Australian Bureau of Statistics

PRIVACY IMPACT ASSESSMENT

Secure Environment for Analysing Data

December 2022

Contents

1. INTRODUCTION

1.1 Background

The Australian Bureau of Statistics (ABS) has developed a new service offering which provides a data service for partners[1] to securely hold their data, including personal information, for analysis purposes and possible sharing with others. The new service, called the Secure Environment for Analysing Data (SEAD) service was designed to enable safe data sharing under arrangements such as the *Data Availability and Transparency Act 2022* (Cth) (**DAT Act**). It also provides a contemporary analytical platform for the ABS or external partners to undertake complex analysis of large datasets.

The ABS DataLab has been in operation since 2016. It is a secure analytical cloud environment for users to undertake complex analysis of detailed information about people, households, businesses, or other entities (microdata) for statistical research or modelling. The ABS uses a series of controls as part of the Five Safes Framework (Five Safes) to mitigate the risk of disclosure in the DataLab.

Commencing in June 2022, the SEAD service can create multiple self-contained instances (pods) within the cloud environment that also underpins the ABS DataLab. Each instance (SEADpod) is administered by, or on behalf of, the ABS or partner using the SEAD service.

The SEAD service:

- aligns with the ABS Data Strategy 2021–22 to 2025
- supports the Australian Data Strategy
- supports data sharing under the relevant laws and legal instruments including the DAT Act.

The SEAD service is separate to the ABS DataLab. Partners who are provisioned a SEADpod have exclusive control of that secure, self-contained environment. This allows each SEADpod to function separately and independently of one another. The service enables partners to leverage the existing controls in place for ABS DataLab using the Five Safes Framework in accordance with their requirements, while maintaining the underlying safe settings protections. The SEAD service offers users the same functionality as the ABS DataLab to enable analysis of microdata. It also supports a range of other functions including research and testing for creating data products and data preparation and process improvement for data integration productions.

The Australian Government Department of Finance (DoF) was the first partner to test a beta SEADpod. Feedback from beta testing has been used to refine the SEAD service. From June 2022, the DoF is exclusively administering its own SEADpod.

[1]The ABS is currently offering SEAD to Commonwealth agencies. Future partners could include other entities such as State and Territory agencies.

ABS plans to use SEADpods from late 2022 for statistical and operational purposes[2], especially for large projects that would benefit from a cloud environment. The ABS is also considering potential updates to multi-agency data integration project (MADIP) data handling processes to transfer data from the Secure Data Integration Environment (SDIE) to SEADpods for approved operational and statistical uses.

1.2 Benefits of SEAD

The ABS DataLab and SEAD environments are:

- Secure: Certified to handle 'Protected' data and subject to a regular program of independent security audits and systems accreditations, including the Information Security Registered Assessor Program (IRAP)[3].
- Contemporary: Scalable cloud-based analytics environments that support a suite of analytical languages, including R, Python, Stata and SAS, and modern data science and machine learning platforms, including Azure Databricks. All microdata in the ABS DataLab and SEAD will be stored in the cloud using data centres that are physically located in Australia.
- Cost-effective: Supports cross-agency use of the SEAD service on a cost recovered basis. Partners benefit from the ABS' investments in developing advanced data infrastructure with sophisticated analysis and data sharing capability.

Partners can take advantage of the SEAD service to:

- Manage risks associated with their current data sharing activities.
- Expand their data sharing activities to create more value, and possibly share data with others.

There are also a range of benefits for ABS use of the SEAD service, including:

- Access to a range of data science analytical tools including but not limited to Python, R and RStudio, STATA, QGIS and SAS.
- Ability to undertake research and testing to improve ABS operations and statistical information with ABS-held data.
- Access to the benefits of a cloud computing environment to enable improvement in operations, including faster turn-around times for data integration projects.

[2] Statistical use refers to any use that directly affects and/or improves the statistical outputs and statistical information of ABS products and services. Operational use refers to any use that facilitates ABS business operations including to coordinate, produce and distribute statistical information and services.
[3] Security audits and systems accreditations are described in more detail in the 2020 Cloud DataLab PIA. See: https://www.abs.gov.au/about/legislation-and-policy/privacy/privacy-impact-assessments

1.3 Scope and purpose of the PIA

The purpose of this Privacy Impact Assessment (PIA) is to consider the potential privacy impacts on people whose personal information may be used as part of the SEAD service. This includes microdata contained in a SEADpod, and the personal information of users of the SEAD system (authorised partner administrators and users as well as ABS users). It will also identify, assess, and outline risk mitigation strategies to manage privacy impacts.

The scope of this PIA will cover two broad use cases outlined below.

- **Model zero: ABS statistical and operational use of SEAD**
- **Model one: Partner self-service use of SEAD**

This PIA builds on the privacy work conducted as part of the 2020 Cloud DataLab PIA and the 2022 Multi-Agency Data Integration Project (MADIP) PIA Update. These PIAs have considered privacy issues relevant to this project and are available on the ABS website.

The ABS is considering future use cases for SEAD including models which involve data sharing between the ABS and partners. The ABS will update this PIA as needed for new operating models considered for the SEAD service in the future.

Further detail about SEAD operating models is outlined in later sections of this report.

1.4 Operating context

The ABS administers the SEAD service within its existing cloud infrastructure that is also used for the ABS DataLab. SEAD can be used by the ABS and partners to share and analyse data using sophisticated data science tools (computer software). Data will not be transferred between SEADpods and ABS DataLab project locations.

SEAD offers two main operating models.

- **Model zero: ABS statistical and operational use by ABS Officers[4].**
  The ABS may use the SEAD service for statistical and operational purposes. For example, the ABS plans to use a SEADpod to undertake research into the testing and evaluation of new methods, tools and environments for data linking. This will allow the ABS to evaluate software and architectural solutions to improve integrated data assets.

  Subject to data custodian consent, the ABS also plans to use the SEAD service to undertake data preparation activities for data integration projects. This will allow the ABS to leverage the benefits of cloud computing to provide scalable and faster turnaround times for data integration projects. ABS officers will always maintain functional separation and handle

[4] ABS officers refer to ABS staff and officers seconded to the ABS from Commonwealth agencies who have been approved for access to either linkage or analytical data within a SEADpod.

either linkage or analytical information[5] for data integration projects for approved statistical and operational purposes only. ABS officers cannot access or see other data held within ABS DataLab, including in other SEADpods.

- **Model one: Partner self-service use of SEAD**
  Partners may use the SEAD to analyse their own data and possibly share the results with others. Under this model, the partner retains exclusive control and management of their data, users, projects, input vetting and output vetting through self-service features in their own SEADpod. ABS SEAD systems administrators are not permitted to access partner information unless first authorised by the partner.

Broad features and responsibilities of the models are described in Table 1 below.

Table 1: Features and responsibilities of SEAD operating models

Feature	Model zero – ABS operational and statistical use	Model one – Safe environment as a service
Cyber system security management	ABS	ABS
Data control	ABS	Partner
User management	ABS	Partner
Project management	ABS	Partner
Input vetting	ABS	Partner
Output vetting	ABS	Partner
Self-service arrangements	ABS	Partner
Statistical and data integration technical expertise and capability	ABS	Partner

2. COLLECTION OF INFORMATION

2.1 Collection

Model zero

Under model zero, the ABS will use information already held in the ABS secure IT environment. Information will be transferred into the SEADpod via secure internal ABS channels. Subject to data custodian agreement, this may include using information already collected for use in integrated data assets, such as MADIP. Collection and transfer of information for MADIP is described in the 2022

[5] Linkage information usually includes personal identifiers such as name, address and date of birth, or other identifiers like Australian Business Numbers. Analytical information refers to variables of interest for analysis, such as occupation, income and health services use, or business type and industry.

MADIP PIA Update. For MADIP data integration projects, this PIA will build upon the current MADIP information flow to allow transfer of data from the SDIE to SEADpods for approved statistical and operational uses.

Model one

Under model one, all information will be collected by the partner as the data custodian and securely transferred from the partner environment to the partner's SEADpod based in the ABS' existing secure cloud environment. The data will be transferred to the ABS via secure electronic means (see Section 4 Information and information flows). Partners can share their data in the SEADpod by allowing access to others through the self-service user management feature.

2.2 Legislation

The legislative arrangements for use of the SEAD service differ for each operating model.

Model zero

Information collected by the ABS under the *Census and Statistics Act 1905* (Cth) (**Census and Statistics Act**) or other relevant legislation can be used in ABS SEADpods by ABS officers. The information may include 'personal' or 'sensitive' information as defined by the *Privacy Act 1988* (Cth) (**Privacy Act**).

Model one

The information contained in a SEADpod is information that is likely to have been collected by the partner under its own legislation or shared with them under other relevant legislation. Partners will have the right to handle the data in the SEADpod.

The ABS acquires information from partners in accordance with its functions outlined in section 6 of the *Australian Bureau of Statistics Act 1975* (Cth) (**ABS Act**). This involves holding partner data for the purpose of providing the SEAD service and providing authorised users access to the data.

Partner data provided to the ABS may be 'personal' or 'sensitive' information as defined by the Privacy Act. The ABS considers that while operating the SEAD service it may 'hold' personal information from partners as per the Privacy Act which states that, 'an entity holds personal information if that entity has possession or control of a record that contains the personal information'. The ABS acts in accordance with its obligations under the Privacy Act to ensure that personal information held is managed in accordance with the principles set out in legislation, including ensuring personal information is kept safe from unauthorised access and misuse.

Under its obligations, the ABS is:

- Responsible to take active measures to ensure the security of personal information held.
- Subject to the requirements of the Notifiable Data Breaches scheme, in conjunction with the partner.

3. INTERACTIONS WITH ABS DATALAB

The ABS SEAD service is separate to the ABS DataLab but shares the same secure data infrastructure. SEADpods are a self-contained instance provisioned within the ABS cloud environment also used for the ABS DataLab. The work carried out in SEADpods is independent of ABS DataLab projects and data made available in the ABS DataLab.

SEADpod users can request data science tools that are currently not available in the ABS DataLab environment. However, the ABS manages the data science tools made available within the SEADpod and may decline to make available any tools that are identified as a security risk.

3.1 ABS DataLab

The ABS DataLab is a secure analytics environment that provides safe access to de-identified[6] microdata. The ABS provides access to approved users for approved projects so they can undertake research aimed at informing the development of social, economic and environmental policies.

In 2020, the ABS replaced the ABS DataLab service with cloud-based infrastructure to futureproof its use as the number, scope and complexity of research projects using ABS microdata increases. The ABS engaged Microsoft to provide services for the cloud-based infrastructure through the over-arching service agreement with the Australian Government (known as VSA4) and subsidiary bilateral agreements.

The processes and controls underpinning the ABS DataLab, including secure access to de-identified microdata, remained largely unchanged following the replacement. However, as the mechanism for service delivery changed, a privacy impact assessment (PIA) was required.

In 2020, the ABS undertook a PIA to evaluate the privacy impacts of transitioning the ABS DataLab to a cloud-based service. This is consistent with the Australian Government Office of the Australian Information Commissioner's Guide to undertaking privacy impact assessments.

The ABS has implemented the recommendations arising from the 2020 Cloud DataLab PIA, most of which related to information about researchers using the DataLab. Recommendations included:

- updating online information to explain the storage and security of microdata in the cloud-based ABS DataLab
- upholding information security in line with the Australian Government Attorney-General's Departments Protective Security Policy Framework
- assessing security requirements against the Australian Government Australian Signals Directorate Australian Cyber Security Centre's Information Security Manual

[6] Personal information is de-identified 'if the information is no longer about an identifiable individual or an individual who is reasonably identifiable' (section 6(1) of the Privacy Act).

- participating in the Australian Signals Directorate's Information Security Registered Assessors' Program
- releasing an ABS DataLab privacy notice in line with Australian Privacy Principle (APP) 5 — Notification of the collection of personal information to inform approved users about the collection, use and disclosure of their personal information
- updating ABS DataLab user agreements and registration process in line with the ABS DataLab privacy notice
- developing a policy on the deletion and retention of ABS DataLab user account information and other related personal information.

Further information on the 2020 Cloud DataLab PIA, including the ABS response and implementation report, is provided at the ABS website.

4. INFORMATION AND INFORMATION FLOWS

4.1 Types of information

The Privacy Act defines personal information as:

> *…information or an opinion about an identified individual, or an individual who is reasonably identifiable:*
>
> *a) whether the information or opinion is true or not; and*
>
> *b) whether the information or opinion is recorded in a material form or not.*

Two types of personal information may be involved in this project:

- microdata contained in a SEADpod
- information about approved SEADpod users.

4.2 Information flows – microdata contained in a SEADpod

High level information flows for model zero and model one are described below and summarised in Figure 1, Appendix A. Figure 1 also includes the information flow for analysing integrated data in the ABS DataLab to highlight the similarities and differences in data handling practices.

Model zero

The ABS is expected to use one or more SEADpods for statistical and operational use by ABS officers.

The types of personal information that may be accessed will vary, depending on the nature of the datasets and the approved project use. Types of personal information will typically include linkage data such as name, address, date of birth, and sex/gender, or analytical data. The ABS may also access personal information which has been anonymised[7] when using the SEAD service.

Linkage data will be held separately from analytical data, in adherence with the separation principle and functional separation[8]. Linkage and analytical information can never be accessed together and access to these different information sets is restricted both within and between SEADpods so that no ABS officer is able to access both sets of information simultaneously. For example, an ABS officer with access to linkage data in the SEADpod will not have access to analytical data in the SDIE.

The ABS will continue to apply the Five Safes for ABS SEAD projects. The controls applied will vary for each project and may be different to the existing controls in place for projects conducted in the ABS DataLab. For example, some projects may require personal identifiers (such as name and address) for testing purposes.

For model zero, data necessary for approved projects will be transferred securely from locations in the ABS secure IT environment (such as the SDIE) to ABS SEADpod(s).

One of the initial uses will be to conduct research into the testing and evaluation of new methods, tools and environments for data linking. In this example, personal identifiers, such as name and address (linkage data) will be securely transferred into an ABS SEADpod to enable this research. Access to this data within the SEADpod will be restricted to approved ABS officers only. No analytical information relating to these records will be held in this environment.

Model one

The ABS enters into an agreement with a partner to provide the SEAD service. The SEADpod is managed using a number of data administration roles as described in Table 2 in Section 4.3. The partner nominates select staff to be their Primary Administrator(s). ABS SEAD systems administrators provision a partner with a SEADpod and nominated partner staff with a Primary Administrator role.

[7] The 2022 MADIP PIA Update describes the ABS' processes for anonymising data.
[8] Further details on the separation principle and functional separation can be found in the 2022 MADIP PIA Update.

Partner Primary Administrators create and manage administrator and analyst roles. Partner administrators are responsible for secure transfer of their own data into and out of their SEADpod. Data is securely transferred in accordance with existing ABS infrastructure and processes, with support provided by the ABS (where required). The overall number of partner administrator roles that can be provisioned for a SEADpod are limited by agreement.

After the partner SEADpod is provisioned, ABS SEAD systems administrators provide IT security services within the SEADpod as requested by the partner.

4.3 Information flows - data about approved SEADpod users

The ABS collects, stores, uses and discloses information about approved SEADpod users for the purposes of managing and operating the SEAD service. This includes information about:

- ABS officers in the ABS SEAD systems administrator roles
- ABS officers using a SEADpod for approved projects
- approved users accessing a SEADpod administered by a partner (including partner primary administrators, administrators, and partner analysts)

The types of personal information collected include:

- name
- employer
- contact information
- email address
- Some location information in the form of originating internet protocol (IP) address

Information about the roles and functions of SEADpod users is described in Table 2 below.

Table 2: Roles and functions of SEADpod users

Role	Function	Operating model
ABS SEAD systems administrator	Provision a SEADpod Perform cyber security and technology performance checks and other technology functions as required	All models
	Provision Primary Administrator roles for partners	Model one
ABS Officers [9]	Document and apply approved Five Safes controls per project Perform statistical and operational activities for approved projects Vet and transfer safe outputs (if any, as required) to the ABS secure IT environment	Model zero
Partner Primary administrator & administrators	Self-service management of the SEADpod including: • Create and manage administrator and analyst roles • Securely transfer their own data into and out of their SEADpod	Model one
Partner analyst	Use partner data within the SEADpod	Model one

[9] ABS officers refer to ABS staff and officers seconded to the ABS from Commonwealth agencies who have been approved for access to either linkage or analytical data within a SEADpod.

5. PRIVACY ISSUES AND ANALYSIS

The ABS has robust governance arrangements in place for the ABS DataLab. The SEAD is based on those arrangements and so also meets a high standard in terms of privacy best practice. Many of the privacy considerations that might otherwise arise have already been addressed in the 2020 Cloud DataLab PIA as well as previous MADIP PIA Updates, which are available on the ABS PIA webpage. These related privacy assessments provide a comprehensive analysis of the projects against the requirements of the Privacy Act and in particular, the Australian Privacy Principles.

This privacy analysis is structured around key privacy issues in relation to information contained in a SEADpod and about SEADpod users. Where possible, existing mitigation strategies are noted. The ABS considers that sufficient protections are in place and that the issues identified in this PIA are a low risk to privacy.

5.1 Information in the SEADpod

5.1.1 Maintaining security of personal information during transfer

The ABS is committed to keeping the personal information it holds safe and secure. Use of the SEAD service may introduce new data security risks when information is transferred into and out of a SEADpod.

Under model zero, only data that is already held securely by the ABS will be transferred to a SEADpod. Data transfer into a SEADpod will use existing secure transfer channels and processes established for transferring data between ABS' internal environments and the ABS DataLab.

Partners commit to complying with the Australian Government Protective Security Policy Framework and other ABS security procedures as required when they engage the ABS to provide the SEAD service. Under model one, it is the partner's responsibility to ensure any information, including personal information, is transferred to the ABS in a secure manner to prevent unauthorised disclosure. Partners are responsible for ensuring information is protected from interception and that security for data transfer is appropriate. These protective behaviours are also similar to those expected for approved ABS DataLab researchers[10], for example using secure internet connections and keeping credentials secure.

Once information is transferred into a SEADpod it is kept secure in accordance with current ABS data protections. The ABS has extensive security systems in place to keep personal information safe and secure. This includes independent IRAP certification for the ABS DataLab, ongoing security audits and regular IT security testing to ensure continued security of personal information of users. The ABS also has an inhouse Information Technology (IT) team dedicated to minimising ongoing security risks. The range of security controls in place are detailed extensively in the 2020 Cloud DataLab PIA and the MADIP PIAs.

[10] For more details on ABS DataLab researcher responsibilities, see the 'Using DataLab responsibly' guidance published to the ABS website.

5.1.2 Fulfilling obligations under privacy requirements

There is a risk of failure by the ABS or a partner to meet legislative requirements for privacy when using the SEAD service. This may include use of personal information in a SEADpod for unauthorised purposes.

The ABS protects privacy and is committed to keeping information safe and secure. The ABS use of the SEAD service (model zero) meets legislative requirements for handling personal information, including the secrecy provisions of the Census and Statistics Act. The ABS projects using the SEAD service will be conducted under similar data handling arrangements to those in MADIP and ABS DataLab, including strict adherence to the separation principle, meaning linkage and analytic data are never accessed together. The ABS will also continue to apply the Five Safes for ABS SEADpod projects to assist in meeting legislative requirements regarding disclosure risk.

It is the responsibility of the partner to ensure that use of personal information contained in a SEADpod is within the purpose for which it was collected or authorised secondary purposes and that their SEADpod users are made aware of their obligations under the relevant legislation. The ABS strongly encourages partners to undertake their own privacy assessments for their use of the ABS SEAD service where appropriate.

The ABS recognises that it is subject to the requirements of the Australian Notifiable Data Breaches scheme, in conjunction with the relevant partner, as the operator of the SEAD service. Incident response and communication protocols for notifiable data breaches will be outlined in agreements (Memorandum of Understandings) between the ABS and the partner.

5.1.3 Protecting against disclosure of data

There is a potential risk that personal information contained in a SEADpod is accessed by unauthorised users. In addition, the information stored in a SEADpod may not be de-identified which means there is an increased risk of identification of personal information. There is a risk of inadequate or improper implementation of access controls by ABS officers or partner staff.

The ABS deploys a broad and extensive range of security controls, including access controls for the ABS DataLab and SEAD. These controls ensure that microdata stored in the ABS DataLab and SEAD is protected and secure from external breaches. The ABS DataLab is subject to periodic IRAP assessments, as prescribed in the Australian Government Information Security Manual (ISM) and Protective Security Policy Framework (PSPF). The ABS DataLab is rated as PROTECTED level of security standards. Security controls are detailed extensively in the 2020 Cloud DataLab PIA and the MADIP PIAs.

When using the SEAD service, the ABS and partners are responsible to:

- Ensure user access is appropriate and authorised
- Apply controls to manage privacy risks, and
- Comply with obligations in accordance with Privacy Act before data disclosed

Under model zero, the ABS will continue to manage disclosure risk using the Five Safes. The ABS projects using the SEAD service will be conducted in strict adherence to the separation principle, meaning linkage and analytic data are never accessed together. Adherence to the separation principle helps reduce disclosure risk and minimise the impact of disclosure, were it to occur.

The ABS has a range of protections and controls in place to manage ABS access to information in a partner's SEADpod. The ABS undertakes regular reviews and audits of access controls. As established in the agreement between the ABS and the partner for model one:

A. Only a limited number of ABS staff (ABS SEAD systems administrators) can access partner information for the purposes of providing the service

B. ABS staff are not permitted to access partner information unless first authorised by the partner

5.1.4 Deletion and retention of data

There is a risk that information may be kept in a SEADpod for longer than required.

Under model zero, the ABS will delete microdata contained in a SEADpod when no longer needed, consistent with the:

- Privacy Act and the ABS Privacy Policy for Statistical Information, and
- Australian Government records management regime regulated by the *Archives Act 1983* (Cth) (**Archives Act**) and the relevant general and ABS-specific records authorities[11].

The ABS will apply current internal governance processes to approved ABS projects using the SEAD service, to ensure appropriate deletion and/or retention of data.

Under model one, the deletion of information contained in a SEADpod is the responsibility of the partner. Information will be retained as required by the partner, and in compliance with the obligations under the Archives Act. The agreement between the ABS and partner outlines partner responsibilities for deletion of information and ABS responsibilities for backup and recovery of information if required.

The ABS is responsible for managing the cloud-based infrastructure underlying the SEAD service. For more detailed information, see the 2020 Cloud DataLab PIA.

[11] The National Archives Authority issues general records authorities to Australian Government agencies. The ABS also adheres to specific records authorities.

5.2 Information about SEADpod users

5.2.1 Risk of inappropriate use

The ABS handles information about SEADpod users in accordance with the ABS Privacy Policy for Managing and Operating Our Business, and similar to ABS DataLab users. There is an operational need to retain SEADpod user information so that, in the event of misuse, including disclosure breach, there is a full history of the individuals who have accessed data over time.

SEADpod users are provided with a link to the ABS DataLab privacy notice during the login process to the SEADpod.

The ABS adheres to a deletion and retention policy specific to DataLab User accounts and related personal information. This policy governs ABS' approach to deletion and retention of user personal information, consistent with requirements of the Privacy Act and the Australian Government records management regime regulated by the Archives Act 1983. The ABS will expand on the current DataLab user deletion and retention policy to document the approach for SEADpod user information.

6. SUMMARY AND RECOMMENDATIONS

The SEAD service uses established cloud infrastructure to securely handle data and the privacy impacts of the DataLab were extensively assessed as part of the 2020 Cloud DataLab PIA. This PIA has built upon previous work to consider any additional privacy impacts associated with the SEAD service for operating models zero and one. Appendix B provides a summary of the privacy assessment and recommendations against each of the APPs.

Based on this assessment, ABS considers that sufficient protections are in place to protect the privacy of personal information for the SEAD service. While the ABS has determined the privacy risks are low, five high level recommendations are proposed to further enhance compliance and/or privacy protections for individuals.

Recommendation 1: ABS to be open and transparent about the handling of personal information for the SEAD project, including requirements to:

A) Publish information about the SEAD to increase public awareness about the service and how data is safely handled within the SEAD.

B) Review and update ABS policies (including the DataLab user deletion and retention policy) and practices related to handling of personal information to include the SEAD service.

Recommendation 2: ABS to review and update internal processes, including for assessment, approval and data handling practices for ABS use of the SEAD service.

Recommendation 3: ABS to develop standardised user agreements and guidance material about the intended application of the SEAD, with specific mention of ABS and partner roles and responsibilities.

Recommendation 4: Partners are responsible to ensure their data use requirements are adhered to by all authorised users in their SEADpod, including partner administrators and partner analysts.

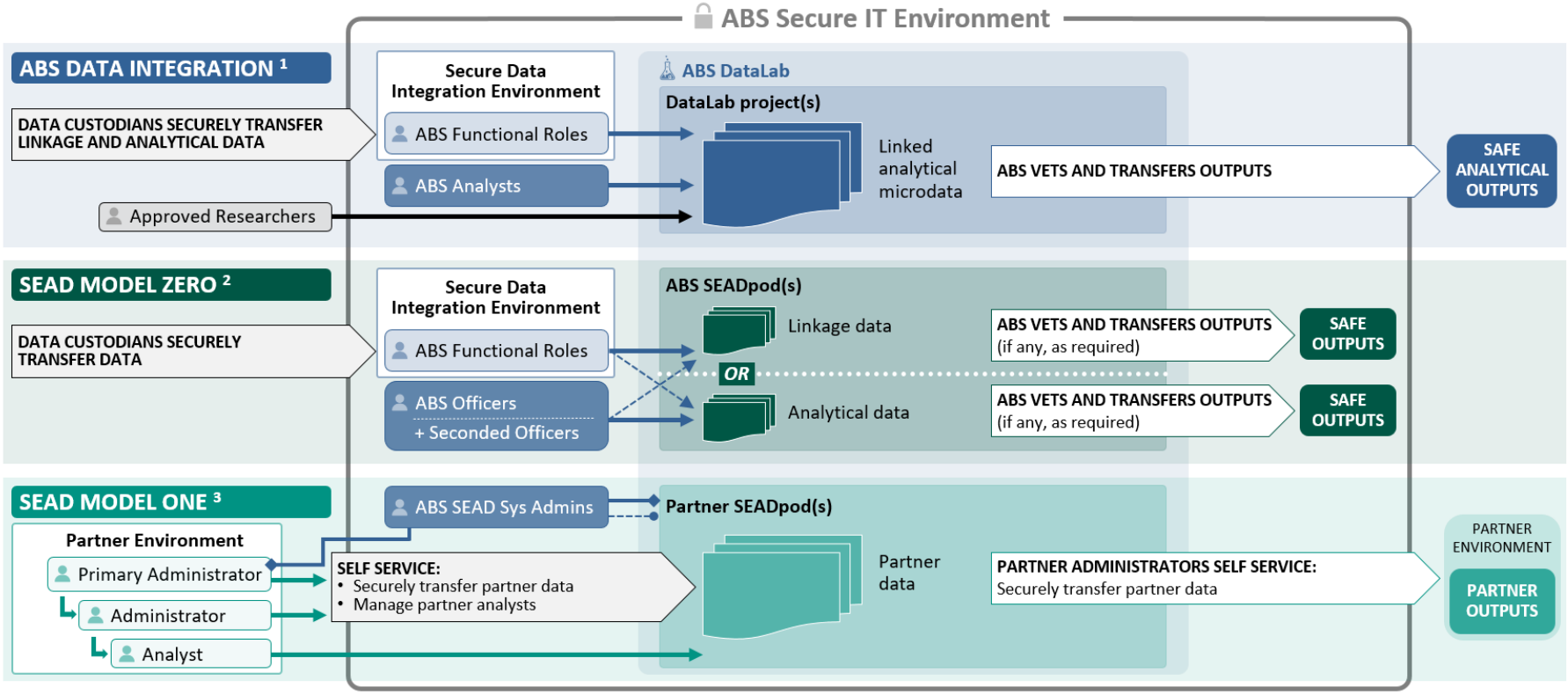
Recommendation 5: Partners are responsible to ensure user access is conducted in accordance with relevant training and guidance material in relation to use of the system.

The ABS will report on the implementation of these recommendations within one year of publication of this PIA.

Outcomes from this PIA will be used to inform future models of the SEAD service offering. The ABS will undertake updates to this PIA where any changes to the SEAD service are expected to significantly impact the privacy of individuals. This may include any new operating models considered for the SEAD service in the future.

APPENDIX A: COMPARATIVE INFORMATION FLOWS

FIGURE 1: Comparative data flow



1. **ABS Data Integration**: The ABS uses a series of controls to provide de-identified linked analytical microdata for analysis in DataLab. Linkage and analytical data is kept separate and prepared for analysis by ABS staff in specific functional roles (Librarian, Linker, Assembler). Linked analytical microdata is transferred to a DataLab project where approved researchers and ABS analysts access the data for approved projects only. For more information about these controls, see the 2022 MADIP PIA Update.
2. **SEAD Model Zero:** Linkage and analytical data is kept separate; prepared and transferred from the ABS Secure Data Integration Environment (SDIE) into an ABS SEADpod by ABS staff in the functional role(s) appropriate to the data. ABS staff and officers seconded from Commonwealth agencies handle either linkage or analytical data within a SEADpod for approved statistical and operational purposes only. Any outputs are vetted and transferred out of an ABS SEADpod into an appropriate location in the ABS Secure IT Environment. For example, linkage microdata output from a SEADpod would be transferred back to the SDIE. Functional separation is maintained at all times.
3. **SEAD Model One:** ABS SEAD Systems Administrators provision a partner with a SEADpod and selected partner staff with a Primary Administrator role. Partner Primary Administrators create and manage administrator and analyst roles. After the partner SEADpod is provisioned, ABS SEAD Systems Administrators provide IT security services within the SEADpod as requested by the partner.

APPENDIX B: SUMMARY OF PRIVACY ASSESSMENT AND RECOMMENDATIONS

Table 3. Summary of privacy assessment and recommendations against the APPs.

APP	Assessment	Commentary and recommendations
APP 1: open and transparent management of personal information	Compliant - further best practice improvements recommended	The ABS privacy policies, privacy statements and collection notices published to the ABS website describe how the ABS manages personal information, both for ABS business operations and for producing statistics. The ABS has practices in place that promote data use transparency, including publishing Privacy Impact Assessments to the ABS website and publishing information about data integration projects to project registers. **Recommendation 1:** ABS to be open and transparent about the handling of personal information for the SEAD project, including requirements to: A. Publish information about the SEAD to increase public awareness about the service and how data is safely handled within the SEAD. B. Review and update ABS policies (including the DataLab user deletion and retention policy) and practices related to handling of personal information to include the SEAD service. **Recommendation 3:** ABS to develop standardised user agreements and guidance material about the intended application of the SEAD, with specific mention of ABS and partner roles and responsibilities.
APP 2: Anonymity and pseudonymity	Not applicable – no action recommended	Personal information collected by the ABS is generally exempt from the anonymity and pseudonymity principle. The ABS provides anonymity to individuals in appropriate circumstances, such as for browsing ABS website content. Some ability for anonymity has been provided for some ABS surveys in the past. The ABS requires identification for partners and individual users to facilitate access to the SEAD service. APP 2 does not apply as it is impracticable for the ABS to deal with partners or individual users who have not identified themselves or have used a pseudonym. ABS use of SEAD (model zero) will not change how the ABS collects personal information as part of the creation of microdata products. Compliance with APP 2 is addressed in further detail in previous PIAs including the 2019 MADIP PIA Update. Partners are responsible for ensuring that personal information they transfer into their SEADpod has been collected in compliance with APP 2.

APP	Assessment	Commentary and recommendations
APP 3: Collection of solicited personal information	Compliant – further best practice improvements recommended	The ABS collects information about approved SEADpod users for the purposes of managing and operating the SEAD service. This collection is reasonably necessary for the ABS to perform its function and safely manage access to, and use of the SEAD service. The ABS handles information about SEADpod users in accordance with the ABS Privacy Policy for Managing and Operating Our Business, and similar to ABS DataLab users. SEADpod users are provided with a link to the ABS DataLab privacy notice during the login process to the SEADpod. Under model zero, the ABS will use information already held in the ABS secure IT environment. ABS use of SEAD will not change how the ABS collects personal information as part of the creation of microdata products. Under model one, all information will be collected by the partner as the data custodian and securely transferred from the partner's environment to the partner's SEADpod via secure electronic means. The ABS acquires and holds the partner's information in accordance with the ABS Act for the purpose of providing the SEAD service to the partner. Partners are responsible for ensuring their collection and use of information contained in their SEADpod is compliant with APP 3. **Recommendation 1B:** Review and update ABS policies (including the DataLab user deletion and retention policy) and practices related to handling of personal information to include the SEAD service.
APP 4: Dealing with unsolicited personal information	Compliant – no action recommended	The ABS has appropriate measures in place to manage the receipt of unsolicited personal information. There are limited opportunities for SEADpod users to supply unsolicited personal information to the ABS. Any unsolicited personal information received from SEADpod users will be handled in accordance with the ABS' policies and procedures. Under model zero, the ABS will use information already held in the ABS secure IT environment. ABS use of SEAD will not change how the ABS deals with unsolicited personal information received as part of the creation of microdata products. Under model one, partners retain exclusive control and management of their data, users, projects, input vetting and output vetting through the self-service features of their SEADpod. Partners are responsible for dealing with unsolicited personal information contained in their SEADpod.

APP	Assessment	Commentary and recommendations
APP 5: notification of the collection of personal information	Compliant - further best practice improvements recommended	SEADpod users are provided with a link to the ABS DataLab privacy notice during the login process to the SEADpod. The ABS will update the existing ABS DataLab privacy notice to inform SEAD users how their personal information will be handled. The DataLab privacy notice is also available on the ABS website. **Recommendation 1B:** Review and update ABS policies (including the DataLab user deletion and retention policy) and practices related to handling of personal information to include the SEAD service.
APP 6: use or disclosure of personal information	Compliant – further best practice improvements recommended	The ABS uses information collected about SEADpod users to operate the SEAD service. Personal information about SEADpod users may be shared with data custodians (model zero) or with partners (model one) as appropriate to the operation of the SEAD service. SEADpod users are provided with a link to the ABS DataLab privacy notice during the login process to the SEADpod. The ABS will update the existing ABS DataLab privacy notice to inform SEAD users how their personal information will be used or disclosed. Under model zero, the ABS projects using the SEAD service will be conducted under similar data handling arrangements to those using MADIP data in the ABS DataLab. Compliance with APP 6 is addressed in further detail in the 2022 and 2019 MADIP PIA Updates. Partners retain exclusive control and management of their data, users, projects, input vetting and output vetting through the self-service features of their own SEADpod. The ABS strongly encourages partners to undertake their own privacy assessments for their use of the ABS SEAD service where appropriate. **Recommendation 1B:** Review and update ABS policies (including the DataLab user deletion and retention policy) and practices related to handling of personal information to include the SEAD service.
APP 7: direct marketing	Not applicable – no action recommended	APP 7 provides that an organisation must not use or disclose personal information it holds for the purpose of direct marketing unless an exception applies. APP 7 may also apply to government agencies in specific circumstances. The ABS does not use or disclose personal information for direct marketing purposes and has not otherwise been prescribed for the purposes of s7A of the Privacy Act. APP 7 is not applicable to the ABS use of the SEAD service. The ABS may contact current and prospective SEAD users to advise on SEAD service features, in accordance with the ABS Privacy Policy for Managing and Operating Our Business. Partners are responsible for ensuring their use of personal information contained in a SEADpod is compliant with APP 7 where applicable.

APP	Assessment	Commentary and recommendations
APP 8: Cross-border disclosure of personal information	Compliant – no action recommended	The SEAD service uses existing cloud infrastructure that is also used for the ABS DataLab. Information contained in a SEADpod will be stored in the cloud using data centres that are physically located in Australia. Compliance with APP 8 is addressed in further detail in the 2020 Cloud DataLab PIA and the 2022 MADIP PIA Update. Partners are responsible for ensuring their handling of personal information contained in a SEADpod is compliant with APP 8, and that their privacy policies and collection notices are appropriate for their use of the SEAD service.
APP 9: Adoption, use or disclosure of government related identifiers	Not applicable - no action recommended	APP 9 does not generally apply to government agencies, except for prescribed commercial activities. Partners are responsible for ensuring their use of government related identifiers contained in a SEADpod complies with legislative requirements.
APP 10: Quality of personal information	Compliant – further best practice improvements	The ABS has processes and systems in place that represent reasonable steps to ensure the quality of personal information. The ABS manages information about SEADpod users in accordance with the ABS Privacy Policy for Managing and Operating Our Business, and similar to ABS DataLab users. The ABS expects SEADpod users to follow current guidance for ABS DataLab users. This includes requirements to provide accurate personal information and to update personal information as needed. APP 10 requirements for the ABS use of the SEAD service (model zero) are consistent with the assessment described in the 2019 MADIP PIA Update and the 2020 Cloud DataLab PIA. Partners are responsible for ensuring their use of personal information contained in a SEADpod is compliant with APP 10 where applicable. **Recommendation 1B:** Review and update ABS policies (including the DataLab user deletion and retention policy) and practices related to handling of personal information to include the SEAD service. **Recommendation 3:** ABS to develop standardised user agreements and guidance material about the intended application of the SEAD, with specific mention of ABS and partner roles and responsibilities.

APP	Assessment	Commentary and recommendations
APP 11: security of personal information	Compliant – further best practice improvements recommended	The ABS is committed to keeping the personal information it holds safe and secure. The ABS regularly reviews and takes reasonable steps to ensure the security of information. The ABS deploys a broad and extensive range of security controls, including access controls for the ABS DataLab and SEAD. The SEAD service uses the existing security systems in place for the ABS DataLab to keep personal information safe. The ABS DataLab is rated to a PROTECTED level of security standards, and so SEADpod(s) are an appropriate environment to securely hold personal information. The ABS will continue to maintain its IRAP certification for the ABS DataLab . Under model zero, the ABS applies additional controls including the Separation Principle and Five Safes Framework for managing disclosure of microdata. Under model one, partners are responsible for ensuring safe data handling practices for their data within the SEADpod and on release from the SEADpod environment. **Recommendation 2:** ABS to review and update internal processes, including for assessment, approval, and data handling practices for ABS use of the SEAD service. **Recommendation 4:** Partners must ensure their data use requirements are adhered to by all authorised users in their SEADpod, including partner administrators and partner analysts. **Recommendation 5:** Partners to ensure user access is conducted in accordance with relevant training and guidance material in relation to use of the system.
APP 12: Access to personal information	Compliant – further best practice improvements recommended	The ABS handles information about SEADpod users in accordance with the ABS Privacy Policy for Managing and Operating Our Business, and similar to ABS DataLab users. On request, the ABS can provide a SEADpod user with access to their personal information. Further detail is provided in the 2020 Cloud DataLab PIA. The ABS Privacy Policy for Statistical Information describes how individuals can access and correct their personal information where collected for the purposes of producing statistics. Under model zero, the ABS will use information already held in the ABS secure IT environment. APP 12 requirements for the ABS use of SEAD are consistent with the 2019 MADIP PIA Update. Under model one, partners retain exclusive control and management of their data, users, projects, input vetting and output vetting through the self-service features of their own SEADpod. ABS and partners will work together to ensure partner self-service use of SEAD is compliant with APP 12. **Recommendation 1B:** Review and update ABS policies (including the DataLab user deletion and retention policy) and practices

APP	Assessment	Commentary and recommendations
		related to handling of personal information to include the SEAD service. **Recommendation 3:** ABS to develop standardised user agreements and guidance material about the intended application of the SEAD, with specific mention of ABS and partner roles and responsibilities.
APP 13: Correction of personal information.	Compliant - further best practice improvements recommended	The ABS handles information about SEADpod users in accordance with the ABS Privacy Policy for Managing and Operating Our Business, and similar to ABS DataLab users. The ABS will adhere to the existing DataLab deletion and retention policy specific to DataLab users accounts in relation to correcting the personal information held. The ABS Privacy Policy for Statistical Information describes how individuals can access and correct their personal information where collected for the purposes of producing statistics. Under model zero, the ABS will use information already held in the ABS secure IT environment. APP 12 requirements for the ABS use of SEAD are consistent with the 2019 MADIP PIA Update. Under model one, partners retain exclusive control and management of their data through the self-service features of their own SEADpod. Partners are responsible for correcting personal information contained in their SEADpod as appropriate for compliance with APP 13. **Recommendation 1B:** Review and update ABS policies (including the DataLab user deletion and retention policy) and practices related to handling of personal information to include the SEAD service.

APPENDIX C: ACRONYMS AND GLOSSARY

Acronyms

Acronym	Term
ABS	Australian Bureau of Statistics
APP	Australian Privacy Principle
DoF	Department of Finance
IRAP	Independent Security Registered Assessors Program
MADIP	Multi-Agency Data Integration Project
PIA	Privacy Impact Assessment
SEAD	Secure Environment for Analysing Data

Glossary

Term	Description
ABS DataLab	A virtual cloud-based environment created by ABS for enabling scaled analysis of sensitive data and the use of contemporary and cost-effective data science tools.
ABS operational use	Operational use refers to any use that facilitates ABS business operations including to coordinate, produce and distribute statistical information and services.
ABS statistical use	Statistical use refers to any use that directly affects and/or improves the statistical outputs and statistical information of ABS products and services.
Analytical information / data	Analytical information / analytical data refers to variables of interest for analysis, such as occupation, income and health services use, or business type and industry.
Australian Privacy Principles	Principles contained in the Privacy Act 1988 (Cth) that regulate the way we collect, store, provide access to, use and disclose personal information.
Authorised / approved users	Means those who are authorised to access a SEADpod.
2020 Cloud DataLab PIA	The ABS conducted a Privacy Impact Assessment of Cloud DataLab in 2020. The Cloud DataLab PIA and ABS response are published on the ABS website.
Linkage information / data	Linkage information / linkage data usually includes personal identifiers such as name, address and date of birth, or other identifiers like Australian Business Numbers.
2022 and 2019 MADIP PIA Updates	The ABS conducted a MADIP PIA Update in 2022. The 2022 MADIP PIA Update and MADIP

Term	Description
	Board response are published on the ABS website. The 2022 MADIP PIA Update built on the 2019 MADIP PIA Update. The 2019 MADIP PIA Update is also published on the ABS Privacy Impact Assessments Register.
Microdata	Data in a unit record file that provides detailed information about people, households, businesses or other types of entities.
Partner	An entity with provisioned access arrangements to use the ABS Secure Environment for Analysing Data.
Personal information	As defined in section 6(1) of the Privacy Act.
Five Safes Framework	A multi-dimensional approach to management disclosure risk which poses specific questions to help assess and describe each risk aspect (or safe) in a qualitative way.
Secure Environment for Analysing Data (SEAD)	The SEAD is a data service that allows for the creation of secure, independent SEADpod instances. The ABS provides access to and technical administration of SEADpod instances.
SEADpod	A SEADpod is a particular instance of a secure, isolated container, created within the established cloud-based infrastructure underpinning the ABS DataLab for approved ABS or Partner users with specific security and data access functionality.
Sensitive information	As defined in section 6(1) of the Privacy Act.