Response to the independent Privacy Impact Assessment of MADIP

April 2018

The Multi-Agency Data Integration Project, or MADIP, is a partnership among Australian Government agencies to explore how to make better use of existing public data consistent with the Public Data Policy Statement.

On behalf of partners, the ABS commissioned an independent Privacy Impact Assessment (iPIA) of MADIP. The iPIA identifies privacy impacts of the project and outlines strategies to mitigate any residual privacy risks before the project moves into an operational phase from 1 July 2018.

MADIP partners are committed to upholding the privacy, secrecy and security of personal information, and to being transparent and open about the project.

To date, MADIP has tested the feasibility and value of combining important national datasets to create a comprehensive picture of Australia for research and statistical purposes, including to support policy analysis, decision making, and service delivery in Australia by governments at all levels.

The iPIA acknowledges there are strong measures in place to protect privacy for MADIP, including legislative safeguards, application of the separation principle, and restricting the use of data to research and statistical purposes which benefit the Australian community.

The iPIA identifies some areas for improvement and provides strategies for managing, minimising, or eliminating residual privacy risks. MADIP partners agree to the iPIA's recommendations and have commenced work to address issues raised in the iPIA.

RECOMMENDATIONS

R1. Improve openness online about data in the MADIP.

ABS should amend the MADIP website to indicate personal information is used by MADIP for statistical and research purposes, including data integration. A list of the linkage and analytical data variables could also be provided.

Agreed.

ABS is in the process of reviewing and updating MADIP content on the ABS website to provide more information and increase transparency. This includes providing more detail about the kinds of data in MADIP, the legal basis for MADIP, and how the data is used by government entities and researchers.

R2. Improve openness about data sources.

ABS may wish to amend publicly available information and relevant Privacy Policies to be more open about the collection of data from agencies and the datasets being integrated in MADIP.

Agreed.

ABS is updating the ABS and Census Privacy Policies to clarify data is shared and used for research and statistical purposes through data integration projects.

A MADIP Privacy Policy is being developed to outline how personal information is handled in the MADIP.

R3. Minimise data sharing.

MADIP governance arrangements and public material should clarify that data minimisation occurs both during data sharing and data access for authorised researchers. MADIP should enhance the minimisation of personal data sharing by:

1. ***Only sharing data items that are reasonably necessary***
2. ***Excluding irrelevant data items where possible***
3. ***Using data categorisation (e.g. Yes / No responses or bands) rather than specific data fields where possible.***

Agreed.

Data minimisation (including data categorisation) is a key feature of the MADIP. Data custodians (the agencies responsible for collecting data shared in MADIP) only share data necessary for use in MADIP. Access to MADIP data assets is only provided to the data necessary for an authorised purpose, such as particular statistical or research projects. These arrangements are consistent with the High Level Principles for Commonwealth Data Integration under which the project is conducted.

Where appropriate MADIP partner agencies will aim to use data categorisation (e.g. yes/no responses or bands) rather than specific data fields. However, partner agencies recognise in many cases researchers will require broader data fields when making use of the de-identified analytical data provided under MADIP. In this context, where MADIP partner agencies provide access to broader

fields of data, they are committed to sharing this data in a secure and safe way to ensure that the privacy, secrecy, and security of that data is maintained.

R4. Review and minimise the amount of sensitive data.

MADIP should implement a review of all sensitive data fields to assess whether it is reasonably necessary to acquire sensitive data. Unnecessary data fields should be removed from future data acquisition and deleted / quarantined from existing MADIP data holdings.

Agreed.

ABS manages all data acquired by MADIP consistent with the processes required when handling personal information. When providing public access to this data, ABS is legally obliged to ensure no individual is reasonably identifiable from the data remaining after the de-identification process. Public access is only given to the data necessary for each authorised project.

Consultation with users confirms all data included in MADIP is important for a range of research and statistical purposes.

R5. Amend ABS privacy notices to clarify scale of third party data acquisition.

To deliver best practice in openness and transparency, ABS may wish to review and amend privacy notices to clarify the scale of third party data acquisition, the use of automated and bulk third party data acquisition and the expanded list of third parties that are involved.

Agreed.

ABS is reviewing its privacy notices (such as online and on data collection forms) to clarify that information may be shared and used for research and statistical purposes consistent with legislation including the *Census and Statistics Act 1905*.

Detail on the scale of data shared is out of scope of these privacy notices and is provided in other information publicly available about MADIP.

MADIP operates in accordance with the High Level Principles for Commonwealth Data Integration, including minimising the data that is shared. Data sharing for MADIP is not an automated process and does not involve entire datasets: agencies agree to share data pursuant to a specific request(s), and provide a subset of population-based data items which are reasonably necessary for MADIP. This approach has been undertaken as part of MADIP partner agencies' commitment to ensure privacy considerations are reflected in the continued development of the project, ensuring a 'privacy by design' approach.

R6. Amend other MADIP agencies' privacy notices to clarify scale and nature of third party data sharing.

To deliver best practice in openness and transparency, MADIP Partner Agencies may wish to review and amend privacy notices to clarify the scale and detail of disclosure to the ABS for MADIP and the use of automated and bulk data sharing.

Agreed.

MADIP agencies other than ABS are considering updating relevant privacy notices to clarify the nature of data sharing and use is for research and statistical purposes.

Detail on the scale of data shared is out of scope of these privacy notices and is provided in other information publicly available about MADIP.

MADIP agencies note data sharing for MADIP is not an automated process and does not involve entire datasets: agencies agree to share data pursuant to a specific request(s), and provide a subset of population-based data items which are reasonably necessary for MADIP.

R7. Amend all MADIP agencies' privacy notices to describe data sharing for the MADIP as a secondary purpose.

To deliver best practice in openness and transparency, MADIP Partner Agencies may wish to consider amending privacy notices at the point of collection, as well as other public information, to indicate that data may be shared and used for statistical and research purposes, including data integration.

Agreed.

MADIP agencies are considering updating relevant privacy notices to clarify that information may be shared and used for research and statistical purposes. These updates (covered in our response to Recommendations 5 and 6) are relevant for the sharing and use of data in MADIP for both primary and secondary purposes in accordance with the *Privacy Act 1988*.

R8. In future, data sharing governance (e.g. Public Interest Certificates) should differentiate between personal information and sensitive information. The legal basis for and public interest in data sharing should be clearly disclosed to the public.

To deliver best practice in data management, MADIP Partner Agencies may wish to consider differentiating between general personal information and sensitive information in future Public Interest Certificates issued for the MADIP. The asserted legal basis / public interest in sharing and integrating sensitive information in MADIP should be clearly disclosed to the public.

Agreed.

ABS is currently updating publicly available information to clearly outline the legal basis for MADIP.

A number of MADIP partner agencies already clearly list personal information and sensitive personal information variables in their Public Interest Certificates (PICs).

However, partner agencies agree where they have capacity to do so, they will strengthen approaches to differentiating between personal information and sensitive information in PIC arrangements.

R9. Mandate regular independent security risk assessments for MADIP.

The ABS should commission regular independent security risk assessments for MADIP. The reviews should establish minimum security standards for all data sharing and require further independent security risk assessments for any new data exchanges.

Agreed.

ABS has strong data security measures in place to safeguard MADIP data.

ABS has commissioned an independent Information Security Registered Assessors' Program (IRAP) review of MADIP. Pending the outcomes of this assessment, ABS will consider recommendations to improve the security of information in MADIP, including regular independent assessments.

R10. Consider alternative data sharing models on an ongoing basis.

MADIP should consider alternative data sharing models on an ongoing basis. The current data centralisation model should be the subject of constant evaluation against alternatives such as a federated model. These evaluations should assess the comparative security risk profile of each model (amongst other factors).

Agreed.

MADIP operates under a centralised data sharing model in which data is shared for the project and stored securely by an Accredited Integrating Authority, the ABS, for linkage and creation of analytical datasets necessary for statistical and research purposes. Within ABS, this is not a pure centralised model, as datasets are stored separately, and personal information is also stored separately from analytical information to reflect best practice in security and available technology.

One alternative data sharing model is a federated system where subsets of data are extracted by data custodians and linked by an Accredited Integrating Authority like the ABS in a secure web-based environment e.g. via cloud technology. As advised by experts, this data sharing model is not feasible in the current technical environment. MADIP agencies will consider whether other data sharing models (including federated models) are appropriate, present lower security risks, and are viable as MADIP evolves.

R11. Impose the highest possible security standards to match the risk profile of data.

MADIP should impose security standards consistent with the Australian Government Information Security Manual and the Protective Security Framework on data sharing arrangements, to reflect the sensitivity and scale of the data being exchanged.

Agreed.

MADIP agencies are committed to keeping data secure, and will continue to manage data in accordance with legislative requirements and Australian Government standards including the Information Security Manual and Protective Security Policy Framework.

RESPONSE TO IPIA

R12. Consider data retention and destruction requirements.

MADIP should continue to review its approach to data retention and destruction.

Agreed.

The need to retain data for MADIP is considered annually by the Accredited Integrating Authority, the ABS, in consultation with the other MADIP agencies. A retention and destruction policy is being developed for MADIP which clarifies this current practice.

R13. Publish detailed information on access request process (i.e. for individuals to access their personal information).

The MADIP Agreement, the MADIP website and relevant privacy policies should provide detail on the MADIP Access request process. Note: These access requests do not relate to the process of accessing analytical information for research, as this information is de-identified.

Agreed.

MADIP agencies provide information about how people can access their personal information through their privacy policies.

ABS is updating its website and MADIP governance materials to explain how individuals can apply to access their personal information in MADIP.

R14. Strengthen and enhance MADIP governance arrangements.

The ABS and MADIP Partner Agencies need to continually review, strengthen and enhance the MADIP governance framework, including:

- ***A. Legal basis / Public Interest Certificates***
- ***B. Register of agreements***
- ***C. Data minimisation***
- ***D. Limits on the use of data***
- ***E. Data quality assessment***
- ***F. Minimum security requirements***
- ***G. Compliance audits***

Agreed.

The MADIP Agreement and other governance materials (such as data sharing agreements) already provide a strong foundation for the project, and outline the legal basis for data sharing and use, permissible uses of data, and data security requirements.

MADIP agencies will consider updating governance materials to provide more specific detail, and to address other recommendations from the iPIA to improve transparency.

galexia

Australian Bureau of Statistics (ABS)

Independent Privacy Impact Assessment (PIA) for the Multi-Agency Data Integration Project (MADIP)

26 March 2018 (GC504)

Contact: Galexia
Level 11, 175 Pitt Street, Sydney NSW 2000
ABN: 72 087 459 989
Ph: +61 2 9660 1111
www.galexia.com
Email: manage@galexia.com

Document Control

Client

This document has been written for the Australian Bureau of Statistics (ABS).

Document Purpose

This document is an Independent Privacy Impact Assessment (PIA) for the sharing of government data for research and statistical purposes via the Multi-Agency Data Integration Project (MADIP).

Document Identification

Document title	ABS MADIP Independent Privacy Impact Assessment (PIA)
Document filename	gc504_ABS_MADIP_PIA_2018_v13_20180326.pdf

Client Details

Australian Bureau of Statistics (ABS) <www.abs.gov.au>
ABS House
Ground Floor
45 Benjamin Way
Belconnen ACT 2617

Consultant Details

Consultant Contact **Galexia** <www.galexia.com>
Level 11, 175 Pitt Street, Sydney NSW 2000
Phone: +612 9660 1111
Email: manage@galexia.com

Peter van Dijk (Managing Director)
Mobile: +61 419 351 374 (Peter van Dijk)

Document Authors Galexia (Chris Connolly and Peter van Dijk were the principal consultants)

Reference	GC504
Project email	abs@galexia.com

Copyright

Contents

1. Executive Summary **6**
1.1. Approach and Scope 6
1.2. Australian Privacy Principle (APP) Compliance Summary 7
2. Scope and Methodology **12**
2.1. Scope 12
2.2. PIA Guidelines 13
2.3. Privacy legislation 13
3. MADIP Overview **14**
3.1. ABS overview 14
3.2. Proposed data sharing in MADIP 14
3.3. Governance 17
3.4. MADIP Data Flow – Overview 18
3.4. Potential benefits 20
3.5. Privacy Strengths and Weaknesses 21
4. Is the data 'personal information'? **22**
4.1. The Law 22
4.2. OAIC Guidelines 22
4.3. MADIP – Overview 22
4.4. 'Personal information' finding 23
5. APP 1. Open and transparent management of personal information **24**
5.1. The Law 24
5.2. MADIP – Overview 24
Recommendation 1. Improved openness about data fields 25
Recommendation 2. Improved openness about data sources 26
5.3. APP 1. Finding 27
6. APP 2. Anonymity and Pseudonymity **28**
6.1. The Law 28
6.2. MADIP – Overview 28
6.3. APP 2. Finding 28
7. APP 3. Collection of solicited personal information **29**
7.1. The Law 29
7.2. OAIC Guidelines 30
7.3. MADIP – Overview 30
Recommendation 3. Minimisation of data sharing 31
Recommendation 4. Minimise amount of sensitive data 31
7.4. APP 3. Finding 32

8. APP 4. Dealing with unsolicited personal information **33**
8.1. The Law 33
8.2. MADIP – Overview 33
8.3. APP 4. Finding 33
9. APP 5. Notification of the collection of personal information **34**
9.1. The Law 34
9.2. MADIP – Overview 34
Recommendation 5. Amend privacy notices to clarify scale of third party data acquisition 35
Recommendation 6. Amend privacy notices to clarify the scale and nature of data sharing 35
9.3. APP 5. Finding 36
10. APP 6. Use or disclosure of personal information **37**
10.1. The Law 37
10.2. OAIC Guidelines 37
10.3. MADIP – Overview 38
Recommendation 7. Amend privacy notices to ensure that data sharing with MADIP is described as a secondary purpose 39
10.4. APP 6. Finding 41
11. APP 7. Direct marketing **42**
11.1. The Law 42
11.2. MADIP – Overview 42
11.3. APP 7. Finding 42
12. APP 8. Cross-border disclosure of personal information **42**
12.1. The Law 42
12.2. MADIP – Overview 43
12.3. APP 8. Finding 43
13. APP 9. Adoption, use or disclosure of government related identifiers **44**
13.1. The Law 44
13.2. MADIP – Overview 44
13.3. APP 9. Finding 44
14. APP 10. Quality of personal information **45**
14.1. The Law 45
14.2. OAIC Guidelines 45
14.3. MADIP – Overview 45
14.4. APP 10. Finding 46
15. APP 11. Security of personal information **47**
15.1. The Law 47
15.2. OAIC Guidelines 47
15.3. MADIP – Overview 47

Recommendation 9. Mandate regular independent security risk assessments for MADIP 48
Recommendation 10. Consider alternative data sharing models on an ongoing basis 48
Recommendation 11. Impose highest possible security standards to match risk profile of data 49
Recommendation 12. Consider data destruction and de-identification requirements 49
15.4. APP 11. Finding 50
16. APP 12. Access to personal information 51
16.1. The Law 51
16.2. MADIP – Overview 51
Recommendation 13. MADIP should publish detailed information regarding access requests 51
16.3. APP 12. Finding 52
17. APP 13. Correction of personal information 53
17.1. The Law 53
17.2. OAIC Guidelines 53
17.3. MADIP – Overview 54
17.4. APP 13. Finding 54
18. Governance 55
Recommendation 14. Strengthen and enhance MADIP Governance arrangements 57
19. Appendix 1 – Acronyms 58
20. Appendix 2 – Stakeholder Consultation 58

1. Executive Summary

1.1. Approach and Scope

Galexia has been commissioned by the Australian Bureau of Statistics (ABS) to prepare an Independent Privacy Impact Assessment (PIA) for the proposed sharing of government data for research and statistical purposes via the Multi-Agency Data Integration Project (MADIP).

The PIA process is being conducted in accordance with *PIA Guidelines* issued by the Office of the Australian Information Commissioner. The ABS has agreed to publish the PIA as part of their ongoing consultation with stakeholders and the community.

The purpose of the PIA is to assist in identifying and managing privacy issues that are raised by the sharing of data between ABS and other agencies in MADIP. The key objectives are:

1. To formalise data sharing arrangements for research and statistical purposes;
2. To create a safe and secure environment for research that requires the integration of data from multiple sources; and
3. To create an effective governance framework for data sharing.

Since 2015 MADIP has been operating as an evaluation – testing the technical capability of the Partner Agencies to share data in a way that delivers useful outputs, whilst preserving privacy. The evaluation phase is expected to draw to a close in 2018.

Information contained in this PIA is based on:

- Meetings with ABS, including senior management, technical staff, legislation and policy staff and the data linkage centre team;
- Meetings with MADIP Partner Agencies (further details included in Appendix 1 – Stakeholder Consultation);
- Meetings with external stakeholders, notably the Office of the Australian Information Commissioner (OAIC) and the Department of Prime Minister and Cabinet (PM&C) (further details included in Appendix 1 – Stakeholder Consultation);
- Documentation related to the proposal (further details in Appendix 2 – Background Information);
- General research and literature review on privacy and data sharing issues; and
- Review of relevant privacy legislation and guidelines.

Galexia's advice in this PIA concentrates on the following areas:

- **Privacy legislation compliance**
  The PIA assesses the proposed sharing of data between a range of Commonwealth agencies (for research and statistical purposes) against the Australian Privacy Principles (APPs) in the Commonwealth Privacy Act;
- **Practical measures to address privacy**
  The PIA identifies several practical measures that can be taken to manage privacy issues; and
- **Governance**
  The PIA considers key privacy governance steps that could be implemented to ensure the ongoing protection of privacy once the data sharing arrangements are operational.

1.2. Australian Privacy Principle (APP) Compliance Summary

The PIA assesses the MADIP data sharing arrangements against the APPs in the Privacy Act.

The recommendations provided in this PIA are intended to apply only to MADIP. In many ways MADIP is a unique and complex project and the advice in this report is designed to assist the ABS and partners to manage MADIP data flows in line with best practice with respect to protecting privacy.

The analytical data that forms the main component of MADIP is held separately from personal information used for linkage purposes (including name and address information). The separation of this data and method that it is managed by the ABS means that individuals are not reasonably identifiable for the purposes of the *Privacy Act 1988* (the Privacy Act).

The following table summarises the main findings, with links to further information and detailed discussion in the body of the report:

Australian Privacy Principle (APP)	Compliance Status	Galexia Commentary	Galexia Recommendation
APP 1 – Openness and Transparency	**Partially compliant** **Further measures possible**	The ABS maintains a public Privacy Policy and a Census Privacy Policy. Until recently, these privacy policies have only included a brief mention of data integration MADIP Partner Agencies also have public Privacy Policies. These policies have not been the subject of detailed consideration in this PIA, but they appear to only provide limited information in relation to data sharing. The MADIP website contains some useful information, but has some gaps. The ABS and MADIP Partner Agencies are currently in the process of updating Privacy Policies and website information to include specific references to data sharing and data integration.	**R1. Improved openness about data fields** ABS should amend the MADIP website to indicate personal information is used by MADIP for statistical and research purposes, including data integration. A list of the linkage and analytical data variables could also be provided. **R2. Improved openness about data sources** ABS may wish to amend publicly available information and relevant Privacy Policies to be more open about the collection of data from agencies and the datasets being integrated in MADIP.
APP 2 – Anonymity and Pseudonymity	**Compliant**	ABS provides some limited anonymity to general website visitors. All other data collected by MADIP is covered by exceptions to the anonymity principle.	

APP 3 – Collection of solicited personal information	**Partially compliant** **Further measures possible**	APP 3 requires agencies to only collect data that is 'reasonably necessary'. Although MADIP does not collect data directly from consumers, this requirement still applies to data acquired by MADIP through data sharing arrangements. MADIP has a strong data minimisation culture in place, including implementation of the High Level Principles for Commonwealth Data Integration. However, there is room for further strengthening of the data minimisation approach. The other requirements of APP 3 can be met by reliance on the exceptions that apply where data collection is authorised by a specific law. While there is no dedicated specific legislation for MADIP, the sharing of data with MADIP is authorised by legislation specific to the Partner Agencies.	**R3. Minimisation of data sharing** MADIP governance arrangements and public material should clarify that data minimisation occurs both during data sharing and data access for authorised researchers. MADIP should enhance the minimisation of personal data sharing by: 1. Only sharing data items that are reasonably necessary 2. Excluding irrelevant data items where possible 3. Using data categorisation (e.g. Yes / No responses or bands) rather than specific data fields where possible. **R4. Minimise amount of sensitive data** MADIP should implement a review of all sensitive data fields to assess whether it is reasonably necessary to acquire sensitive data. Unnecessary data fields should be removed from future data acquisition and deleted / quarantined from existing MADIP data holdings.
APP 4 – Dealing with unsolicited personal information	**Compliant**	Dealing with unsolicited personal information is not a significant issue for MADIP.	
APP 5 – Notification	**Action required**	In MADIP a variety of Agency data is shared with the ABS. Compliance with APP 5 therefore needs to be assessed for each proposed disclosure. The ABS uses clear and comprehensive forms to provide notice of privacy issues to its direct client base. These forms are compliant with many of the requirements of APP 5. However, both ABS and Partner Agency privacy notices (e.g. forms, online applications) do not provide clear information about disclosure of data to MADIP and the use of automated and bulk data sharing. (Automated sharing is where data is automatically shared rather than where information on a specific individual or group of individuals is provided on request. Bulk data sharing is where all population data is shared rather than a sample of data subjects).	**R5. Amend privacy notices to clarify scale of third party data acquisition** To deliver best practice in openness and transparency, ABS may wish to review and amend privacy notices to clarify the scale of third party data acquisition, the use of automated and bulk third party data acquisition and the expanded list of third parties that are involved. **R6. Amend privacy notices to clarify the scale and nature of data sharing** To deliver best practice in openness and transparency, MADIP Partner Agencies may wish to review and amend privacy notices to clarify the scale and detail of disclosure to the ABS for MADIP and the use of automated and bulk data sharing.

APP 6 – Use or Disclosure	**Partially compliant** **Further measures possible**	APP 6 envisages a link between the use of data and the purposes of the collecting agency. Once data is shared with another agency, for their purposes, the parties must rely on an exception to APP 6. Overall, this PIA categorises the supply of data to the ABS for MADIP as either a primary purpose or a reasonably expected secondary purpose under APP 6 (depending on the privacy notices issued by agencies). Some additional care should be taken regarding the disclosure of sensitive information by Partner Agencies to MADIP.	**R7. Amend privacy notices to ensure that data sharing with MADIP is described as a secondary purpose** To deliver best practice in openness and transparency, MADIP Partner Agencies may wish to consider amending privacy notices at the point of collection, as well as other public information, to indicate that data may be shared and used for statistical and research purposes, including data integration. **R8. MADIP Partner Agency legal authorities (e.g. Public Interest Certificates) should differentiate between general personal information and sensitive information** To deliver best practice in data management, MADIP Partner Agencies may wish to consider differentiating between general personal information and sensitive information in future Public Interest Certificates issued for the MADIP.. The asserted legal basis / public interest in sharing and integrating sensitive information in MADIP should be clearly disclosed to the public.
APP 7 – Direct Marketing	**Compliant**	Direct marketing is not applicable in this PIA.	
APP 8 – Cross Border Disclosure	**Compliant**	Cross border data transfers are not applicable to MADIP. They have not been considered in detail in this PIA.	
APP 9 – Government Related Identifiers	**Compliant**	APP 9 is not applicable in this PIA.	
APP 10 – Quality of Personal Information	**Compliant**	The ABS has extensive systems in place for ensuring that its own data is accurate. There is continual assessment of the accuracy of data linking processes in MADIP.	

APP 11 – Security	**Action required**	Most data used in MADIP for analysis is de-identified. The data initially acquired for MADIP includes sensitive data. The scale of the data involved is also significant. It will be important for security settings to match the potential harm of any breaches. Currently there are strong security measures in place for MADIP. These include: - Storage of all data in the ABS 'NextGen Infrastructure Environment', - implementation of functional separation of linkage data from other data variables, - Implementation of the 5 Safes Framework, and - Restricting access to MADIP via the ABS DataLab. APP 11 requires reasonable steps to be taken to protect MADIP data from unauthorised access. The ABS is aware of this requirement and has recently commissioned an Independent Security Risk Assessment of MADIP. At the time of this PIA, the review has not yet been completed. APP 11 also requires MADIP to establish appropriate rules for the destruction and de-identification of data. The ABS is aware of this issue and the MADIP Privacy Work Plan includes an item regarding the development of a data retention policy for MADIP.	**R9. Mandate regular independent security risk assessments for MADIP** The ABS should commission regular independent security risk assessments for MADIP. The reviews should establish minimum security standards for all data sharing and require further independent security risk assessments for any new data exchanges. **R10. Consider alternative data sharing models on an ongoing basis** MADIP should consider alternative data sharing models on an ongoing basis. The current data centralisation model should be the subject of constant evaluation against alternatives such as a federated model. These evaluations should assess the comparative security risk profile of each model (amongst other factors). **R11. Impose highest possible security standards to match risk profile of data** MADIP should impose security standards consistent with the Australian Government Information Security Manual and the Protective Security Framework on data sharing arrangements, to reflect the sensitivity and scale of the data being exchanged. **R12. Consider data destruction and de-identification requirements** MADIP should continue to review its approach to data retention and destruction.
APP 12 – Access	**Action required**	The ABS has access policies and procedures in place for its own data that are compliant with APP 12. ABS also has a special exemption available for access requests. APP 12 requires the ABS and MADIP Partner Agencies to provide clear information to consumers on how they can access their data. The extent of access to MADIP data may be limited by exemptions that are available to the ABS under privacy and FOI legislation. The ABS is aware of this issue and has recently begun work on developing a specific Access and Corrections Policy for MADIP. ABS intends to provide public information (e.g. MADIP FAQ and Privacy Policy) to include content on how individuals can request access to and correction of their information in MADIP. Access to the MADIP source datasets is not in scope.	**R13. MADIP should publish detailed information regarding access requests** The MADIP Agreement, the MADIP website and relevant privacy policies should provide detail on the MADIP Access request process. **Note:** These access requests do not relate to the process of accessing analytical information for research, as this information is de-identified.

APP 13 – Correction	**Compliant**	The ABS and MADIP Partner Agencies are compliant with the complaints and corrections requirements of APP 13. This position will, potentially, be strengthened by the development of a specific Access and Corrections Policy for MADIP. Work on this new policy began in early 2018. At the time of writing this PIA, the new policy is not available. Although not strictly required, MADIP could benefit from a small expansion of complaints management. Specifically, ABS and MADIP Partner Agencies could go beyond strict compliance with APP 13 and share all data corrections and correction statements.	
Governance		MADIP needs to comply with a variety of requirements contained in: - Privacy legislation (the APPs) - MADIP Partner Agency legislation - MADIP Public Interest Certificates - The MADIP Partner Agreement It is also important to continually address issues that may arise from public expectations or perception issues that are associated with such a large, high profile, high risk project. ABS / MADIP Partner Agencies continue to strengthen and enhance their compliance and governance arrangements for MADIP.	**R14. Strengthen and enhance MADIP Governance arrangements** The ABS and MADIP Partner Agencies need to continually review, strengthen and enhance the MADIP governance framework, including: **A.** Legal basis / Public Interest Certificates **B.** Register of agreements **C.** Data minimisation **D.** Limits on the use of data **E.** Data quality assessment **F.** Minimum security requirements **G.** Compliance audits

2. Scope and Methodology

Galexia has been commissioned by the Australian Bureau of Statistics (ABS) to prepare an independent Privacy Impact Assessment (PIA) for the proposed sharing of government data for research and statistical purposes via the Multi-Agency Data Integration Project (MADIP).

The primary purpose of this PIA is to:

- Analyse the impacts that the Project will have on the privacy of individuals whose (de-identified) information will be made available to authorised government and non-government researchers;
- Identify privacy risk areas in relation to compliance with the APPs and community expectations; and
- Identify, assess and (if appropriate) recommend options for managing, mitigating or eliminating negative privacy impacts, including proposed controls and safeguards.

This PIA does not:

- Cover the data activities of ABS as a whole;
- Assess the application or, or compliance with, restrictions on the handling of 'protected information' pursuant to secrecy provisions in portfolio legislation (other than the extent to which the collection, use or disclosure of personal information will be 'authorised or required by law' pursuant to those secrecy provisions for the purposes of APPs 3.4, 3.6 and 6.2);
- Cover other individuals whose personal information may be collected and handled in the context of the project (e.g. personal information about researchers who apply for data access); or
- Consider State or Territory privacy laws, or compliance by researchers with applicable privacy laws or secrecy provisions.

2.1. Scope

The scope of the overall PIA is limited to the following items:

In Scope	Out of Scope
High level identification of potential compliance issues in the context of the Australian privacy legal framework,	Detailed compliance with specific sectoral / State or Territory legislation
Review of key documents related to the proposed data sharing arrangements	Review of the entire suite of ABS or Partner Agency documentation
Limited stakeholder consultation consisting of selected internal stakeholders and selected Partner Agencies.	Extensive public consultation, open invitation consultation, assessment of public attitudes etc. (This task is initially being completed by ABS as a separate project).
Review of existing security assessment/s	Full security audit or assessment.
High level identification and review of legal documentation	Detailed legal advice
Focus on overall privacy compliance for ABS and MADIP	Detailed analysis and consideration of the specific privacy issues for each of the MADIP Partner Agencies

Focus on current MADIP evaluation and existing MADIP data sets, with brief consideration of future plans for the collection of longitudinal data for some data sets including Census 2016	Detailed consideration of the future inclusion of additional data sets
Focus on MADIP as a stand-alone data integration program, with brief consideration of broader context	Comprehensive consideration about the scope and role of a Whole of Government Data Custodian – as canvassed in the Productivity Commission Report

2.2. PIA Guidelines

The Independent PIA is being conducted in accordance with the PIA Guidelines issued by the Office of the Information Commissioner.[1]

2.3. Privacy legislation

The Independent PIA is being written in the light of current Commonwealth privacy legislation – the Privacy Act 1988. The Act sets out the Australian Privacy Principles (APPs),[2] which regulate the collection, use and disclosure of personal information by Commonwealth Agencies and private sector organisations.

The Australian Government Agencies Privacy Code (the Code) is also relevant. The Code was registered on 27 October 2017 and commences on 1 July 2018. <https://www.oaic.gov.au/privacy-law/australian-government-agencies-privacy-code/>.

[1] <http://www.oaic.gov.au/privacy/privacy-resources/privacy-guides/privacy-impact-assessment-guide>.

[2] The 13 APPs are in Schedule 1 of the *Privacy Amendment (Enhancing Privacy Protection) Act 2012*, which amends the *Privacy Act 1988*. They came into force on 12 March 2014.

3. MADIP Overview

3.1. ABS overview

The Australian Bureau of Statistics (ABS) is Australia's national statistical agency, providing statistics on a wide range of economic, social, population and environmental matters of importance to Australia.

The ABS is subject to significant confidentiality provisions contained in various legislation. The most relevant include:

- *Australian Bureau of Statistics Act 1975* (Cth);
- *Census and Statistics Act 1905* (Cth); and
- *Privacy Act 1988* (Cth) and *Australian Privacy Principles* (the APPs)

The *Australian Bureau of Statistics Act 1975* (Cth) gives the ABS the authority to integrate data from a range of sources and to support the maximum usage of these data by official bodies for statistical and research purposes. Additionally, the *Census and Statistics Act 1905* (Cth) applies to data brought into the ABS for the purposes of MADIP.

3.2. Proposed data sharing in MADIP

The Multi-Agency Data Integration Project (MADIP) is a cross-portfolio government partnership to demonstrate how the Australian Government can make better use of existing public data for policy analysis, research, and statistical purposes.

Since 2015 MADIP has been in an evaluation phase.

The current MADIP Partner Agencies are:

- Australian Bureau of Statistics (ABS)
- Australian Taxation Office (ATO)
- Department of Education and Training (DET)
- Department of Health
- Department of Human Services (DHS)
- Department of Social Services (DSS)

The MADIP evaluation combines information on healthcare, education, government payments, personal income tax, demographics and housing

In 2018 MADIP will be expanded to include the 2016 Census and present opportunities for longitudinal study of some data.

The following table provides a very high level summary of a selection of the proposed data sharing arrangements:

MADIP Project Partner	Participation in MADIP	Data	Legal Basis / Legal Agreement	Method of sharing
ABS	Data Custodian Accredited Integrating Authority	Census of Population and Housing: 2011 and 2016	n/a	n/a

ATO	Data Custodian	Personal Income Tax: 2010/11 to 2015/16	An exception (contained in Table 7 in section 355-65 of Schedule 1 to the *Taxation Administration Act 1953*) allows the ATO to release personal information to the Australian Statistician for the purpose of 'administering the *Census and Statistics Act 1905*'. An MOU is in place.	Secure file transfer
DET	Data Custodian	Australian Early Development Census (AEDC): 2009, 2012, 2015	No specific legislation applies to the AEDC, so the provisions of the *Privacy Act 1988* are applied. An MOU is in place.	AEDC data is transferred to MADIP via the ABS secure portal.
Health	Data Custodian	Medicare Benefits Scheme (MBS) Claims Dataset: 2011-2016 Pharmaceutical Benefits Scheme (PBS) Claims Dataset: 2011-2016 Centralised Register of Medical Practitioners Provider Directory (CRMPPD): 2011-2016	An exception in Section 130 of the *Health Insurance Act 1973* allows personal information to be divulged to a specific party if the Minister (or their delegate) certifies in writing that the disclosure is 'necessary in the public interest'. Multiple Public Interest Certificates (PICs) have been issued. An MOU is not in place – the parties exchanged letters of authorisation.	MBS and PBS data is delivered via secure file transfer from the Department of Health).
DHS	Data Custodian for health data	Medicare Enrolments Database (MEDB): 2006-2016	Refer to Health letter of exchange and PICs. DHS provides the MEDB to ABS	There is no direct transfer from Health. MEDB data is delivered via secure file transfer from DHS.

DSS	Data Custodian	Social Security and Related Information: 2009-2016 1	Various DHS legislation allows personal information to be disclosed to a specified party where a Public Interest certificate has been issued. This includes: 1. *Social Security (Administration) Act 1999* 2. *Social Security (Public Interest Certificate Guidelines) (DSS) Determination 2015* 3. *A New Tax System (Family Assistance) (Administration) Act 1999* 4. *Family Assistance (Public Interest Certificate Guidelines) Determination 2015* 5. *Paid Parental Leave Rules 2010* (under the *Paid Parental Leave Act 2010*) 6. *Student Assistance Act 1973* 7. *Student Assistance (Public Interest Certificate Guidelines) Determination 2015* The disclosure must be 'necessary in the public interest … in a particular case or class of cases'. The disclosure must also comply with the *Family Assistance (Public Interest Certificate Guidelines) Determination 2015*. Section 14 of the Determination allows disclosure for statistical research and analysis where there is a link to the administration of the Family Assistance law. A Public Interest Certificate (PIC) has been issued. A MOU is in place.	Secure file transfer.

The legal basis for each disclosure is set out in more detail in the following documents:

- Head Agreement
- Subsidiary Agreement
- Public Interest Certificate (PIC) 2015
- Public Interest Certificate (PIC) 2017

Agency	Head Agreement	Subsidiary Agreement	PIC 2015	PIC 2017
ATO	YES	YES	N/A	N/A
DET	YES	YES	N/A	N/A
DSS	YES	YES	YES	YES
Health and DHS	YES	YES	YES	YES

3.3. Governance

MADIP is being conducted in accordance with the High Level Principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes (High Level Principles)[3].

Currently there are three levels of project governance in place:

1. The Deputy Secretaries Data Group, reporting to the Secretaries Data Group, is responsible for driving the overall Public Sector Data Management agenda, which includes oversight of MADIP.
2. A Project Board composed of senior representatives from the Partner Agencies sets the strategic direction of MADIP and is responsible for monitoring implementation.
3. Operational responsibility for the MADIP is vested in an Accredited Integrating Authority (the ABS).

Current governance arrangements are set out in the MADIP Agreement. The MADIP Agreement sets out the vision and terms of the MADIP, and is the basis for subsidiary data sharing agreements between the data custodians and the Accredited Integrating Authority.

Governance for the MADIP is in the process of transitioning to a new structure, to support the project in its operational phase under the Data Integration Partnership for Australia (DIPA). The new structure is:

1. People Centred Data Oversight Committee – SES Band 3 level members provide strategic oversight of how people centred data in DIPA (including MADIP) is managed and used;
2. People Centred Data Analytical Unit – SES Band 1 members provide direction on operational and analytical issues; and
3. Accredited Integrating Authority (ABS) – responsible for management and linkage of data, and providing secure access.

[3] The High Level Principles are available at <http://www.nss.gov.au>.

3.4. MADIP Data Flow – Overview

The diagram on the following page summarises the current data linking methodology:

Diagram on following page – Overview of Proposed Linkage [Diagram supplied by ABS on 16 March 2018

Information from the source datasets in the MADIP is collected by (Census) or shared with (other administrative datasets) the ABS and stored securely in accordance with the separation principle.[4]

Prior to linking, personal information is anonymised. For administrative datasets this is undertaken in the Librarian role, for Census 2016 this is undertaken in the extra Librarian roles of Census Name Manager (purely for name preparation) and Census Librarian.

Stage 1: The core administrative datasets – Medicare Enrolments (MEDB), Personal Income Tax (PIT), and Social Security and Related Information (SSRI), are linked using anonymised name[5] and other personal information including Date of Birth (DOB) and geocoded address.

Stage 2: Census 2016 will be linked to the core datasets using a Lossy encoded version of name[6] along with other personal information, for example DOB and geocoded address.

Stage 3: Census 2011 will be linked to the other core datasets without name information, as this has been destroyed, by using geocoded address and other demographic characteristics.

Other administrative datasets, for example the Australian Early Development Census (AEDC), will be linked to the core datasets using anonymised name and other personal information including Date of Birth (DOB) and geocoded address.

As depicted by the right hand side of the diagram, once linkages are complete, analytical datasets are merged (by an Assembler) using the linkage results (containing no personal information) and customised datasets for researcher (Analysts) use created.

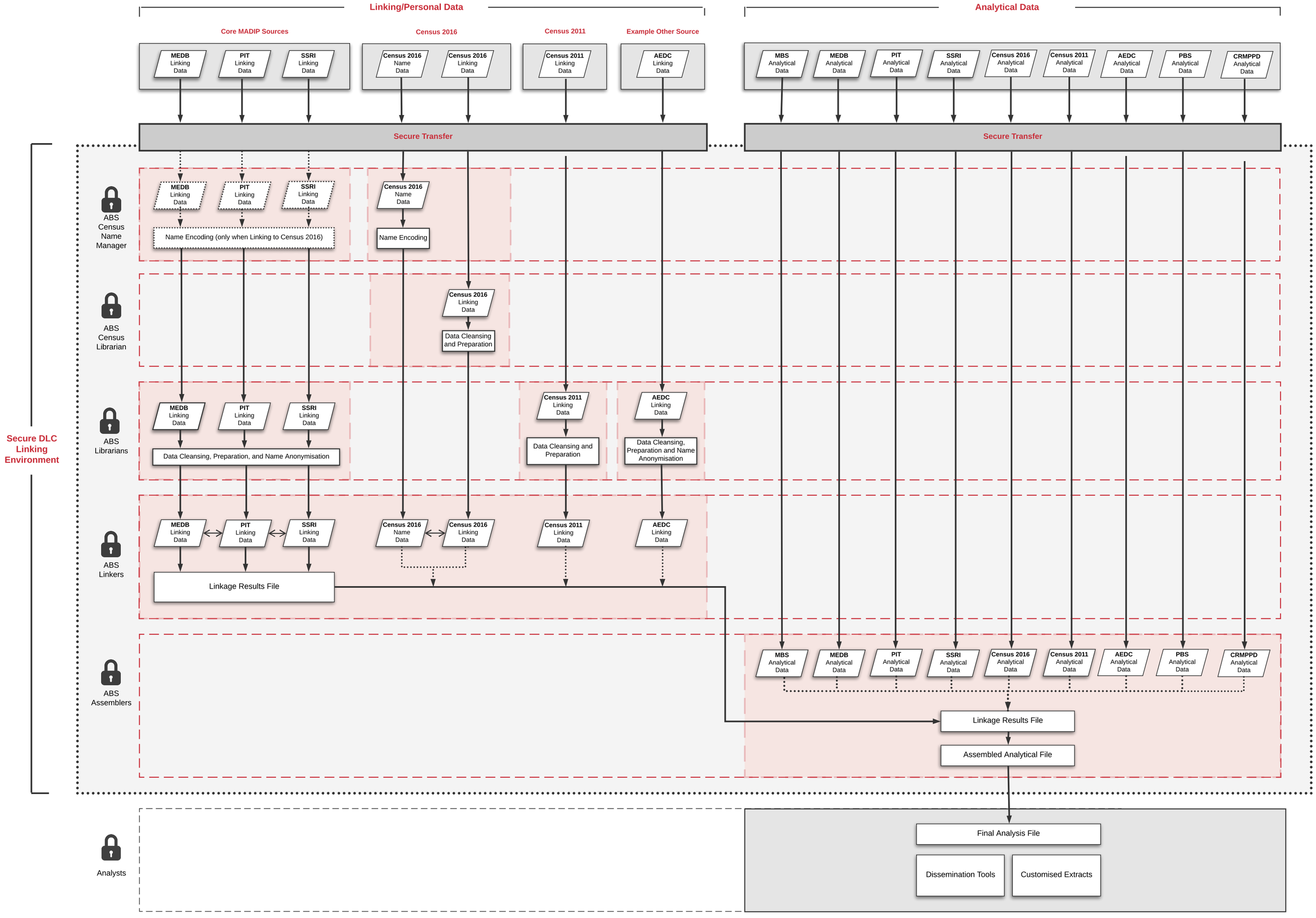
Analysis is only performed on files that do not contain information which is likely to enable a person to be identified.

[4] Further information on the separation principle is contained in the *Guide for Data Integration Projects involving Commonwealth Data for Statistical and Research Purposes* (National Statistical Service, 2014) available at: <https://statistical-data-integration.govspace.gov.au/topics/applying-the-separation-principal>.

[5] Names from these datasets are converted into an unrecognisable string using a simple character replacement technique that protects the name information from being spontaneously recognised and does not result in a loss of information.

[6] Names are encoded into an irreversible, unrecognisable value (e.g. a string of character and numeric values), where each value represents multiple names. The increased security results in a loss of information.

MADIP Data Flow



3.5. Privacy Strengths and Weaknesses

Galexia considers that the current design and implementation of MADIP has a number of privacy strengths and weaknesses. These are set out briefly, and further information is provided in relevant sections later in this report.

Strengths

- There is no **new** collection of personal information from individuals. MADIP is integrating personal information that individuals have already provided to a select group of Agencies;
- The Accredited Integrating Authority (ABS) is subject to legislative prohibition on releasing any data that is likely to lead to the identification of an individual (*Census and Statistics Act 1905* (Cth));
- The MADIP 'separation principle' establishes significant practical barriers to the potential combination of personal data such as name and address with the other content data;
- Currently, MADIP data can only be accessed by approved and vetted research staff in a secure environment under constant monitoring;
- MADIP is conducted in accordance with the High Level Principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes[7] (the High Level Principles), including a requirement that data is only used for policy analysis, research, and statistical purposes (not for monitoring or compliance);
- Penalties and sanctions, including imprisonment and hefty fines, are in place in the *Census and Statistics Act 1905* (Cth) for any unauthorised access to MADIP data or inappropriate use of the data;
- Some public information is available regarding MADIP (e.g. on the ABS website[8]);
- The objectives and likely outcomes of MADIP are clearly in the public interest and are likely to deliver significant community benefit;
- The objectives and likely outcomes of MADIP have a reasonable degree of support from community stakeholders; and
- The ABS and MADIP Partner Agencies recognise the importance of privacy and have been in regular communication with the OAIC and are committed to an independent PIA process.

Weaknesses

- MADIP has already integrated substantial data sets, prior to detailed consultation with stakeholders or the public, and prior to the completion of an independent PIA;
- Although some public information is now available regarding MADIP (e.g. on the ABS website), this information did not initially address or discuss some of the key MADIP details that are likely to be of interest to individuals (further details on this issue are discussed in APP 1. Open and transparent management of personal information);
- Although MADIP (to date) has been characterised as an **evaluation**, all available data, including sensitive data, has been acquired, consolidated and integrated. There have been some minor restrictions that are consistent with an evaluation (e.g. restricted research access to the data), but in most areas relevant to privacy MADIP is operating as a fully functioning program;
- MADIP has acquired a substantial amount of information that should be categorised under the *Privacy Act* as **sensitive information** (this issue is discussed in greater detail in APP 3. Collection of solicited personal information); and

[7] <http://www.nss.gov.au/nss/home.NSF/pages/High+Level+Principles+for+Data+Integration+-+Content>

[8] <http://www.abs.gov.au/websitedbs/D3310114.nsf/home/Statistical+Data+Integration+-+MADIP>

- **MADIP data is retained for lengthy periods,** including the raw data initially provided by Partner Agencies, and including the name and address data (separated, but still retained). MADIP data is retained for as long as a business requirement exists, and is likely to result in data being stored for lengthy periods.

4. Is the data 'personal information'?

4.1. The Law

A starting point for our discussion of privacy compliance is whether or not the data that is proposed to be shared by / with ABS is personal information.

The Commonwealth *Privacy Act 1988* states:

> *Personal information means information or an opinion about an identified individual, or an individual who is reasonably identifiable.*
> <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-b-key-concepts#personal-information>

4.2. OAIC Guidelines

In May 2017 the OAIC provided guidance on personal information:

> *What Is Personal Information?,* Office of the Australian Information Commissioner (OAIC), 5 May 2017 <https://www.oaic.gov.au/agencies-and-organisations/guides/what-is-personal-information>.

4.3. MADIP – Overview

The proposed data sharing arrangements incorporate a mix of personal information and non-personal information.

To align with ABS data management practices, the ABS manages all data acquired by MADIP with processes appropriate for 'personal information'. The analytical information has the name and address removed and is subsequently not 'personal information' for the purposes of the *Privacy Act* – providing it is not 'reasonably re-identifiable'. When providing access to researchers, the ABS ensures that no individual is reasonably identifiable from the data remaining after the de-identification process.[9]

The broad categories of data items shared for MADIP include:

- name,
- basic demographic details (age, DOB, gender),
- country and city of birth,
- home address,
- religious affiliation,
- sexuality,
- financial information,
- health information,
- welfare related information,
- education related information, and
- Indigenous status.

[9] As noted above, the ABS have advised that information is managed to minimise spontaneous recognition of individuals, including rigorous application of the Separation Principle, the 5 Safes Framework, and other measures used to ensure confidentiality of data (refer also to the ABS Confidentiality Series).

4.4. 'Personal information' finding

The Privacy Commissioner advises that:

> where it is unclear whether an individual is 'reasonably identifiable', an organisation should err on the side of caution and treat the information as personal information[10]

Nearly all of the data initially provided to MADIP can be linked to an individual.

However, directly identifiable linkage data is only used to bring datasets together. The de-identified analytic data is kept separate from the personal linkage data. The analytical data used in MADIP is managed by the ABS in such a way as to minimise the likelihood of spontaneous identification of individuals. This includes a rigorous application of 'functional separation' and other systems and security protocols, as described in the section in APP 11 below.

An additional question is whether or not some of the data falls into the category of sensitive information. This has serious implications for APP 3 and APP 6 (discussed below).

Sensitive information[11] means:

> *(a) information or an opinion about an individual's:*
>
> *(i) racial or ethnic origin; or*
> *(ii) political opinions; or*
> *(iii) membership of a political association; or*
> *(iv) religious beliefs or affiliations; or*
> *(v) philosophical beliefs; or*
> *(vi) membership of a professional or trade association; or*
> *(vii) membership of a trade union; or*
> *(viii) sexual orientation or practices; or*
> *(ix) criminal record;*
> *that is also personal information; or*
>
> *(b) health information about an individual; or*
>
> *(c) genetic information about an individual that is not otherwise health information; or*
>
> *(d) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or*
>
> *(e) biometric templates.*

Sensitive information is shared by MADIP Partner Agencies and the ABS with MADIP. The ABS manages this information with processes appropriate for sensitive information. The main data fields that are likely to be managed as sensitive information in MADIP are health, sexuality, racial, ethnic and religious data. This issue is discussed in further detail in the sections on APP 3 and APP 6 (below).

The analytical information has the name and address removed and is *subsequently* not 'sensitive information' for the purposes of the Privacy Act – providing it is not 'reasonably re-identifiable'. When providing access to researchers, the ABS ensures that no individual is reasonably identifiable from the data remaining after the de-identification process.

This approach is compatible with the guidance from the Office of the Australian Information Commissioner (OAIC) to take a 'cautious' approach to the categorisation of data. This approach is also appropriate given the high risk profile of the MADIP data set.

[10] Office of the Australian Information Commissioner (OAIC), Guide to securing personal information, 2015, <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>.

[11] Section 6 of the Privacy Act 1988 <http://www.austlii.edu.au/au/legis/cth/consol_act/pa1988108/s6.html>.

5. APP 1. Open and transparent management of personal information

5.1. The Law

APP 1 — open and transparent management of personal information

1.2 An APP entity must take such steps as are reasonable in the circumstances to implement practices, procedures and systems relating to the entity's functions or activities that:

> *(a) will ensure that the entity complies with the APPs / registered code; and*
>
> *(b) will enable the entity to deal with inquiries or complaints from individuals about the entity's compliance with the APPs / registered code.*

1.3 An APP entity must have a clearly expressed and up to date policy (the APP privacy policy) about the management of personal information by the entity.

1.4 (minimum contents of the privacy policy)

1.5 An APP entity must take such steps as are reasonable in the circumstances to make its APP privacy policy available:

> *(a) free of charge; and*
>
> *(b) in such form as is appropriate.*

More information:
<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-1-app-1-open-and-transparent-management-of-personal-information>.

5.2. MADIP – Overview

ABS maintains a public Privacy Policy that can be accessed at
<http://www.abs.gov.au/websitedbs/D3310114.nsf/Home/Privacy>.

The Privacy Policy states:

> *As part of its statistical collections, the ABS collects data from individuals, households and businesses, as well as from administrative sources.*

There is also a specific Census Privacy Policy at
<http://www.abs.gov.au/websitedbs/censushome.nsf/home/privacypolicy>.

The Census Privacy Policy states:

> *As an accredited data integrating authority, the ABS complies with a set of key principles for any project that combines Census data with other data, including assessing every project to ensure that the project provides a significant public benefit and safeguards privacy.*
>
> *and*
>
> *For the 2016 Census, the ABS will destroy names and addresses when there is no longer any community benefit to their retention or four years after collection (i.e. August 2020), whichever is earliest.*

These sections of the two Privacy Policies provide some useful information, and they do contain one brief mention of data integration. There are no specific references to MADIP and an average reader is unlikely to be aware a of the scale and significance of data integration being conducted under MADIP.

In part, this is because these are ABS and Census privacy policies, rather than a MADIP privacy policy (no such policy exists). In early 2018 the ABS began assessing whether or not a specific MADIP Privacy Policy should be developed. At the time of writing this PIA, no firm decision had been reached on this issue.

Further information on MADIP is available on the ABS website and also on the National Statistical Service (NSS) website.

The ABS website provides a detailed overview of MADIP and links to key resources, including the MADIP FAQs, MADIP Case Studies and the High Level Principles for Data Integration Involving Commonwealth Data for Statistical and Research Purposes <http://www.abs.gov.au>.

The NSS website provides limited information on MADIP <http://www.nss.gov.au>.

However, some of the key MADIP information is not currently available at either website.

In early 2018 the ABS established a MADIP Privacy Work Plan to enhance privacy management for MADIP. Item 4 of the Work Plan describes ABS's intention to amend the MADIP website to provide detail on:

1. MADIP Agreement;
2. Other data sharing agreements for MADIP;
3. Register of MADIP PICs and description of legal authority for data sharing;
4. Data item list and category description;
5. List of sensitive information in MADIP;
6. Register of research projects;
7. Register of research project proposals;
8. Info on process for access requests or complaints; and
9. Contact info for MADIP parties.

Once implemented, this expansion of public information regarding MADIP will enhance compliance with APP 1.

The following checklist provides a useful summary of the key issues regarding openness and transparency:

APP 1. Openness and transparency	Action / Status	Galexia Commentary
A. Does the entity provide a public privacy policy?	**Compliant**	ABS maintains a public Privacy Policy and a Census Privacy Policy. Each MADIP Partner Agency maintains a public privacy policy. There is no specific overall MADIP privacy policy, and MADIP might benefit from the development of a specific privacy policy (similar to the specific Census privacy policy).
B. Does the Policy include: (a) the kinds of personal information that the entity collects and holds;	**Compliant** **Further measures possible**	This information is only included at a very high level in the ABS Privacy Policy, the ABS Census Privacy Policy and the individual MADIP Partner Agency privacy policies, and not in a way that makes a specific link to MADIP. The ABS MADIP website lists the Partner Agencies and the key datasets, but does not provide a list of the numerous data fields that are being shared. There is also no list of the sensitive information being shared in MADIP. The concern is that without the full list of data fields, it is unlikely that an individual reading the various privacy policies and the MADIP FAQs would grasp the full scale and detail of the kinds of personal information shared in MADIP. The MADIP Privacy Work Plan includes proposed steps to address this issue. **Recommendation 1. Improved openness about data fields** ABS should amend the MADIP website to indicate personal information is used by MADIP for statistical and research purposes, including data integration. A list of the linkage and analytical data variables could also be provided.

C. Does the Policy include: (b) how the entity collects and holds personal information;	**Compliant** **Further measures possible**	The ABS Privacy Policy and the Census Privacy Policy both require modification to ensure that consumers are aware that MADIP collects extensive, bulk personal information from other agencies. The current policies only include the briefest of mentions of data integration and a confusing reference to collection from 'administrative sources'. The MADIP Privacy Work Plan includes proposed steps to address this issue. **Recommendation 2. Improved openness about data sources** ABS may wish to amend publicly available information and relevant Privacy Policies to be more open about the collection of data from agencies and the datasets being integrated in MADIP.
D. Does the Policy include: (c) the purposes for which the entity collects, holds, uses and discloses personal information;	**Compliant**	This information is included in the ABS Privacy Policy. Additional detail is provided on the MADIP website.
E. Does the Policy include: (d) how an individual may access personal information about the individual that is held by the entity and seek the correction of such information;	**In progress**	This information is included in the ABS Privacy Policy and Census Privacy Policy. However, it is written in a way which is specific to other ABS activities (not MADIP), including references to the National Archives provisions for retention of the census. The MADIP website does not provide any information on how access requests can be made in relation to MADIP. However, the MADIP Privacy Work Plan includes proposed steps to address this issue. Access requests are discussed in more detail at APP 12. Access to personal information.
F. Does the Policy include: (e) how an individual may complain about a breach of the APPs / registered code, and how the entity will deal with such a complaint;	**In progress**	This information is included in the ABS Privacy Policy and Census Privacy Policy. The MADIP Agreement also includes a specific MADIP complaints process. However, the MADIP website does not provide any information on how complaints can be made in relation to MADIP, and the MADIP Agreement is not (currently) a public document. However, the MADIP Privacy Work Plan includes proposed steps to address this issue.
G. Does the Policy include: (f) whether the entity is likely to disclose personal information to overseas recipients;	**Compliant**	This information is included in the ABS Privacy Policy. It is not a major issue in MADIP.
I. Does the Policy include: (g) if the entity is likely to disclose personal information to overseas recipients—the countries in which such recipients are likely to be located.	**Compliant**	This information is included in the ABS Privacy Policy. It is not a major issue in MADIP.

5.3. APP 1. Finding

It is important for the ABS to be open about the large scale automated acquisition of bulk personal information from MADIP Partner Agencies in MADIP, as well as its own role as a data contributor.

Some limited information is provided in the ABS Privacy Policy and Census Privacy Policy, but not enough to comply with APP 1 or to provide consumers with a reasonable picture of the scale and detail of data shared in MADIP.

Some additional information is provided on the MADIP website, but there are gaps, including key legal documents and a full list of data fields.

The ABS and MADIP Partner Agencies could also consider the development of a specific MADIP Privacy Policy, to reflect the scale and significance of this large national data asset.

The ABS is aware of these issues and is working towards significant improvements in openness and transparency. In early 2018 the ABS established a MADIP Privacy Work Plan to enhance privacy management for MADIP.

6. APP 2. Anonymity and Pseudonymity

6.1. The Law

APP 2 — anonymity and pseudonymity

2.1 Individuals must have the option of not identifying themselves, or of using a pseudonym, when dealing with an APP entity in relation to a particular matter.

2.2 Subclause 2.1 does not apply if, in relation to that matter:

> *(a) the APP entity is required or authorised by or under an Australian law, or a court/tribunal order, to deal with individuals who have identified themselves; or*
>
> *(b) it is impracticable for the APP entity to deal with individuals who have not identified themselves or who have used a pseudonym.*

More information:
<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-2-app-2-anonymity-and-pseudonymity>.

6.2. MADIP – Overview

Some limited anonymity is provided in relation to general browsing of the ABS website and accessing information resources related to MADIP.

For the detailed MADIP activities, the anonymity principle is not particularly relevant.

APP 2. Anonymity	Action / Status	Galexia Commentary
A. Where lawful and practicable, are individuals given the option of: – Not identifying themselves, or – Identifying themselves with a pseudonym?	**Compliant**	The ABS provides some limited anonymity to general website visitors. All of the data shared in MADIP is covered by exceptions to the anonymity principle.

6.3. APP 2. Finding

While not limiting or downplaying the requirement for entities to provide anonymous and pseudonymous options to consumers in appropriate transactions and services on a case-by-case basis, APP 2 is not relevant to the day to day operation of MADIP. APP 2 is not the subject of detailed consideration in this PIA.

7. APP 3. Collection of solicited personal information

7.1. The Law

APP 3 — collection of solicited personal information

Personal information other than sensitive information

3.1 If an APP entity is an agency, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities.

3.2 If an APP entity is an organisation, the entity must not collect personal information (other than sensitive information) unless the information is reasonably necessary for one or more of the entity's functions or activities.

Sensitive information

3.3 An APP entity must not collect sensitive information about an individual unless:

(a) the individual consents to the collection of the information and:

(i) if the entity is an agency — the information is reasonably necessary for, or directly related to, one or more of the entity's functions or activities; or

(ii) if the entity is an organisation — the information is reasonably necessary for one or more of the entity's functions or activities; or

(b) subclause 3.4 applies in relation to the information.

3.4 This subclause applies in relation to sensitive information about an individual if:

(a) the collection of the information is required or authorised by or under an Australian law or a court/tribunal order; or

(b) a permitted general situation exists in relation to the collection of the information by the APP entity [none are relevant to MADIP]; or…

[Galexia Note: some further exceptions for health bodies, enforcement bodies and non-profit organisations – not relevant here]

3.5 An APP entity must collect personal information only by lawful and fair means.

3.6 An APP entity must collect personal information about an individual only from the individual unless:

(a) if the entity is an agency:

(i) the individual consents to the collection of the information from someone other than the individual; or

(ii) the entity is required or authorised by or under an Australian law, or a court/tribunal order, to collect the information from someone other than the individual; or

(b) it is unreasonable or impracticable to do so.

Some additional exceptions known as permitted general situations also apply – these can be found in Section 16A of the Act.

7.2. OAIC Guidelines

The *PIA Guidelines* issued by the OAIC contain a set of hints and risks under the category of personal information to be collected.

The Privacy Risks they have identified include:

- Collecting unnecessary or irrelevant personal information, or intrusive collection; and
- Bulk collection of personal information, some of which is unnecessary or irrelevant.

In addition to these risks, the collection of personal information should generally be kept to a minimum and personal information should normally be collected from the data subject.

The *PIA Guidelines* also contain a set of hints and risks under the category of method of collection.

The Privacy Risks they have identified include:

- Individuals unaware of the collection or its purpose; and
- Covert collection is generally highly privacy invasive, and should only occur under prescribed circumstances.

More information:
<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-3-app-3-collection-of-solicited-personal-information>.

7.3. MADIP – Overview

It can be difficult to apply the concept of data 'collection' to MADIP, as the project is based on data sharing rather than the direct collection of data. The MADIP Agreement refers to the process as 'data acquisition'. However, the OAIC Guidance makes it clear that word "collection" should be broadly interpreted and can be applied to data acquired under data sharing arrangements.

APP 3 contains several 'absolute' requirements (such as 3.1 and 3.5) and several conditional requirements that contain exceptions.

In terms of the absolute requirements, MADIP must therefore only acquire information that is reasonably necessary (APP 3.1) and only acquire information by lawful and fair means.

In terms of the conditional requirements, MADIP is able to rely on the exceptions that are available for acquiring personal information where data sharing is authorised by a law.

The sharing of data with **MADIP** is not directly authorised by any specific law, as MADIP does not operate under a specific legal framework. Instead, sharing with MADIP is allowed based on a combination of notice to consumers (although, see the discussion of notices under APP 5) and exceptions in APP 3, complemented by further exceptions in the legislation that governs MADIP Partner Agencies. The overall result is that the sharing of personal information and sensitive information in MADIP is legal, in that it complies with the relevant exceptions in the *Privacy Act* and the MADIP Partner Agency legislation.

The sharing of **sensitive** information raises some additional compliance requirements under APP 3 and APP 6. These additional requirements apply to the agencies that initially collect sensitive personal information.

MADIP has already acquired and integrated a significant amount of sensitive information. This includes:

1. Health information;
2. Ethnicity and racial background;
3. Indigenous status;
4. Religious affiliation; and
5. Sexuality.

The following table summarises some of the key issues regarding sharing of personal data from the perspective of MADIP:

APP 3. Collection of solicited information	Action / Status	Galexia Commentary
A. Is collected information reasonably necessary for, or directly related to, one or more of the entity's functions or activities?	**Compliant** **Further measures possible**	For the sharing of data with MADIP, it is important to ensure that there is a link between the acquisition of the data by MADIP and the overall purposes and objectives of MADIP. MADIP has a strong data minimisation culture in place, including implementation of the High Level Principles for Commonwealth Data Integration. However, there is room for further strengthening of the data minimisation approach. For example, it may be possible to meet the objectives of MADIP without recording every single detail of ancestry and ethnicity. It may be sufficient to collect data on whether a particular individual or their parents were born 'overseas', without the additional details on 'country of birth'. There may be numerous other similar examples. The intention of this approach is not to restrict valid research activity – it is to ensure that all data items and level of detail are / continue to be appropriate. **Recommendation 3. Minimisation of data sharing** MADIP governance arrangements and public material should clarify that data minimisation occurs both during data sharing and data access for authorised researchers. MADIP should enhance the minimisation of personal data sharing by: 1. Only sharing data fields that are reasonably necessary 2. Excluding irrelevant data items where possible 3. Using data categorisation (e.g. Yes / No responses or bands) rather than specific data fields where possible
B. Is NO sensitive information about an individual collected (unless a relevant exception applies)?	**Compliant** **Further measures possible**	Significant sensitive data has already been acquired under MADIP, including health data, religious affiliation, sexuality and ethnicity. The original collection of sensitive data by Agencies requires either explicit consent or reliance on another APP exception. Reliance on explicit consent is not always possible, but where it can be implemented it has the dual benefit of meeting the requirements of APP 3 and helping to meet the expectations of consumers. The sharing of sensitive data with MADIP can be achieved by reliance on the exception in APP 3.4 (a), which allows sensitive data to be acquired where this is authorised by a specific law. MADIP also has a role to play in ensuring that the acquisition and sharing of sensitive data in MADIP is minimised. This will help to reduce the overall risk profile of MADIP and to help the project align with community expectations. **Recommendation 4. Minimise amount of sensitive data** MADIP should implement a review of all sensitive data fields to assess whether it is reasonably necessary to acquire sensitive data. Unnecessary data fields should be removed from future data acquisition and deleted / quarantined from existing MADIP data holdings.

C. Is personal information collected only by lawful and fair means?	**Compliant**	ABS and MADIP Partner Agencies have taken steps to ensure that all data being shared under MADIP has been collected by lawful and fair means. MADIP would benefit from the development of a Public Register citing the legal basis / public interest certificate for each disclosure of data from Partner Agencies to MADIP. This is discussed in further detail in the sections on openness (APP 1) and governance.
D. Is personal information about an individual collected only from the individual (unless a relevant exception applies)?	**Compliant**	MADIP is a data integration, combining data from multiple sources. It is likely that the acquisition of data from multiple sources is compliant with APP 3 due to the broad exceptions in APP 3.6.

7.4. APP 3. Finding

APP 3 contains several 'absolute' requirements (such as 3.1 and 3.5) and several conditional requirements that contain exceptions.

In terms of the absolute requirements, MADIP must therefore only acquire information that is reasonably necessary (APP 3.1) and only acquire information by lawful and fair means. This PIA includes two recommendations to ensure that MADIP is taking steps to minimise the data that is collected, in order to meet the requirement in APP 3.1.

In terms of the conditional requirements, MADIP is able to rely on the exceptions that are available for acquiring personal information where data sharing is authorised by a law.

8. APP 4. Dealing with unsolicited personal information

8.1. The Law

APP 4 requires entities who receive unsolicited personal information to determine whether or not they could have collected the information under APP 3. If they determine that they could *not* have collected the personal information; the information must be destroyed.

More information:
<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-4-app-4-dealing-with-unsolicited-personal-information>.

8.2. MADIP – Overview

APP 4 requires agencies and organisations to assess unsolicited information as it arrives, and destroy it if it is information that they could not have collected themselves.

Although the ABS and MADIP Partner Agencies are bound by the rules on unsolicited personal information, this APP is not particularly relevant to MADIP.

APP 4. Dealing with unsolicited information	Action / Status	Galexia Commentary
A. Are there circumstances in which the ABS may receive unsolicited personal information?	**Compliant**	MADIP is very unlikely to receive unsolicited personal information.
B. Does the ABS have a policy in place for managing unsolicited personal information in accordance with the Privacy Act?	**Compliant**	This requirement is not relevant to MADIP.

8.3. APP 4. Finding

MADIP is unlikely to have an impact on APP 4 compliance.

9. APP 5. Notification of the collection of personal information

9.1. The Law

APP 5 — notification of the collection of personal information

5.1 At or before the time or, if that is not practicable, as soon as practicable after, an APP entity collects personal information about an individual, the entity must take such steps (if any) as are reasonable in the circumstances:

> *(a) to notify the individual of such matters referred to in subclause 5.2 as are reasonable in the circumstances; or*
>
> *(b) to otherwise ensure that the individual is aware of any such matters.*

5.2 The matters for the purposes of subclause 5.1 are as follows:

> [Galexia Note: itemised list follows]

More information:
<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-5-app-5-notification-of-the-collection-of-personal-information>.

9.2. MADIP – Overview

APP 5 contains a series of 'absolute' requirements with no exceptions.

The compliance of ABS and MADIP Partner Agencies with APP 5 can be assessed using the following checklist. The table concentrates on issues relevant to the ABS. Galexia has not assessed the compliance of MADIP Partner Agencies in detail:

APP 5. Notification	Action / Status	Galexia Commentary
A. Does the entity provide notice of its identity and contact details?	**Compliant**	ABS notices correctly identify ABS and include relevant contact details. MADIP Partner Agency notices correctly identify each agency and include relevant contact details
B. Does the entity provide notice of third party collection? (if relevant)	**Action required** **(in progress)**	Generally, the ABS and MADIP Partner Agency notices do not provide notice of the scale of third party collection that is envisaged under MADIP. For example, the ABS notice has a short and potentially confusing reference to the potential collection of information from 'administrative sources', without further elaboration. This term may create confusion as MADIP makes clear promises that data will never be used for monitoring, enforcement or 'administration'. Although third party collection is briefly mentioned, a consumer is unlikely to be on notice regarding bulk sharing of third party data, automated sharing of third party data, or the range of third parties involved. ('Automated sharing' is where data is automatically shared rather than where information on a specific individual or group of individuals is provided on request. 'Bulk data sharing' is where all population data is shared rather than a sample of data subjects). This issue is the subject of a current review at ABS. In early 2018 the ABS established a MADIP Privacy Work Plan to enhance privacy management for MADIP. Item 7 of the Work Plan includes the consideration of improvements to ABS privacy notices.

		Recommendation 5. Amend privacy notices to clarify scale of third party data acquisition To deliver best practice in openness and transparency, ABS may wish to review and amend privacy notices to clarify the scale of third party data acquisition, the use of automated and bulk third party data acquisition and the expanded list of third parties that are involved.
C. Does the entity provide notice of the fact that the collection is required or authorized? (if relevant)	**Compliant**	Generally, ABS and MADIP Partner Agency notices include extensive notice regarding the collection of data that is authorised by law, with details of relevant legislation. For example, ABS notices regarding the Census are clear on this issue.
D. Does the entity provide notice of the purpose of collection?	**Compliant**	Generally, ABS and MADIP Partner Agency notices include extensive notice regarding the original purpose of collection of data.
E. Does the entity provide notice of the main consequences (if any) for the individual if all or some of the personal information is not collected?	**Compliant**	Generally, ABS and MADIP Partner Agency notices include sufficient notice regarding the consequences of not providing data. For example, ABS notices regarding the Census make it clear that the provision of data is mandatory.
F. Does the entity provide notice of any other APP entity, body or person, or the types of any other APP entities, bodies or persons, to which the APP entity usually discloses personal information of the kind collected?	**Action required** **(in progress)**	In MADIP a variety of data may be shared between agencies and MADIP and then between MADIP and researchers. Compliance with APP 5 (f) therefore needs to be assessed for each proposed disclosure. Current MADIP Partner Agency notices do not provide notice of the scale of disclosure that is taking place under MADIP. Although disclosure to other Agencies is discussed in broad terms, a consumer is unlikely to be on notice regarding bulk, automated disclosure to MADIP or the fact that all of their data is disclosed. For example, all DHS privacy notices state: *Your information may be used by the department, or given to other parties where you have agreed to that, or where it is required or authorised by law (including for the purpose of research or conducting investigations).* This type of statement minimises the nature of data sharing and also conflates research and investigations. Notices should ideally clarify that all data is automatically shared with MADIP for research and statistical purposes and would also reassure consumers that data sharing with MADIP is **not** for investigative purposes. This issue is the subject of a current review at ABS. In early 2018 the ABS established a MADIP Privacy Work Plan to enhance privacy management for MADIP. Item 8 of the Work Plan includes the consideration of improvements to MADIP Partner Agency privacy notices. **Recommendation 6. Amend privacy notices to clarify the scale and nature of data sharing** To deliver best practice in openness and transparency, MADIP Partner Agencies may wish to review and amend privacy notices to clarify the scale and detail of disclosure to the ABS for MADIP and the use of automated and bulk data sharing.

G. Does the entity provide notice that the privacy policy contains information about how the individual may access their personal information and seek the correction of such information?	**Compliant**	Generally, ABS and MADIP Partner Agency notices include a brief notice regarding the availability of access to data. Typically, consumers are directed to the Privacy Policy for further information. Although such notices technically meet the APP requirements in relation to each agency, they provide little information or assistance to a consumer who has an access request or query in relation to MADIP. Solutions to this issue are discussed elsewhere in the sections on openness and access.
H. Does the entity provide notice that the privacy policy contains information about how the individual may complain?	**Compliant**	Generally, ABS and MADIP Partner Agency notices include a very brief notice regarding the availability of a complaints process. Typically, Consumers are directed to the Privacy Policy for further information.
I. Does the entity provide notice of whether the entity is likely to disclose the personal information to overseas recipients (and if so, where)?	**Compliant**	Generally, ABS and MADIP Partner Agency notices include a very brief notice regarding the potential disclosure of data to other countries. This issue is not particularly relevant to MADIP.

9.3. APP 5. Finding

Generally, ABS and MADIP Partner Agency notices are compliant with many of the requirements of APP 5.

However, these notices typically paint a picture that most data is collected from individuals, rather than third parties, and that any exceptions to this approach are minor. The forms also paint a picture that data is disclosed to a small number of other agencies for a range of very specific purposes. Research may be briefly mentioned as one of these purposes, but it is highly unlikely that a person reading the notice would understand that all of their data is automatically shared with MADIP and integrated with other data they have provided to other agencies.

ABS is conscious of the need to raise awareness of MADIP. The privacy notices used by ABS and MADIP partners are in the process of being reviewed and updated to ensure that all parties are open about the use of bulk and automated data sharing and data linking practices.

10. APP 6. Use or disclosure of personal information

10.1. The Law

APP 6 — use or disclosure of personal information

Use or disclosure

6.1 If an APP entity holds personal information about an individual that was collected for a particular purpose (the primary purpose), the entity must not use or disclose the information for another purpose (the secondary purpose) unless:

> *(a) the individual has consented to the use or disclosure of the information; or*
>
> *(b) subclause 6.2 or 6.3 applies in relation to the use or disclosure of the information.*

6.2 This subclause applies in relation to the use or disclosure of personal information about an individual if:

> *(a) the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose and the secondary purpose is:*
>
> > *(i) if the information is sensitive information — directly related to the primary purpose; or*
> >
> > *(ii) if the information is not sensitive information — related to the primary purpose; or*
>
> *(b) the use or disclosure of the information is required or authorised by or under an Australian law or a court/tribunal order; or*
>
> *...*
>
> *(e) the APP entity reasonably believes that the use or disclosure of the information is reasonably necessary for one or more enforcement related activities conducted by, or on behalf of, an enforcement body.*

10.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Australian Information Commissioner contain a set of hints and risks under the category of purpose, use and disclosure.

The Privacy hints they have identified include:

- No surprises! Use personal information in ways that are expected by the individual
- No surprises! Tell the individual about disclosures

The Privacy Risks they have identified include:

- Using personal information for unexpected secondary purposes
- Unnecessary or unexpected data linkage
- Unexpected disclosures can lead to privacy complaints

More information:
<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-6-app-6-use-or-disclosure-of-personal-information>.

10.3. MADIP – Overview

MADIP involves a significant expansion of the use and disclosure of personal data.

The OAIC's PIA Guidelines, discussed above, warn against the unexpected or surprise use of data.

In MADIP, the ABS is managing the integration of numerous data sets that have previously been maintained in separate 'silos'. In turn, Government as a whole is benefiting from some ABS data being integrated into MADIP.

The disclosure of data by agencies to MADIP is not directly authorised by any specific law, as MADIP does not operate under a specific legal framework. Instead, the disclosure is based on a combination of notices to consumers (although, refer to the discussion of notices under APP 5) and exceptions in APP 6, complemented by further exceptions in the legislation that governs MADIP Partner Agencies.

For Census data, the ABS is usually prohibited from disclosing any data that identifies an individual. But in this case the data is collected directly by the ABS under the *Census and Statistics Act 1905* (Cth), and the ABS is also the Accredited Integrating Authority for MADIP, so no prohibited disclosure occurs under MADIP.

For the MEDB and MCDB data there are normally strict restrictions on the disclosure of identifiable information. However, an exception in Section 130 of the *Health Insurance Act 1973* (Cth) provides that the Secretary or the Chief Executive of Medicare may disclose information collected under the Act, where the Minister certifies that it is necessary in the public interest.

For the PIT data, there are normally strict restrictions in place regarding the disclosure of any data that identifies an individual. However, the ATO is permitted to disclose this data to the Australian Statistician under the *Taxation Administration Act 1953* (Cth) for the 'purpose of administering the *Census and Statistics Act 1905*'. MADIP is conducted under this legislation.

For the SSRI data there are normally strict restrictions on the disclosure of identifiable information. However, several exceptions allow the data to be disclosed where it is in the public interest. These are found in:

- Section 208 of the *Social Security (Administration) Act 1999* (Cth);
- Section 168 of the *A New Tax System (Family Assistance) (Administration) Act 1999* (Cth);
- Section 128 of the *Paid Parental Leave Act 2010* (Cth); and
- Section 355 of the *Student Assistance Act 1973* (Cth).

The overall result is that the disclosure of personal information and sensitive information in MADIP is legal, in that it complies with the relevant exceptions in the *Privacy Act* and the MADIP Partner Agency legislation.

Compliance with APP 6 requires can be achieved by obtaining consent in some circumstances. However, this presents challenges for a data sharing project like MADIP:

- A large majority of the data that will be shared or matched has already been collected by the ABS and MADIP Partner Agencies, and it is difficult to obtain consent for sharing data that may have been collected some years ago;
- Data in MADIP covers all Australians, including children and individuals who do not have the capacity to provide consent;
- MADIP is expected to include longitudinal data, not just 'snapshot' data, and consent requirements for individuals may change over time (e.g. where a child becomes an adult and is now able to provide their own consent); and
- The majority of data collected in MADIP was originally collected in circumstances where the collection was mandatory (e.g. the census) or the consumer has no real alternative other than providing the information (e.g. health, taxation and welfare). No MADIP Partner Agencies offer a separate consent process (i.e. you cannot consent to the provision of services and object to the use of your data for research).

In practice, the role of consent will therefore be very limited in MADIP. The sharing of the data with MADIP therefore relies heavily on exceptions to APP 6, as discussed in the table below.

However, the MADIP program does have some potential safeguards against the *further* disclosure of personal information. For example, the ABS assert that 'MADIP data has the added protection of the *Census and Statistics Act* 1905 which ensures that no data will be released in a manner that will enable an individual to be identified'. Significant sanctions apply for the unauthorised disclosure of MADIP data.

The following table summarises the key compliance tasks relevant to APP 6:

APP 6. Use or Disclosure	Action / Status	Galexia Commentary
A. Has the entity clearly defined the primary purpose of collection and identified any secondary purposes?	**Compliant** **Further measures possible**	The ABS privacy notices describe the primary purpose and secondary purposes. As a primary function of ABS is research and the provision of statistics, it is easy for ABS to comply with APP 6 in relation to its own contribution of data to MADIP. However, for MADIP Partner Agencies the situation is more complex. The data is proposed to be shared with MADIP (and then with researchers) for a variety of research related purposes. As many of these purposes will be purposes that are relevant to other parties, not the collecting agency, they are unlikely to be covered by the primary purpose of collection. Whether or not MADIP Partner Agencies have clearly identified these secondary purpose depends on the agency and the specific form being completed by the consumer. This issue is the subject of a review by the ABS. In early 2018 the ABS established a MADIP Privacy Work Plan to enhance privacy management for MADIP. Item 8 of the Work Plan includes the consideration of improvements to MADIP Partner Agency privacy notices. **Recommendation 7. Amend privacy notices to ensure that data sharing with MADIP is described as a secondary purpose** To deliver best practice in openness and transparency, MADIP Partner Agencies may wish to consider amending privacy notices at the point of collection, as well as other public information, to indicate that data may be shared and used for statistical and research purposes, including data integration.

B. Will the entity only disclose personal information for a secondary purpose with consent (or a relevant exception)? **[Non sensitive information]**	**Compliant**	In MADIP a variety of data is proposed to be shared by agencies with the ABS. Compliance with APP 6 therefore needs to be assessed for each proposed disclosure. Where data is shared with another agency for purposes that are more closely related to *their* activities (e.g research managed by the ABS), rather than a function of the original collecting agency (e.g. taxation or health management) then APP 6 requires either consent or reliance on an exception. Where the data sharing still retains some link to a function of the original collecting agency, then the exceptions in APP 6.2 (a) can be used (meaning that data can be disclosed without consent). However, this exception require a degree of 'reasonable expectation' by consumers that the disclosure will occur, and this may be difficult to achieve for MADIP Partner Agencies in relation to bulk and automated data sharing for a wide range of research and statistical purposes under the banner of MADIP. This exception will be easier to use once the community is more aware of MADIP and data sharing falls within the reasonable expectations of consumers. MADIP has not yet reached this stage. However, MADIP Partner Agencies can also rely on the exception in APP 6.2 (b) – that the disclosure is authorised by a law. Some agencies have specific legislative provisions; others rely on Public Interest Certificates issued under legislative instruments.
B. Will the entity only disclose personal information for a secondary purpose with consent (or a relevant exception)? **[Sensitive information]**	**Compliant** **Further measures possible**	In MADIP a significant amount of sensitive information is shared. Where sensitive data is shared with another agency for purposes that are more closely related to *their* activities (e.g research managed by the ABS), rather than a function of the original collecting agency (e.g. taxation or health management) then APP 6 requires either consent or reliance on another exception. APP 6.2 (a) (i) allows sensitive information to be shared where the secondary purpose is **directly** related to the original purpose. This higher test will be very difficult to apply in MADIP for most Partner Agencies. This exception also requires a degree of 'reasonable expectation' by consumers that the disclosure will occur, and this will be extremely difficult to achieve for MADIP Partner Agencies in relation to bulk and automated data sharing of sensitive data for a wide range of research and statistical purposes under the banner of MADIP. MADIP Partner Agencies can also rely on the exception in APP 6.2 (b) – that the disclosure is authorised by a law. Some agencies point to their own specific legislative provisions. Others are relying on Public Interest Certificates. An additional issue is that the agency legislation and public interest certificates do not differentiate between general personal information and sensitive information. **Recommendation 8. MADIP Partner Agency legal authorities (e.g. Public Interest Certificates) should differentiate between general personal information and sensitive information** To deliver best practice in data management, MADIP agencies may wish to consider differentiating between general personal information and sensitive information in future Public Interest Certificates issued for the MADIP. The asserted legal basis / public interest in sharing and integrating sensitive information in MADIP should be clearly disclosed to the public

C. Is any biometric information only disclosed for a secondary purpose in accordance with Clause 6.3 and the relevant OAIC Guidelines?	**Compliant**	No biometric data is shared in MADIP.
D. Is a written note made of any disclosures that are made relying on the law enforcement exception?	**Compliant**	MADIP disclosures do not rely on the law enforcement exception.

10.4. APP 6. Finding

The disclosure of data by agencies to MADIP is not directly authorised by any specific law, as MADIP does not operate under a specific legal framework. Instead, the disclosure is based on a combination of notices to consumers and exceptions in APP 6, complemented by further exceptions in the legislation that governs MADIP Partner Agencies.

APP 6 usually envisages a link between the use of data and the purposes of the collecting agency. Once data is shared with another agency, for their purposes, the consent of the individual is required.

However, MADIP Partner Agencies can also rely on the exception in APP 6.2 (b) – that the disclosure is authorised by a law. Some agencies point to their own specific legislative provisions. Others are relying on Public Interest Certificates.

Compliance with APP 6 therefore only requires some minor enhancements for MADIP, as set out above.

11. APP 7. Direct marketing

11.1. The Law

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.

More information:
<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-7-app-7-direct-marketing>.

11.2. MADIP – Overview

Direct marketing is not relevant to MADIP.

11.3. APP 7. Finding

Direct marketing is not relevant to MADIP.

12. APP 8. Cross-border disclosure of personal information

12.1. The Law

APP 8 states that before an organisation discloses personal information to an overseas recipient, they must take reasonable steps to ensure that the overseas recipient does not breach the APPs in relation to the information. The organisation that discloses personal information to an overseas recipient is accountable for any acts or practices of the overseas recipient. Several exceptions apply.

APP 8 — Cross-border disclosure of personal information

*8.1 Before an APP entity discloses personal information about an individual to a person (the **overseas recipient**):*

> *(a) who is not in Australia or an external Territory; and*
>
> *(b) who is not the entity or the individual;*

the entity must take such steps as are reasonable in the circumstances to ensure that the overseas recipient does not breach the Australian Privacy Principles (other than Australian Privacy Principle 1) in relation to the information.

Note: In certain circumstances, an act done, or a practice engaged in, by the overseas recipient is taken, under section 16C, to have been done, or engaged in, by the APP entity and to be a breach of the Australian Privacy Principles.

8.2 Subclause 8.1 does not apply to the disclosure of personal information about an individual by an APP entity to the overseas recipient if:

> *(a) the entity reasonably believes that:*
>
> > *(i) the recipient of the information is subject to a law, or binding scheme, that has the effect of protecting the information in a way that, overall, is at least substantially similar to the way in which the Australian Privacy Principles protect the information; and*
> >
> > *(ii) there are mechanisms that the individual can access to take action to enforce that protection of the law or binding scheme; or*
>
> *(b) both of the following apply:*

(i) the entity expressly informs the individual that if he or she consents to the disclosure of the information, subclause 8.1 will not apply to the disclosure;

(ii) after being so informed, the individual consents to the disclosure; or

(c) [Galexia note: several additional exceptions apply, but it is difficult to see how these will be relevant to MADIP]

More information:
<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-8-app-8-cross-border-disclosure-of-personal-information>.

12.2. MADIP – Overview

Cross border data transfers are not particularly relevant to MADIP.

12.3. APP 8. Finding

Cross border data transfers are not particularly relevant to MADIP. They have not been considered in detail in this PIA.

13. APP 9. Adoption, use or disclosure of government related identifiers

13.1. The Law

APP 9 states that an organisation must not adopt a government related identifier of an individual as its *own* identifier. In addition, an organisation must not use or disclose a government related identifier of an individual unless the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual. Some other exceptions apply.

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-9-app-9-adoption-use-or-disclosure-of-government-related-identifiers>.

13.2. MADIP – Overview

APP 9 contains two key requirements:

The first is that organisations must not adopt a government identifier as their own identifier. This is designed to prevent the development of de facto national identifiers. For example, organisations cannot use the Tax File Number (issued by the Commonwealth government) as their own identifier.

Each MADIP Partner Agency uses its own unique identifiers and is compliant with this first requirement.

The second requirement of APP 9 is that government related identifiers should not be disclosed except in specific situations where the disclosure is reasonably necessary to verify identity. The OAIC guidelines note that:

> *the circumstances in which an organisation may use or disclose government related identifiers under APP 9.2 are narrower in scope than the circumstances in which an organisation may use or disclose other personal information under APP 6*

However, organisations are allowed to use or disclose government related identifiers if the use or disclosure is reasonably necessary for the organisation to verify the identity of the individual (APP 9.2(a)).

APP 9 does not generally apply to agencies apart from some prescribed commercial activities undertaken by agencies. The MADIP Partner Agencies do not undertake such activities as part of their business as usual practices.

The ABS may incidentally use a government related identifier as part of its identity linking and identity verification process, however these are never disclosed by the ABS to any external parties. This use of identifiers would be covered by the exception in APP 9.2(a).

13.3. APP 9. Finding

APP 9 does not apply to agencies such as the ABS.

14. APP 10. Quality of personal information

14.1. The Law

APP 10 — quality of personal information

10.1 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity collects is accurate, up-to-date and complete.

10.2 An APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information that the entity uses or discloses is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant.

14.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Australian Information Commissioner contain a set of hints and risks under the category of data quality.

The Privacy Risks they have identified include:

- Retaining personal information unnecessarily
- Making decisions based on poor quality data

More information:
<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-10-app-10-quality-of-personal-information>.

14.3. MADIP – Overview

Data quality is a core objective of MADIP. The ABS plays an important role in verifying identity links based on information that is submitted by MADIP Partner Agencies.

There is a need to mitigate and manage some risks in terms of data quality and the ABS is conscious of the importance of accurate data and accurate data linking processes. In MADIP, research outputs and analysis will be relied on by a range of third parties, including policy makers and planners.

Some of the potential risk areas include:

1. Basing decisions on information supplied by third parties may lead to errors. These could be errors based on poor quality links, incorrect information or out of date information;
2. Making links between diverse data sets is a difficult process, and some incorrect matches are likely to emerge;
3. Relying on third party data (rather than data supplied directly by the data subject) means that the ABS (and researchers) may only receive a limited view of the consumer's full circumstances. For example, the data may be missing important contextual information;
4. Relying on third party data may lead to situations where the ABS is unaware that the consumer is challenging the accuracy of that data; and
5. Where data is shared between agencies and the ABS the data may be stored in multiple locations, leading over time to multiple data sets with slightly different data.

The following table summarises compliance with APP 10, but it is very important to note that the data quality issues need to be assessed on a case by case basis for each disclosure.

APP 10. Data Quality	Action / Status	Galexia Commentary
A. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information collected is accurate, up-to-date and complete?	**Compliant**	The ABS has extensive systems in place for ensuring that its own data is accurate. These systems are not the subject of detailed consideration in this PIA. MADIP may have an impact on data quality and this will have to be assessed on a case by case basis.
B. Has the entity taken such steps (if any) as are reasonable in the circumstances to ensure that the personal information **that the entity uses or discloses** is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant?	**Compliant**	There is a continual assessment of data linking processes in MADIP to assess the accuracy of data that can be provided by Partner Agencies.

14.4. APP 10. Finding

The ABS has extensive systems in place for ensuring that its own data is accurate.

MADIP may have an impact on data quality and this will have to be assessed on a case by case basis. There is continual assessment of data linking processes in MADIP to check the accuracy of data.

15. APP 11. Security of personal information

15.1. The Law

APP 11 requires entities to take such steps as are reasonable in the circumstances to protect personal information from misuse, interference and loss; and from unauthorised access, modification or disclosure.

Also, if the organisation no longer needs the information for any purpose for which the information may be used or disclosed, they must take such steps as are reasonable in the circumstances to destroy the information or to ensure that the information is de-identified.

15.2. OAIC Guidelines

APP 11 has a wide scope for interpretation, as it includes multiple tests for what is 'reasonable in the circumstances'. Some additional guidance is available from the Office of the Australian Information Commissioner (OAIC) in the form of guidelines:

- *Guide to securing personal information*, OAIC, 2015 <https://www.oaic.gov.au/agencies-and-organisations/guides/guide-to-securing-personal-information>

More information: <https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information>.

15.3. MADIP – Overview

Given the significant security risks in a project of MADIP's size it is vital that regular independent security risk assessments are undertaken. As MADIP involves the acquisition of data from a variety of partners, using a diverse range of transfer and storage methods, the management of security risks is complex.

The ABS is aware of this requirement and has recently commissioned an independent security risk assessment of MADIP. At the time of writing this PIA, the review has not yet been completed.

In relation to compliance with APP 11, MADIP faces the following challenges (this is not an exhaustive list):

1. **The security risk profile of the data involved in MADIP is extremely high**, as it MADIP relies on the initial acquisition of personal information and sensitive information that would have an impact on individuals, MADIP and individual agencies if it was made available;
2. The combined amount of data in MADIP makes it one of **Australia's largest and richest sources of detailed personal information**;
3. Data provided by MADIP Partner Agencies is comprehensive and **covers the entire population** – it is not a sample of available data; and
4. The value of the data to third parties is high, and the **data could be the target of external attack** (e.g. hacking or impersonation attempts).

In addition, the data retention and data destruction requirements of APP 11 are very difficult to manage where data is shared amongst multiple agencies and data is intended to be retained indefinitely.

The following table provides a high level summary of potential compliance with APP 11 regarding MADIP. This summary is not a substitute for the full independent security risk assessment (which is currently in progress).

APP 11. Security	Action / Status	Galexia Commentary
A. Has the entity taken such steps as are reasonable in the circumstances to protect the information from misuse, interference and loss?	**Action required**	MADIP has a very high security risk profile, and it is vital that all aspects of MADIP are subject to regular, independent security risk assessments. At the time of completing this PIA, the ABS has commissioned a full iRAP assessment of the 'end to end' MADIP process for data acquisition, integration and storage. The assessment is being conducted in accordance with the Australian Signals directorate (ASD) InfoSec Registered Assessors Program (iRAP). This is an important first step in ensuring confidence in the security of MADIP, but compliance with APP 11 will require ongoing, regular independent assessments. **Recommendation 9. Mandate regular independent security risk assessments for MADIP** The ABS should commission regular independent security risk assessments for MADIP. The reviews should establish minimum security standards for all data sharing and require further independent security risk assessments for any new data exchanges. In addition to the independent assessment of the current approach to security at MADIP, the ABS should also continue to examine the best available security models for sharing data amongst agencies. The current model requires all MADIP Partner Agency data to be supplied to a single location for integration. Alternative models may become feasible over time, such as federated data sharing models. The security strengths and weaknesses of these models should be assessed, and MADIP should not tie itself down to a single approach. The ABS is aware of this issue and the MADIP Privacy Work Plan includes an item regarding the ongoing consideration of data sharing models for MADIP. **Recommendation 10. Consider alternative data sharing models on an ongoing basis** MADIP should consider alternative data sharing models on an ongoing basis. The current data centralisation model should be the subject of constant evaluation against alternatives such as a federated model. These evaluations should assess the comparative security risk profile of each model (amongst other factors).
B. Has the entity taken such steps as are reasonable in the circumstances to protect the information from unauthorised access, modification or disclosure?	**Compliant**	The ABS has processes in place to guard against unauthorised access while the data is held by the ABS. ABS legislation includes severe penalties for unauthorised access (although it is unclear if these also apply to data provided by MADIP Partner Agencies while the data is in transit).
C. Does the level of security in the application match the potential harm caused by breaches of privacy?	**In progress**	The data being exchanged in MADIP includes sensitive personal information that is initially provided to MADIP. The scale of the data involved is also significant. It is important for security settings to match the potential harm of any breaches.

		The ABS already applies high security standards to MADIP, but it may be necessary to strengthen these standards based on the findings and recommendations of the independent security risk assessment that is currently in progress. **Recommendation 11. Impose highest possible security standards to match risk profile of data** MADIP should impose security standards consistent with the Australian Government Information Security Manual and the Protective Security Framework on data sharing arrangements, to reflect the sensitivity and scale of the data being exchanged.
D. Will detailed access trails be retained and scrutinised for security breaches?	**In progress**	The ABS already applies detailed access logging requirements to MADIP, but it may be necessary to strengthen these requirements based on the findings and recommendations of the independent security risk assessment that is currently in progress.
E. Will a data retention policy / destruction schedule be developed which requires retention of personal information only for the period required for use?	**Action required**	The ABS has a formal data retention policy in place for its own data. However, the intention in MADIP is that data will be retained as long as there is a business need to do so. In practice, data can be retained indefinitely, and MADIP is designed to be an 'enduring' data set. The indefinite retention of data raises the security risk profile of MADIP. It may also raise concerns for data subjects, as they have not directly agreed to be subjects in the equivalent of a longitudinal data study. This issue is the subject of a review by the ABS. In early 2018 the ABS established a MADIP Privacy Work Plan to enhance privacy management for MADIP. Item 13 of the Work Plan includes the consideration of the development of a MADIP data retention policy. **Recommendation 12. Consider data destruction and de-identification requirements** MADIP should continue to review its approach to data retention and destruction.
F. Is personal information de-identified as soon as possible?	**Compliant**	MADIP has a sophisticated approach to the de-identification of data. 1. Names and addresses are separated from other information in most source datasets prior to supply for MADIP (and are supplied separately). 2. Identifiable information is de-identified in the linkage process (e.g. through encoding), prior to analytical datasets being assembled for use by researchers. 3. Analytical data provided to researchers do not contain directly identifiable information, and outputs are checked for confidentiality prior to release. ABS have advised that names and addresses collected in the 2016 Census will be securely retained for up to four years (i.e. up to August 2020), and only while there is community benefit in doing so. Census names are encoded prior to use in data integration projects (such as the MADIP), which enables the ABS to maximise the value of Census data and protect privacy. ABS has advised that encoded Census names ● Cannot be reversed to a single value, ● Are stored in separate computing environments, and ● Can only be accessed by ABS staff who are not using analytical variables such as family status and housing arrangements

15.4. APP 11. Finding

The data being exchanged in MADIP has a very high security risk profile, and APP 11 requires reasonable steps to be taken to protect MADIP data from unauthorised access.

The ABS is aware of this requirement and has recently commissioned an independent security risk assessment of MADIP. At the time of this PIA, the review has not yet been completed.

Currently there are strong security measures in place for MADIP. These include:

- Storage of all data in the 'NextGen Infrastructure Environment',
- Implementation of functional separation of linkage data from other data variables,[12]
- Implementation of the 5 Safes Framework,[13] and
- Restricting access to MADIP via the ABS DataLab.[14]

APP 11 also requires MADIP to establish appropriate rules for the destruction and de-identification of data.

The ABS is aware of this issue and the MADIP Privacy Work Plan includes an item regarding the development of a data retention policy for MADIP.

Compliance with APP 11 and the establishment of a comprehensive security compliance framework for MADIP is recognised as a priority action item for the ABS.

[12] More information on the Seperation Principle is contained in *A Guide for Data Integration Projects Involving Commonwealth Data for Statistical and Research Purposes* (Australian Government National Statistical Service), available at <https://statistical-data-integration.govspace.gov.au/topics/applying-the-separation-principal>.

[13] More information on the Five Safes Framework is contained in *Managing the Risk of Disclosure: The Five Safes Framework* (Australian Bureau of Statistics, Confidentiality Series 116.0, August 2017) available at: <http://www.abs.gov.au/ausstats/abs@.nsf/Latestproducts/1160.0Main%20Features4Aug%202017?opendocument&tabname=Summary&prodno=1160.0&issue=Aug%202017&num=&view=>.

[14] For a general overview of relevant protections in place at the Australian Bureau of Statistics, refer to: *The Confidentiality Series* (ABS 116.0, August 2017), available at: <http://www.abs.gov.au/ausstats/abs@.nsf/mf/1160.0>.

16. APP 12. Access to personal information

16.1. The Law

APP 12 — access to personal information

Access

12.1 If an APP entity holds personal information about an individual, the entity must, on request by the individual, give the individual access to the information.

Exceptions to access…

More information:
<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-11-app-11-security-of-personal-information>.

16.2. MADIP – Overview

Access requests under APP 12 raise some complex issues for MADIP.

Each individual agency remains responsible for managing access requests relating to their own data holdings, and this includes the ABS in relation to its own core data sets. Some MADIP access requests may also be received by the Accredited Integrating Authority (also ABS) and there may be some confusion about whether an access request to the ABS automatically covers data held by MADIP.

ABS has a **general exemption** to access requests to MADIP data. The *Privacy Act* allows an agency to refuse access where they are authorised under Freedom of Information (FOI) legislation to refuse access. The *Freedom of Information Act 1982* (Cth) (Schedule 2, Part II, Division 2) exempts the ABS from providing access to documents containing information collected under the *Census and Statistics Act 1905* (Cth). This general exemption could be extended to cover MADIP as the *Census and Statistics Act 1905* (Cth) is also the legislation under which the ABS acquires MADIP data in its role as the Accredited Integrating Authority.

The other MADIP Partner Agencies are not subject to this exception, and under APP 12 they may still be deemed to 'hold' personal information where they have shared it with another agency. That is, they may retain their access request responsibilities.

The following table summarises the key requirements of APP 12:

APP 12. Access	Action / Status	Galexia Commentary
A. Can the individual ascertain whether the entity has records that contain personal information, the nature of that information and the steps that the individual should take to access their record?	**Action required**	ABS has general access policies and procedures in place, but there is no specific information available in relation to MADIP access requests. The ABS is aware of this issue and has recently begun work a statement on Access and Corrections Policy for MADIP and will make this available as part of the MADIP FAQ. **Recommendation 13. MADIP should publish detailed information regarding access requests** The MADIP Agreement, the MADIP website and relevant privacy policies should provide detail on the MADIP Access request process. **Note:** These access requests do not relate to the process of accessing analytical information for research, as this information is de-identified.

B. If an agency holds personal information about an individual, does the agency, on request by the individual, give the individual access to the information? (unless relevant exceptions apply)	**Compliant**	ABS has access policies and procedures in place that are fully compliant with APP 12 in relation to its own data. Data collected under the Census legislation is exempt from access requests, and this may extend to MADIP data held by the ABS.

16.3. APP 12. Finding

APP 12 requires the ABS and MADIP Partner Agencies to provide clear information to consumers on how they can access their data. The extent of access to MADIP data may be limited by exemptions that are available to the ABS under privacy and FOI legislation.

The ABS is aware of this issue and has recently begun work on a statement on Access and Corrections and will make this available as part of the MADIP FAQ.

17. APP 13. Correction of personal information

17.1. The Law

APP 13 — correction of personal information

Correction

13.1 If:

> *(a) an APP entity holds personal information about an individual; and*
>
> *(b) either:*
>
> > *(i) the entity is satisfied that, having regard to a purpose for which the information is held, the information is inaccurate, out of date, incomplete, irrelevant or misleading; or*
> >
> > *(ii) the individual requests the entity to correct the information;*
>
> *the entity must take such steps (if any) as are reasonable in the circumstances to correct that information to ensure that, having regard to the purpose for which it is held, the information is accurate, up to date, complete, relevant and not misleading.*

Notification of correction to third parties

13.2 If:

> *(a) the APP entity corrects personal information about an individual that the entity previously disclosed to another APP entity; and*
>
> *(b) the individual requests the entity to notify the other APP entity of the correction;*

the entity must take such steps (if any) as are reasonable in the circumstances to give that notification unless it is impracticable or unlawful to do so.

…

Dealing with requests

13.5 If a request is made under subclause 13.1 or 13.4, the APP entity:

> *(a) must respond to the request:*
>
> > *(i) if the entity is an agency — within 30 days after the request is made; or*
> >
> > *(ii) if the entity is an organisation — within a reasonable period after the request is made; and*
>
> *(b) must not charge the individual for the making of the request, for correcting the personal information or for associating the statement with the personal information (as the case may be).*

17.2. OAIC Guidelines

The *PIA Guidelines* issued by the Office of the Australian Information Commissioner contain a set of hints and risks under the category of correction of personal information.

- Getting access to personal information should be clear and straightforward.
- Inaccurate information can cause problems for everyone!

More information:
<https://www.oaic.gov.au/agencies-and-organisations/app-guidelines/chapter-13-app-13-correction-of-personal-information>.

17.3. MADIP – Overview

The ABS already has policies and procedures in place for complaints and the correction of inaccurate data. However, these policies and procedures are designed for data that is collected and held by ABS. MADIP will require an expansion of complaints management and the correction of data to ensure that all Partner Agencies are covered.

All MADIP Partner Agencies provide mechanisms for dealing with corrections and complaints, detailed in their privacy policies. Correction of source data is the responsibility of the relevant custodian.

The following table sets out the key steps that will be required in order to comply with APP 13:

APP 13. Correction	Compliant	Galexia Commentary
A. UPON REQUEST Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information?	**Compliant**	ABS has correction policies and procedures in place that are fully compliant with APP 13 in relation to its own data. For MADIP, Clause 17.2 of the MADIP Agreement sets out a simple 'referral' process for managing any complaints received by MADIP Partner Agencies that require the cooperation of other MADIP participants.
B. UPON LEARNING OF INACCURACIES Does the entity take such steps (if any) as are reasonable in the circumstances to correct that information? (where the inaccuracy relates to a purpose for which the information is held)	**Compliant**	ABS has correction policies and procedures in place that are fully compliant with APP 13 in relation to its own data. For MADIP, Clause 17.2 of the MADIP Agreement sets out a simple 'referral' process for managing any complaints received by MADIP Partner Agencies that require the cooperation of other MADIP participants.
C. UPON REQUEST ONLY Will corrections and annotations be disseminated to third parties to whom personal information has previously been disclosed?	**Compliant** **Further measures possible**	In MADIP requests for disseminating corrections to third parties will need to be honoured by the ABS and all MADIP Partner Agencies. This is essential for compliance with APP 13. In addition, corrections to any data that has been shared should be disseminated to Partner Agencies, even in the absence of a request, for data quality purposes. ABS and MADIP Partner Agencies could go beyond strict compliance with APP 13 and share all data corrections, not just in response to a specific request by the data subject.

17.4. APP 13. Finding

The ABS and MADIP Partner Agencies are compliant with the complaints and corrections requirements of APP 13.

This position will potentially be strengthened by the development statement on Access and Corrections for MADIP. Work on this statement began in early 2018 and it will be made available in the MADIP FAQ. Although not strictly required, MADIP could benefit from a small expansion of complaints management and the correction of data to ensure that all Partner Agencies are covered. Specifically, ABS and MADIP Partner Agencies could go beyond strict compliance with APP 13 and share all data corrections and correction statements.

18. Governance

In MADIP, the ABS and Partner Agencies are subject to more than compliance with the APPs, so a broader governance framework is required.

MADIP needs to comply with a variety of requirements contained in:

- Privacy legislation (the APPs)
- MADIP Partner Agency legislation
- MADIP Public Interest Certificates
- The MADIP Partner Agreement

Additional compliance requirements may come from audit findings and recommendations (in time, these will become more important), and best practice guidance (e.g. developed by the Department of Prime Minister and Cabinet).

It is also important to continually address issues that may arise from public expectations or perception issues that are associated with such a large, high profile, high risk project.

It makes sense for MADIP to address all of these compliance requirements in a single framework, and there is an initial agreement in place between the parties – the MADIP Agreement.

ABS / MADIP Partner Agencies continue to strengthen and enhance their compliance and governance arrangements for MADIP. For example, MADIP Partner Agencies have recently agreed to establish a new MADIP Oversight Committee and Working Group.

The following table summarises (briefly) several requirements that could be included in the MADIP governance arrangements. Note that this table only addresses issues to be covered relevant to privacy and security. Other headings are not covered in this PIA. Some governance arrangements are already in place or under development, as noted in the table.

Governance Issue	MADIP Requirement	MADIP Progress	Partner Agency Requirement	Partner Agency Progress
A. Legal basis / Public Interest Certificates	The governance arrangement should identify a clear legal basis, usually in legislation, for each participant's role in collecting and integrating the data. A public register of the legal basis for each MADIP Partner Agency to share data with MADIP should be maintained. A public register of any Public Interest Certificates issued by MADIP Partner Agencies should be maintained.	**Completed, but not published.**	Where data is being collected by a MADIP Partner Agency and then disclosed to the ABS, a legal basis for the disclosure should be identified. Reliance on exceptions rather than a specific authority to disclose data should be minimised.	**Completed, but not published.**

B. Register of agreements	MADIP should maintain and publish a register of all data exchanges that have been agreed with Partner Agencies. The register should include information on the date of the agreement and its expiry (or review), the nature of the data being shared and any conditions imposed on the data sharing arrangement.	**In progress**		
C. Data minimisation	MADIP should include mandatory requirements to minimise the data that is provided by Partner Agencies. This should include as a minimum a specific test for whether sensitive information should be acquired by MADIP.	**In progress**		
D. Limit use to one purpose	MADIP should identify a specific purpose for each data exchange and prohibit the use of the shared data for any additional purposes. (This is already in place in the MADIP Agreement and other MADIP documentation).	**In place**		
E. Data quality assessment	MADIP should conduct a data quality assessment before relying on data that has been shared. (This is already in place in the MADIP Agreement and is being implemented by project evaluations).	**In place**		
F. Minimum security requirements	MADIP should mandate the ongoing conduct of independent security risk assessments at regular intervals. Following the initial assessment, MADIP should establish minimum security requirements based on the recommendations of the assessment. An independent security risk assessment should be conducted for any new data transfers, changes to the core arrangements, or any significant expansion of MADIP.	**In progress**		

G. Compliance audits	MADIP should establish a compliance audit regime that covers ABS's own compliance, complemented by imposing a compliance audit requirement on Partner Agencies. The audits should examine: 1. Compliance with the APPs; 2. Compliance with conditions imposed by ABS or Partner Agencies; 3. Compliance with other secrecy and confidentiality requirements; and 4. Compliance with minimum security standards	**Under discussion**	Partner Agencies should be bound by a compliance audit requirement. This could either be an expansion of existing audit arrangements or a new specific audit regime for data sharing.	**Under discussion**

Recommendation 14. Strengthen and enhance MADIP Governance arrangements

The ABS and MADIP Partner Agencies need to continually review, strengthen and enhance the MADIP governance framework, including:

- **A.** Legal basis / Public Interest Certificates
- **B.** Register of agreements
- **C.** Data minimisation
- **D.** Limits on the use of data
- **E.** Data quality assessment
- **F.** Minimum security requirements
- **G.** Compliance audits

19. Appendix 1 – Acronyms

Acronym	Term
ABS	Australian Bureau of Statistics
APP	Australian Privacy Principle
APS	Australian Public Service
ATO	Australian Taxation Office <www.ato.gov.au>
DHS	Department of Human Services <www.humanservices.gov.au>
IRAP	InfoSec Registered Assessors Program <www.asd.gov.au/infosec/irap.htm>
MADIP	Multi-Agency Data Integration Project
MOU	Memorandum of Understanding
OAIC	Office of the Australian Information Commissioner <www.oaic.gov.au>
PIA	Privacy Impact Assessment

20. Appendix 2 – Stakeholder Consultation

During the development of this PIA Galexia met with the following organisations:

- Australian Bureau of Statistics (ABS)
- Department of Health
- Department of Social Security (DSS)
- Office of the Australian Information Commissioner (OAIC)
- Australian Taxation Office (ATO)
- Prime Minister & Cabinet (PM&C)
- Department of Education and Training (DET)

Additional stakeholder consultation regarding MADIP is being completed by ABS as a separate project.