

Project or initiative

Brief project or initiative description and intended goals/outcomes	The project involves the use of Australian Business Register (ABR) data to support Department of Employment and Workplace Relations (the department) compliance efforts in relation to skills programs and better enable the identification of undeclared interests, organisational affiliations, and relationships. This PTA will consider the collection and use of personal information that may potentially be obtained the ABR, noting that this project will primarily focus on organisations rather than individuals, with no sensitive information to be handled.
Key implementation date/s	2025 – Ongoing
Key internal and external stakeholders	Compliance Intelligence Team Digital Solutions Division

Section 1: Personal information

Q1. Does the project or initiative involve the handling of personal information¹? - If you answered 'yes', identify the type of personal information and the way you will handle it by checking the relevant boxes below. - If you answered 'no', proceed to the 'Outcome' section of this assessment and record that a PIA is not necessary.						Yes
Type of information	Collect	Use	Disclose	Store	Destroy ²	

¹ 'Personal information' is information or an opinion, whether true or not, and whether recorded in a material form or not, about an identified individual, or an individual who is reasonably identifiable.

² Except in accordance with the *Archives Act 1983* or the department's Information Management Policies.

Names	☒	☒	☐	☒	☐	☐
Signatures	☐	☐	☐	☐	☐	☐
Addresses	☒	☒	☐	☒	☐	☐
Email addresses	☒	☒	☐	☒	☐	☐
Telephone numbers	☒	☒	☐	☒	☐	☐
Dates of birth	☐	☐	☐	☐	☐	☐
Sex or gender	☐	☐	☐	☐	☐	☐
Opinions or feedback	☐	☐	☐	☐	☐	☐
Commentary	☐	☐	☐	☐	☐	☐
CRNs or JSIDs	☐	☐	☐	☐	☐	☐
USIs or CHESSNs	☐	☐	☐	☐	☐	☐
Tax file numbers	☐	☐	☐	☐	☐	☐
Financial information	☐	☐	☐	☐	☐	☐
Bank account details	☐	☐	☐	☐	☐	☐
Identity documents	☐	☐	☐	☐	☐	☐
Racial or ethnic origin	☐	☐	☐	☐	☐	☐
Political opinions	☐	☐	☐	☐	☐	☐
Membership of a political association	☐	☐	☐	☐	☐	☐
Religious beliefs or affiliations	☐	☐	☐	☐	☐	☐
Philosophical beliefs	☐	☐	☐	☐	☐	☐
Memberships of a trade union	☐	☐	☐	☐	☐	☐
Sexual orientation or practices	☐	☐	☐	☐	☐	☐
Criminal Record	☐	☐	☐	☐	☐	☐
Health information	☐	☐	☐	☐	☐	☐
Genetic information	☐	☐	☐	☐	☐	☐
Biometric information	☐	☐	☐	☐	☐	☐
If not listed above, specify other type/s of personal information handled in the project or initiative:						
• ABN/ACN • Business Name • Entity Type • GST status • Australian Charities and Not-for-profits Commission details						

How will personal information be collected, used, disclosed, stored, destroyed, and/or de-identified in the project or initiative?

You should explain how each type of information involved in the project or initiative will be handled, including, for example, whether information will be collected directly from individuals or from a third party, whether information will be stored in the cloud and who information will be disclosed to and why.

The Compliance Intelligence team will regularly download bulk data from the ABR Explorer to support currency and reliability of data in our holdings.

All data used will rely on the information being readily available to the public. The data being sought for this project is focussed on organisations, rather than individuals, though data on sole traders will be included. No sensitive information will be handled.

The public information will be loaded and stored in approved departmental data environments (Databricks/SQL) with connections to SID and Power BI reports. The data environments are resource group controlled and only development programmers will have direct access to this data. Approved staff will be able to view the outputs via SID and Power BI reports. A Privacy Impact Assessment (PIA) has been completed on the use of SID, its safety protocols and procedures, and the use of open-source data within its environment. Including for the purposes of data matching activities with existing and future information held in SID. In addition, a PIA has been completed on Databricks and a Privacy Threshold Assessment on open source data. This assessment has considered, and aligns with, the other PTA and PIAs.

This data will be used by operational staff to support compliance activities through checks and the identification of linkages—such as undeclared interests, organisational affiliations, and relationships.

How many individuals' personal or sensitive information will be handled in the project or initiative?

Approximately
22,000,000

Section 2: New or changed ways of handling personal information

Q2. Will personal information be handled in a new or changed way?

If you answered 'yes', identify the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s) by checking the relevant boxes below.

Yes

- | | |
|-------------------------------------|---|
| ☒ | The <u>nature or type</u> of the personal information being handled is new or different. |
| ☐ | The <u>scope</u> of the personal information being handled is new or different. |
| ☒ | The personal information is being handled in a new or different <u>context</u> . |
| ☐ | The <u>purpose</u> for which the personal information is being handled is new or different. |
| ☐ | The <u>risk</u> of handling the personal information is new or different. |

If not listed above, explain the different way(s) personal information is being handled in this project or initiative compared to the department's existing practice(s).

Note, the Compliance Intelligence team currently accesses the data through the ABR ABN Lookup ([ABN Lookup](#)). The different context is the bulk handling of the data through Databricks and SQL.

If you answered 'no', explain the way personal information is being handled in this project or initiative which is the same or similar to the department's existing practice(s).

You should provide the name of the same or similar project or initiative where the practice(s) have been assessed previously and reflect on whether the controls are current and working, or will be working, well in this project or initiative.

Section 3: Likely impact on the privacy of individuals

Q3. Is the project or initiative likely to have a significant impact on the privacy of individuals?

No

To assess if the project or initiative is likely to have a significant impact, identify if any risk factors below apply:

- | | |
|-------------------------------------|--|
| ☒ | Handling large amounts of personal information. |
| ☐ | Handling sensitive information ³ . |
| ☐ | Handling personal information in a way that is likely to raise public concern or unlikely to have community support. |
| ☐ | Handling the personal information of individuals who are vulnerable. ⁴ |
| ☒ | Handling personal information where there may be negative impacts on physical and mental wellbeing of individuals or consequences for reduced access to public services, discrimination, financial loss or identity theft. |
| ☐ | Disclosing personal information outside of the department, including to other Commonwealth agencies and/or contracted services providers. |
| ☐ | Using or disclosing personal information for profiling or behavioural predictions. |
| ☐ | Using personal information for automated decision-making. |
| ☐ | Collecting personal information through systematic monitoring or tracking of individuals. |
| ☒ | Collecting personal information without individuals' consent or without telling individuals their personal information is being collected. |
| ☒ | Using information for data matching or linking unconnected personal information. |
| ☐ | Developing legislation to modify the operation of the <i>Privacy Act 1988</i> or seeks to rely on the 'required or authorised by law' exception in the Australian Privacy Principles. |

³ Sensitive information is information or an opinion about an individual's racial or ethnic origin, political opinions, membership of a political association, religious beliefs or affiliations, philosophical beliefs, membership of a professional or trade association, membership of a trade union, sexual orientation or practice or criminal record, as well as health information about an individual or genetic or biometric information about an individual.

⁴ May include children, 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.

☒ Handling personal information for activities of a long term or permanent duration.	
If not listed above, describe the risk factors that would contribute to the project or initiative having a significant impact on the privacy of individuals.	
If you answered 'no', explain why the project or initiative is unlikely to have a significant impact on the privacy of individuals, including what, if any, mitigation strategies your project or initiative has or intends to implement to reduce the level of privacy risk:	
The information to be used in this project is already available to the public through general searches, with all webpages easily accessible. Data sets for the purposes of this project are accessed through ABR Explorer and analysis will focus primarily on the organisations rather than individuals. The Compliance Intelligence team closely adheres to departmental privacy and security protocols in protecting the use of information. Furthermore, any information that could be used for an adverse action against a participant of a departmental program will direct staff responsible for these actions to return to the source of the data. This is an intelligence project. As a result, the privacy impact on individuals and organisations that could be captured by the program has no additional risk compared to the base level that exists for the information already being openly available and regularly updated by the relevant official Commonwealth data custodians.	
Is the project or initiative consistent with the department's commitment to respecting and protecting the personal information it holds?	Yes
If you answered 'no', explain why the project is not consistent with the department's commitment to respecting and protecting the personal information it holds.	

Outcome

If you answered 'yes' to the above three questions, it is likely that your project or initiative may pose a high privacy risk and a PIA will be required under the Privacy Code.

Outcome	A PIA is not required as there are no high privacy risk elements or no new or changed ways of handling personal information
---------	---

I confirm that this threshold assessment is accurate and complete. The threshold assessment correctly identifies personal and sensitive information handled in this project or initiative, and appropriately assesses the likelihood that the project or initiative includes potentially high privacy risk elements.

Approved by: s 22(1) , s 22(1) , Compliance Branch

Date: 17/06/2025

A copy of this privacy threshold assessment must be retained on file and sent to the [Privacy Officer](#).