Maddocks

Australian Bureau of Statistics

Privacy Impact Assessment Update

2025 Person Level Integrated Data Asset – Detailed Justice Data

Date of analysis – 24 September 2025
Date of finalisation – 21 November 2025

Contents

Part A   Executive Summary

1.   Introduction

1.1   The Person Level Integrated Data Asset (**PLIDA**), formerly known as the Multi-Agency Data Integration Project (**MADIP**), is a secure, enduring, person-based research data asset that combines broad sets of information about the Australian population. PLIDA creates a comprehensive picture of Australian residents included in the dataset (**Data Subjects**) over time and facilitates the use and re-use of available data for authorised statistical analysis and research conducted by approved research institutions from government, universities, and public policy institutes (**Researchers**).

1.2   The Australian Bureau of Statistics (**ABS**) is the accredited integrating authority for PLIDA and is responsible for:

1.2.1   combining the datasets in PLIDA;

1.2.2   providing access to PLIDA data to only those individuals who have been authorised to access PLIDA data for approved research projects (**Authorised Users**);

1.2.3   ensuring the security of data contained within PLIDA; and

1.2.4   ensuring that all research results and other outputs from the use of PLIDA data are produced in a manner that means there is no reasonable likelihood of the reidentification of Data Subjects occurring.

1.3   The ABS and other entities (**Data Custodians**) contribute data to, and have a responsibility for data within, PLIDA.

1.4   PLIDA has evolved over time, and the ABS has undertaken several major privacy impact assessments (**PIAs**) in relation to PLIDA as it has developed.[1] There have also been specific PIA processes conducted in relation to particular matters or issues connected to PLIDA, that have considered actual or planned changes or updates to PLIDA as they arise.[2]

1.5   The ABS has observed increasing interest from Data Custodians and Researchers in linking data that relates to the interactions of Data Subjects with crime and/or the police or justice systems in Australia. Such data would include:

1.5.1   data in records from police, courts, corrections facilities, and/or justice departments, about a Data Subject's interactions with those entities in relation to suspected or actual criminal conduct. For example, this may include information about a Data Subject's police charges, criminal court appearances and sentencing, or detention or non-custodial sentences. It may also include other information about a Data Subject, potentially including information about their racial or ethnic origin, or health or disability; and

---

[1] Previous PIAs completed in relation to PLIDA can be found at: https://www.abs.gov.au/about/legislation-and-policy/privacy/privacy-impact-assessments.

[2] For example, a PIA process was conducted in November 2020 for the linkage of data from the Cancer Institute of NSW, and a PIA process in relation to the linkage of health data to PLIDA was conducted in 2024. Copies of the relevant PIAs are also available at: https://www.abs.gov.au/about/legislation-and-policy/privacy/privacy-impact-assessments.

1.5.2   any data from other entities referencing a Data Subject's interactions with police, courts, corrections facilities, and/or justice departments in relation to suspected or actual criminal conduct. For example, this may include information about a Data Subject's participation in an employment or housing program that indicates that the Data Subject has a criminal conviction or interactions with domestic violence or drug offences in their background (this could include data that is 'self-reported' to the entity). Again, this could include other information about a Data Subject, potentially including information about their racial or ethnic origin, or health or disability.

(referred to in this PIA as **Detailed Justice Data**).

1.6   Detailed Justice Data included in PLIDA could be used for the development of research, evaluation and statistics that may inform, for example:

1.6.1   policy development in areas such as public safety and criminal justice; and

1.6.2   understanding of risk factors, social and economic influences, and general trends in those areas.

1.7   Detailed Justice Data has previously been included in PLIDA and used by Researchers in discrete limited examples for approved research projects, but such data has not yet been included as a specific enduring dataset in PLIDA (that would then be available for reuse in any approved research project). To date, the potential privacy impacts associated with specific projects that have involved linking Detailed Justice Data to PLIDA have been assessed on a case-by-case basis (for example, through the ABS conducting an internal PIA or privacy threshold assessment (**PTA**) process).

1.8   The ABS wishes to explore the privacy risks, issues and impacts associated with the inclusion of Detailed Justice Data in PLIDA more broadly, with a view to providing assurance to Data Custodians, Researchers and their Authorised Users, and the general public, that these matters have been properly considered.

1.9   As such, the ABS has engaged Maddocks to conduct a further PIA (**PIA Update**) process to build on previous PIAs in relation to PLIDA, and to comprehensively consider the privacy impacts of including and linking Detailed Justice Data within PLIDA, and any additional risk mitigation strategies that could be put into place.

2.   This PIA Process

2.1   Undertaking a PIA is consistent with the requirements of the Privacy (Australian Government Agencies – Governance) APP Code 2017 (**APP Code**), which has applied since 1 July 2018. The APP Code requires agencies to undertake a written PIA for all 'high privacy risk' projects or initiatives that involve new or changed ways of handling personal information, but undertaking a PIA for other projects which have not been assessed as representing 'high privacy risk' is also consistent with privacy best practice.

2.2   The *Guide to undertaking privacy impact assessments* issued by the Office of the Australian Information Commissioner (**OAIC**), further explains that PIAs should be revisited and updated, or a new PIA should be conducted, when changes to a particular project are considered which may impact how personal information is handled.

2.3   As such, this PIA Update is being conducted as part of the ABS' continued commitment to its 'privacy by design' approach to PLIDA to:

2.3.1   consider PLIDA's continued compliance with the *Privacy Act 1998* (Cth) (**Privacy Act**), including the Australian Privacy Principles (**APPs**), and privacy best practice, in relation to the inclusion of Detailed Justice Data in PLIDA;

2.3.2   support development of best practice strategies for inclusion, and subsequent access and use, of Detailed Justice Data in PLIDA;

2.3.3   help the ABS, and the governance board established for the operations and strategic direction of PLIDA (**PLIDA Board**), to manage any new or increased privacy risks and impacts identified in relation to Detailed Justice Data and to improve efficiency and consistency for approaches to future proposed linkages of Detailed Justice Data; and

2.3.4   provide assurance to the ABS and other stakeholders that the privacy elements of the future management of Detailed Justice Data as part of PLIDA have been robustly considered.

3.   Structure of this PIA Update Report

3.1   This PIA Update report consists of:

3.1.1   a summary of our findings and recommendations to address identified privacy risks (**Part A [Executive Summary]**);

3.1.2   our methodology and further information about the scope of our work (**Part B [Methodology and Assumptions]**);

3.1.3   a description of the background context to PLIDA and Detailed Justice Data (**Part C [Project Description and Information Flows]**);

3.1.4   a discussion of specific privacy impacts, risks and issues associated with the incorporation of Detailed Justice Data in PLIDA (**Part D [Detailed Privacy Analysis]**);

3.1.5   a table containing our overall compliance risk ratings against each APP in relation to all of the topics covered by this PIA Update report (**Part E [Summary of Privacy Compliance]**); and

3.1.6   a glossary of defined terms (**Part F [Glossary]**).

4. Summary of Findings

4.1 We commend the ABS for commissioning this PIA Update, which is a measure consistent with the APP Code and privacy best practice, and further demonstrates ABS' commitment to implementing a 'privacy by design' approach to PLIDA.

4.2 The data within a Detailed Justice Data set would, if the relevant Data Subjects were identified, include personal information that is also 'sensitive information' as defined in the Privacy Act (being information about an individual's criminal record, and also potentially information about their racial or ethnic origin). It may also include data that does not meet the definition of sensitive information but would still have a high level of inherent sensitivity for the individuals to which it relates. If a Data Subject were to be identified, any inappropriate disclosure or use of Detailed Justice Data may cause them harm in the form of discrimination or mistreatment, or psychological harms including feelings of humiliation or embarrassment.

4.3 Data Subjects from Aboriginal and/or Torres Strait Islander communities, or those with mental health challenges, are likely to be overrepresented in Detailed Justice Data sets. As highlighted by stakeholders who were consulted for this PIA Update, it will be important to ensure that governance arrangements for the handling of such data considers the particular perspectives of those Data Subjects. For example, the Framework for Governance of Indigenous Data (which was co-designed by Australian Public Service agencies and Aboriginal and Torres Strait Islander partners) (**GID**) touches on the importance of Indigenous Data Sovereignty for Aboriginal and/or Torres Strait Islander people, as a critical consideration for the handling of Indigenous data.

4.4 In addition, the nature of Detailed Justice Data means that it needs to be carefully analysed and interpreted by Researchers, to avoid incorrect findings, or biased and damaging research narratives, being made about a particular demographic cohort - even though individual Data Subjects will not be identified, research findings could still have the potential to cause harm to individuals who are known to be a member of a particular population, group or community, including through incorrect assumptions being made about their characteristics as a result of the analysis.

4.5 Overall, we consider that the existing PLIDA governance and other processes and procedures, including those that have been recently implemented or are in the process of being implemented as a result of other PIA processes in relation to PLIDA, will be appropriate to address or mitigate the identified privacy risks. In particular:

4.5.1 the recently developed guidelines which will be followed whenever new datasets are being considered for addition to PLIDA,[3] which will be applied to any addition of new Detailed Justice Data sets, will provide a solid foundation to address the risks associated with increasing the size and contents of PLIDA generally (these guidelines will ensure that new Detailed Justice Data sets are only added to PLIDA after proper consideration of the public benefit, utility, sensitivities or restrictions, and data safety issues associated with doing so);[4]

4.5.2 the existing technical and non-technical processes and arrangements used by the ABS for receiving and linking new datasets to PLIDA (in preparation for them being available for use in approved research projects) will also support appropriate handling of this type of data, particularly:

---

[3] See the ABS *PLIDA Data and Legislation* webpage for discussion of considerations that inform the integration of new types of data in PLIDA, available at: https://www.abs.gov.au/about/data-services/data-integration/integrated-data/person-level-integrated-data-asset-plida/plida-data-and-legislation

[4] As discussed in *Recommendation 2: Criteria for including datasets in MADIP* from the *ABS 2022 MADIP PIA Update – Privacy Impact Assessment* (Update to 2019 Privacy Impact Assessment), dated 25 May 2025, available at: https://www.abs.gov.au/about/legislation-and-policy/privacy/privacy-impact-assessments

(a)   implementation of the 'Separation Principle', so that direct identifiers of Data Subjects will be processed separately to analytical data within the Detailed Justice Data set, and will not be included in analytical information that may be accessed by Authorised Users from Researchers for approved projects; and

(b)   the existing security measures, such as restricting access to data to only approved individuals in secure environments, performing regular security reviews, and logging and monitoring all access to PLIDA data, are reasonable steps to ensure that Detailed Justice Data in PLIDA is appropriately protected;[5] and

4.5.3   the existing processes and arrangements for allowing access to analytical data within PLIDA for approved research projects are also likely to be appropriate for this type of data, particularly:

(a)   the current arrangements designed to implement the Five Safes Framework will provide a good basis for the approval of research projects that seek to access Detailed Justice Data; and

(b)   the current arrangements for Authorised Users from Researchers to gain access to PLIDA data to undertake approved projects (via the DataLab, after receiving appropriate training, and with oversight by the ABS) are also likely to be appropriate to protect this type of data.

4.6   However, we consider that the particular nature of Detailed Justice Data raises some additional privacy risks, for which we believe the PLIDA Board should take additional measures as described in the recommendations set out in paragraph 5.1, to build upon the strong foundation of existing PLIDA arrangements and ensure PLIDA continues to meet best practice expectations of the Australian community.

5.   Recommendations

5.1   This PIA makes the following recommendations in relation to the implementation of the Project. Each of these recommendations reflect strategies that are designed to facilitate implementation of best privacy practice, rather than recommendations designed to mitigate a risk of non-compliance with the Privacy Act.

Recommendation 1	Data ethics consideration for projects analysing Detailed Justice Data *(Best practice recommendation)*	Relevant APPs
Rationale Stakeholders reflected that a key concern was proper consideration of ethical issues associated with research using Detailed Justice Data. Such ethical issues might arise from • the inherent sensitivity of Detailed Justice Data, and how it may be amplified due to the over representation of certain populations;		**All APPs**

---

[5] These measures have been considered in detail in previous PIA processes (see https://www.abs.gov.au/about/legislation-and-policy/privacy/privacy-impact-assessments).

Recommendation 1	Data ethics consideration for projects analysing Detailed Justice Data *(Best practice recommendation)*	Relevant APPs

- the possibility for unintended biases and damaging research narratives to be perpetuated due to the inappropriate handling of Detailed Justice Data; and/or

- the importance of research design involving engagement with individuals that are from cohorts likely to be affected by the research.

These issues mean that it will be critical for ethical issues to be properly considered before proposed PLIDA research projects using Detailed Justice Data are approved.

Consideration of ethical issues is already built in to current PLIDA project approval processes, but some stakeholders expressed concerns that the relevant Data Custodians (who are responsible for approving proposed projects seeking to access Detailed Justice Data) may not be appropriately placed or supported to make key determinations in relation to specific ethical issues associated with Detailed Justice Data

This raises the following risk:

Privacy Risk 1: The risk that specific ethical issues associated with the use of Detailed Justice Data may not be appropriately considered by Data Custodians as part of PLIDA project approval processes.

The ABS has been strengthening consideration of data ethics by developing a framework that can be used to consider PLIDA projects (**Data Ethics Framework**). We congratulate the ABS on its work in undertaking the development of this framework to date but consider that it could be further tailored to facilitate its application to projects involving Detailed Justice Data in PLIDA. Although it may not be necessary to complete a data ethics assessment for every proposed project that seeks to access Detailed Justice Data, we consider that it is appropriate that this be at least *considered* by Researchers and Data Custodians for every such project, and for conclusions about its use to be properly documented.

Recommendation 1.1:

We **recommend** the ABS consider further developing the draft Data Ethics Framework (including a draft ABS Data Ethics Assessment Tool) so that it specifically applies to proposed research projects involving the use of Detailed Justice Data in PLIDA. For example, this could be achieved by:

- better referencing Detailed Justice Data as a particular category of data for which the Data Ethics Framework should (or at least, can) be applied, noting that the draft does already refer in some places to 'crime' and 'justice' data;

- reflecting the existing or planned ABS processes for involvement of cultural consideration by the ABS Centre of Aboriginal and Torres Strait Islander Statistics (**CoATSIS**), which can also involve ethical considerations, as one appropriate assurance measure for consideration of projects involving use of Detailed Justice Data; and/or

Recommendation 1	Data ethics consideration for projects analysing Detailed Justice Data *(Best practice recommendation)*	Relevant APPs
• potentially giving examples of how ethical consideration of the use of Detailed Justice Data might be strengthened (e.g. ways to mitigate potential unintended biases, the value of engaging affected communities meaningfully in research design, and / or ways the principles outlined in the GID may be applied to research projects involving Aboriginal and/or Torres Strait Islander Data Subjects). **Recommendation 1.2:** After the draft Data Ethics Framework is finalised, we **recommend** that the ABS update its documentation for PLIDA processes to reference how this should be used as part of PLIDA project approval processes. For example, this could involve: • making changes to published information, to direct potential Researchers to consider the Data Ethics Framework as part of their project proposal (and also to advise Data Custodians about its potential for use as part of the approval process); and • potentially, updating template PLIDA project proposal forms (e.g. to either require Researchers to provide a draft ABS Data Ethics Assessment Tool, or explain why this is not needed for the relevant project).	

Recommendation 2	Accompanying information for datasets *(Best practice recommendation)*	Relevant APPs
Rationale Stakeholders reflected the concern that some Detailed Justice Data which may be linked to PLIDA on an enduring basis may have inherent quality issues and other limitations. They stressed that it will be very important for Researchers to be made aware of such issues when selecting and analysing such data for research projects. For example, Detailed Justice Data might have been initially recorded at a very high level and/or in a way that does not reflect important considerations for research looking at issues on a local or regional scale, or it may have been recorded through a self-reporting process with its inherent potential for inaccuracies. If Researchers are not properly informed about any limitations or quality issues associated with Detailed Justice Data in PLIDA, this will raise the following privacy risk: **Privacy Risk 2:** The risk of inherent data quality issues, which may lead to inappropriate research conclusions with the potential for privacy and other harms to be caused to individuals, communities and populations (even if Data Subjects themselves are not identified). Providing further opportunities for Data Custodians to record details relevant to the quality of Detailed Justice Data in PLIDA, and for Authorised Users from Researchers to have access to such details prior to making a project proposal, is likely to be beneficial in further ensuring that only suitable research projects are approved, and that research outputs from Detailed Justice Data do not adversely impact on the privacy of individuals.	**APP 10**

Recommendation 2	Accompanying information for datasets *(Best practice recommendation)*	Relevant APPs
Recommendation 2: We **recommend** the ABS consider mechanisms that would allow Authorised Users from potential Researchers (for whom a Detailed Justice Data set in PLIDA is discoverable)[6] to have access to information about any quality and utility issues in respect of that data, such as any limitations inherent in the scale of the data or the processes used to collect it. For example, Data Custodians could be asked to provide this information about their Detailed Justice Data at the point of its inclusion in PLIDA (or, for any such data sets already linked to PLIDA, as part of making them discoverable)[7], and for this information to be then clearly displayed to Authorised Users from potential Researchers discovering that data set.	

Recommendation 3	Guidance for Data Custodians *(Best practice recommendation)*	Relevant APPs
Rationale Stakeholders identified that research involving use of Detailed Justice Data may pose a heightened reidentification risk, particularly if the data shows unique journeys through a particular criminal justice system, or characteristics of Data Subjects in small populations (e.g. it may show particular mental or other health conditions that affect only a small number of individuals in Australia; or relate to Data Subjects in remote areas with small populations). Any reidentification of Data Subjects would involve the potential for unauthorised use and disclosure of their personal information, with associated privacy, and other, consequences. While PLIDA already has important existing mitigation strategies in place to address reidentification risks, it is important to recognise that Data Custodians also play an essential role in addressing this and other risks through the project approval process. Some stakeholders reflected that in the context of Detailed Justice Data, there may be additional support and tailored guidance that could be provided to Data Custodians, particularly for entities that are new to the Data Custodian role, to ensure that they can appropriately perform their role in relation to PLIDA. This raises the following privacy risk: **Privacy Risk 3:** Data Custodians may not be appropriately supported to consider the particular sensitivities and reidentification risks associated with proposed projects involving use of Detailed Justice Data.	

---

[6] This refers to a potential Researcher having access to information *about* the data set, rather than having access to information *within* the data set.

[7] We understand that the ABS is currently undertaking a process to consider the datasets currently within PLIDA, with a view to making them discoverable unless there are important reasons for not doing so.

Recommendation 3	Guidance for Data Custodians *(Best practice recommendation)*	Relevant APPs

Recommendation 3:
 	
We **recommend** the ABS consider whether there are further ways in which Data Custodians that are required to consider a proposed project proposal involving the use of Detailed Justice Data, can be provided with additional guidance and support.
 	
For example:
 	
• the ABS could consider incorporating within the project proposal documents requirements for the proposed Researcher to demonstrate how the project will address (and remove or appropriately mitigate) any additional reidentification risks associated with the use of the particular Detailed Justice Data for that project (e.g. by addressing this in a data linkage plan within the proposal); and/or
 	
• the ABS could consider developing a general guidance document for Data Custodians about Detailed Justice Data which:
 	
    o explains in detail the potential reidentification and other risks that might be associated with a project using Detailed Justice Data;
 	
    o provides general information about the treatments that can or should be considered for such projects to reduce these risks; and
 	
    o provides guidance about how to seek additional advice about a potential reidentification risk for a proposed project (e.g. when and how to conduct a Safe Data Risk Assessment or escalate matters to the ABS Disclosure Review Committee).	

5.2   We understand that the ABS will separately document its responses to the above recommendations.

Part B   Methodology and Assumptions

6.   Our Methodology

6.1   This PIA has been conducted in accordance with the *Guide to undertaking privacy impact assessments* issued by the OAIC, using the methodology in the table below.

6.2   A glossary of defined terms and acronyms is at **Part F [Glossary]** of this PIA report.

Stage	Description of steps
1.	**Plan for the PIA:** We reviewed relevant background material provided by the ABS (listed in **Attachment 2 [Material Reviewed]**), and were provided with a briefing by officers from the ABS. Due to timing constraints, we needed to use an adapted methodology. This involved us planning the steps and timing for conducting the PIA with the ABS in accordance with the steps outlined below.
2.	**Project Description**: We prepared an initial draft Project Description, which described our understanding of the Project. This draft was refined and further finalised following feedback from the ABS.
3.	**Stakeholder consultation:** We assisted the ABS in conducting a formal stakeholder engagement process in relation to the consideration of Detailed Justice Data. The consultation was considered an essential part of this PIA Update process and provided an opportunity for stakeholders to be informed about the matters under consideration, and for us to receive critical feedback and input from stakeholders. We assisted the ABS to prepare and plan the stakeholder consultation workshops, including by providing advice about the scope and nature of stakeholders that should be consulted, and providing input to material to be used during the consultation. Our Project Description from the previous step was provided to stakeholders prior to the consultation workshops as background material to inform the discussions. Stakeholder consultation workshops for this PIA Update involved participation by 22 organisations from a range of entity types (the entities that participated are listed in **Attachment 2 [Material Reviewed]**). We attended the consultation workshops to provide input as required, and to listen to the issues and perspectives discussed during the workshops, to inform and be incorporated into our analysis. We were also provided with additional written feedback provided by some stakeholders, and the ABS' answers to some questions from stakeholders which were taken on notice during the consultations. In addition to the valuable insights gained through the stakeholder consultation process, throughout the PIA Update process we further drew from our knowledge of Australian community expectations gained from our research and related work, to inform our analysis and identification of privacy risks. For example, we considered the *Australian Community Attitudes to Privacy Survey 2023* commissioned by the OAIC, which contains useful information in relation to current community expectations about the handling of personal information.

Stage	Description of steps
4.	**Privacy impact analysis and compliance check**: In this step we focussed on compliance against each relevant APP and privacy best practice. In undertaking our analysis, we considered and applied the *Australian Privacy Principles Guidelines* (**APP Guidelines**) issued by the OAIC, which outline the mandatory requirements of the APPs, how the OAIC will interpret the APPs, and matters that may be taken into account when assessing the ABS's compliance with the Privacy Act. Our analysis of the key privacy issues identified from the PIA is contained at **Part D [Detailed Privacy Analysis]**. For each APP, we allocated a compliance rating that reflects our assessment based on the following descriptors:

Compliance Rating	Description of Compliance Rating
Significant Risk	This rating indicates that we consider that extensive work is required before the ABS will be able to be fully satisfied about compliance with the relevant APP and best privacy practice.
Compliance Risk	This rating indicates that we have identified issues which we consider should be addressed in order to further enhance the privacy protections for individuals.
Improvements to meet best practice	This rating indicates that we have identified measures that can be taken by the ABS to meet privacy best practices.
Compliant	This rating indicates that the APP is either not relevant in the circumstances or that we have concluded that no further mitigation steps are required.

Stage	Description of steps
	A summary of overall application of compliance risk ratings against the APPs for all PIA topics is set out in **Part E [Summary of Privacy Compliance]**.
5.	**Privacy management and addressing risks:** We considered potential mitigation strategies that could reduce or remove the privacy impacts and risks identified during the previous step, and developed our recommendations.
6.	**Draft report:** We prepared a draft version of this PIA report. The draft PIA report was provided to the ABS for review and further circulation as necessary.
7.	**Further refinement of draft PIA report**: Following review of the draft report by the ABS, we further refined our analysis and potential mitigation strategies as required to ensure that privacy risks were appropriately considered and addressed.
8.	**Final report**: We finalised this PIA report. We understand that the PLIDA Board will review this PIA Update report and separately respond to our recommendations.

7.   Assumptions and Qualifications

7.1   The scope of this PIA Update report is limited to consideration of the inclusion of Detailed Justice Data sets as enduring data sets within PLIDA, and their potential for subsequent use for approved research projects. Our consideration is intended to build upon, but not reconsider, matters that were the subject of any previous and / or separate PTA or PIA processes for PLIDA. Rather, this PIA Update process is intended to identify and consider any new or changed privacy risks associated with the matters within its scope.

7.2   We have completed our analysis on the basis that the information provided by the ABS is up to date, correct, and complete. Although **Part C [Project Description and Information Flows]** includes some examples of how Detailed Justice Data has been previously handled within PLIDA, this is for illustrative purposes only, and we have not directly examined the information flows associated with, or expressed a view as to the privacy implications of, those specific examples.

7.3   This PIA also does not consider:

7.3.1   the handling of any data as part of the Criminal Justice Data Asset, which is part of the National Crime and Justice Data Linkage Project and is separately managed by the ABS (and in respect of which a separate PIA process was undertaken); and

7.3.2   data specifically relating to victims or survivors of criminal conduct.

7.4   Our PIA has been undertaken from the perspective of the ABS and its support for the PLIDA Board, but not any other particular entity.

7.5   Our analysis is based upon the provisions of the Privacy Act, and associated case law and guidance material, as in force at the date of analysis on the cover page of this PIA report. This includes the commenced reforms introduced by the *Privacy and Other Legislation Amendment Act 2024* (Cth) (**POLA Act**). While we have endeavoured to take into account proposed reforms that were not introduced by the POLA Act,[8] we suggest the ABS to seek further advice about the privacy implications of those reforms should they be implemented.

---

[8] For example, those further reforms discussed in the *Privacy Act Review Report* release by the Attorney-General's Department (https://www.ag.gov.au/rights-and-protections/publications/privacy-act-review-report) and the Australian Government's response to the *Privacy Act Review Report* (https://www.ag.gov.au/rights-and-protections/publications/government-response-privacy-act-review-report#:~:text=In%20its%20response%20to%20the,to%20best%20protect%20this%20information).

Part C   Project Description and Information Flows

8.   PLIDA Governance

8.1   Previous PIAs have recorded that PLIDA was established through a cross-portfolio government partnership of Commonwealth agencies, including the ABS (which is the accredited integrating authority for PLIDA), the Australian Taxation Office, Department of Education, Department of Health and Aged Care, Department of Social Services, Services Australia and Department of Home Affairs.

8.2   PLIDA is bound by the constraints of:

    8.2.1   the legislation of the Data Custodians that applies to data that they provide to PLIDA;

    8.2.2   the *Census and Statistics Act 1905* (Cth);

    8.2.3   the Privacy Act; and

    8.2.4   social licence from, and the community expectations of, Australians.

8.3   The analytical data in PLIDA is used by Authorised Users for approved research projects in a secure, virtual access environment. PLIDA presents benefits to Australian agencies, the Australian public, researchers, and Data Custodians by:

    8.3.1   providing Australian governments with a powerful tool for informing government decision-making;

    8.3.2   supporting decisions that will help Australians live healthier, happier, and more independent lives;

    8.3.3   making better use of the information that has already been collected to enhance the value of existing public data resources; and

    8.3.4   making a wider range of data available for Researchers.

9.   PLIDA Data

9.1   PLIDA contains high-value, person-centred, and regularly updated, data which are organised separately into 'linkage' data and 'analytical' data (which does not contain any direct-identifiers for Data Subjects).

9.2   The ABS has built a central linkage infrastructure called the 'Person Linkage Spine' (**Spine**) which represents Data Subjects. PLIDA is built by linking the linkage data supplied by Data Custodians to the Spine, instead of linking the analytical data to every other analytical dataset individually. This creates the capacity for separate source datasets to be linked to one another via the Spine, in a flexible and efficient manner. Through the Spine, the analytical datasets can be combined as required and extracts of the linked analytical data can then be used by Authorised Users from Researchers for approved research projects. The Spine enables information to be brought together in relation to Data Subjects who were resident in Australia during a given reference period from 2006 to present. A diagram illustrating the overarching data flows for PLIDA in its current state is included in **Attachment 1 [PLIDA Information Flow Diagram – Current Data Handling Practices]**.

9.3   The ABS is responsible for ensuring that PLIDA analytical data it makes available to Authorised Users is provided in a manner that is not likely to enable the identification of an individual (and therefore meets the requirements to be 'deidentified' under the Privacy Act).[9]

9.4   Previous PIAs have noted the range of security arrangements in place for the IT systems that are used for PLIDA, which protect PLIDA data. In particular, they have recorded that these:

9.4.1   conform with security arrangements set out in the Australian Government Information Security Manual;

9.4.2   ensure that data collection, linkage, and assembly activities for PLIDA datasets are only conducted by an authorised team in the Secure Data Integration Environment;

9.4.3   ensure that access to data by Authorised Users outside the ABS is conducted only by giving access to analytical data within an ABS environment (known as the DataLab);[10]

9.4.4   includes a secured internet gateway which is reviewed annually by the Australian Signals Directorate; and

9.4.5   includes an ongoing program of security audits and system accreditations, including the Information Security Registered Assessors Program.

9.5   Further, PLIDA datasets are handled in accordance with a range of additional privacy protection practices, including:

9.5.1   the Five Safes Framework, which is an internationally recognised approach to managing disclosure risks, which is applied to ensure access to PLIDA data is appropriate. The framework is designed to facilitate safe data release using five elements (Safe People, Safe Projects, Safe Settings, Safe Data and Safe Outputs) which are all assessed independently, but also considered as a whole for each instance of data access;

9.5.2   an ability for data to be added to PLIDA via a once-off linkage (for a specific research project or projects and will not be retained following the completion of the project(s)), or as a part of an enduring analytical asset that is separate to PLIDA; and

9.5.3   transparency about linkages with PLIDA and approved research projects that make use of PLIDA analytical data, through information included on the ABS website.

---

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

[10] A limited number of PLIDA activities can occur on other ABS-controlled infrastructure known as SEADpods (see 2019 PIA Update).

10. Previous Examples of Linking Detailed Justice Data to PLIDA

10.1   Detailed Justice Data that may be included or used through PLIDA encompasses a broad spectrum of data that can range significantly in its level of detail. It could include:

10.1.1   a 'flag' (high level data point indicating a binary outcome, e.g., yes / no, which might indicate, for example, that a Data Subject has a history of violence) – handling such 'high level' Detailed Justice Data was considered as part of the 2024-25 PIA Update; or

10.1.2   it could include more complete records about offences or convictions from institutions like criminal courts or corrective services - as mentioned above, more complete data sets containing Detailed Justice Data have been considered on a case-by-case basis on a small number of occasions, so that the relevant data could then be used for approved research projects,

10.2   Examples of projects involving the linkage of more complete Detailed Justice Data include:

10.2.1   the Better Evidence, Better Outcomes, Linked Data (**BEBOLD**) linkage to PLIDA; and

10.2.2   the Human Services Data Set (**HSDS**) developed for the Their Futures Matter (**TFM**) project.

10.3   Each of these is considered below, to illustrate some of the issues that have previously been considered about the handling of Detailed Justice Data within the PLIDA governance framework, and how those issues have been managed.

BEBOLD

10.4   The BetterStart Group at the University of Adelaide established BEBOLD by integrating a diverse range of South Australian government administrative datasets, along with datasets from not-for-profit organisations. These datasets were provided under formal agreements with data custodians and approved by multiple research ethics committees. BEBOLD was developed to support evidence-informed policy and practice aimed at improving health, wellbeing, and development outcomes.

10.5   We understand that the linkage of BEBOLD to PLIDA is governed by a formal agreement between the University of Adelaide's BetterStart Group and the ABS. This agreement includes approval from each of the entities contributing data for BEBOLD, as well as the relevant ethics committees. Some of the contributing entities included the South Australia Attorney-General's Department, Department of Child Protection, Department for Correctional Services, Department for Education, and Housing Authority.

10.6   BEBOLD contains data about approximately 32 birth cohorts from 1991 (each cohort representing around 20,000 people) and their interactions with various services in South Australia over time, such as housing, education, and crime and justice systems.

10.7   As well as including Detailed Justice Data, the BEBOLD dataset also included other information such as information about birth defects and homelessness status.[11] Data about family units was linked within the dataset so that intergenerational contact with particular systems could be examined.

---

[11] No identifying information about data subjects was included in the BEBOLD dataset.

10.8   The BEBOLD dataset was proposed to be linked with PLIDA to facilitate analyses by South Australia and BetterStart examining topics like the outcomes of investments in supportive programs. Components of BEBOLD (housing, homelessness, health, education, and wellbeing data) were also proposed to be linked with PLIDA for the purposes of the Life Course Data Initiative (**LCDI**) to facilitate analyses examining children's wellbeing and outcomes. The privacy impacts of the LCDI were generally considered in the 2024-25 PLIDA PIA Update.[12]

10.9   To assess the privacy implications of the linking of the BEBOLD dataset with PLIDA, the ABS conducted an internal privacy assessment, which considered issues including:

   10.9.1   transparency and the public benefit of the linking;

   10.9.2   the collection of the combined dataset by the ABS (including application of the State privacy law and processes, and ethical approvals for the initiative);

   10.9.3   access to and use of the combined dataset once included in PLIDA, including the risks of re-identification as a result of unique data elements (such as certain medical information); and

   10.9.4   the retention of the combined dataset.

10.10   The privacy assessment made several recommendations, including to:

   10.10.1   improve transparency about the linkage;

   10.10.2   ensure that ethics approvals would be in place for human research projects;

   10.10.3   recommend further data assessments be conducted to provide reassurance about the potential reidentification risk; and

   10.10.4   restrict access to particular analytical data.[13]

10.11   The privacy assessment also recommended that the privacy impacts of including detailed justice data be further considered in this PIA Update process.

TFM HSDS

10.12   The TFM project was a program within the New South Wales government aimed at improving outcomes for vulnerable children, young people and families. The project was developed in response to a 2015 independent review of the out of home care system in NSW and aimed to use data and evidence to improve support offered to vulnerable cohorts.

---

[12] Available at https://www.abs.gov.au/about/data-services/data-integration/integrated-data/person-level-integrated-data-asset-plida/plidamadip-privacy-impact-assessments. However, this PIA Update process did not consider the BEBOLD (or TFM HDSD linkage projects in any detail).

[13] We note that the ABS has more recently introduced arrangements for Data Custodians to nominate 'standard release' for data they contribute to PLIDA (which means that information about that data being in PLIDA is available to all Researchers, but Data Custodian approval is still required for access to be given to that data); and 'limited release' (which means that information about the data is only available to specific Researchers approved for a particular PLIDA project).

10.13   The HSDS was developed as part of the TFM project. It includes integrated data drawn from more than 60 datasets held by NSW government agencies over time, and includes data on, among other things, child protection, housing, justice, and alcohol and drug treatment. The data includes details such as individuals' names and addresses (i.e. it contains identified personal information).

10.14   The HSDS was integrated with PLIDA (or MADIP, as it was known at the time) as part of a research project to link a subset of the HSDS to other Commonwealth data in MADIP, with the aim of producing findings to inform priority setting and resource allocation across government, in order to improve the long-term outcomes for vulnerable children, young people and their families. The integration was done in accordance with standard PLIDA processes, including the removal of personal information which might identify an individual.

10.15   The ABS conducted a PIA to assess the privacy implications of integrating the HSDS with MADIP. It identified issues in relation to:

10.15.1   the involvement of vulnerable populations;

10.15.2   the sensitive information included in the data (including, in addition to Detailed Justice Data, information about racial or ethnic origin, and health information);

10.15.3   the use of legal authorities other than the consent of the Data Subjects; and

10.15.4   re-identification risks.

10.16   The PIA concluded that the existing MADIP (now PLIDA) governance framework would be sufficient to mitigate the identified risks.

Other non-PLIDA PIAs

10.17   The ABS has also undertaken several PIAs in relation to other integration projects involving Detailed Justice Data, outside of the PLIDA framework, which contain some useful analysis of the privacy risks associated with the handling of Detailed Justice Data:

10.17.1   the ACT Justice and Community Safety PIA considered linkage of administrative data from three ACT justice sectors (police, criminal courts and corrective services), to help inform evaluation of the ACT's 'Reducing Recidivism by 25% by 2025 Plan'; and

10.17.2   the National Criminal Justice Data Linkage Project PIA, which considered linkage of data sets provided by State and Territory police, criminal courts, and corrective service agencies across Australia, to form a longitudinal and enduring nationally linked Criminal Justice Data Asset (**CJDA**). The CJDA is intended to address issues around insufficient data that were raised in the Council of Australian Governments' *Prison to Work Report* (2016), to improve outcomes for prisoners and ex-prisoners.

Part D   Detailed Privacy Analysis

11.   Introduction

11.1   In this **Part D [Detailed Privacy Analysis]**, we examine:

11.1.1   some overarching issues and concerns identified in connection with the inclusion and use of Detailed Justice Data set within PLIDA; and

11.1.2   more specific potential privacy risks and impacts associated with:

(a)   including Detailed Justice Data in PLIDA, in particular on an enduring basis; and

(b)   using Detailed Justice Data within PLIDA for specific research projects.

11.2   Although we have considered the application of all APPs in relation to this topic, we have only included discussion about the APPs as relevant to particular issues or important considerations that we have identified.

12.   Overarching Considerations for Detailed Justice Data

Inherent sensitivities associated with Detailed Justice Data

12.1   There is an inherent high level of sensitivity associated with Detailed Justice Data due to the fact that the inappropriate handling of it may, if Data Subjects were to be identified, have significant adverse consequences for those individuals, or people associated with those individuals (including their families or broader community). For example, an individual who is known to have an interaction with the criminal or justice system may face discrimination or mistreatment, or be the subject of humiliation or embarrassment, if information about that association were to be inappropriately accessed and/or disclosed in an unauthorised manner.

12.2   The Privacy Act recognises the particular sensitivity of information about an individual's criminal record by categorising it as 'sensitive information', which is a subset of personal information that is afforded more stringent privacy protections under the Privacy Act.

12.3   We further observe that Detailed Justice Data may face overlapping sources of sensitivity due to the over representation of certain populations within the criminal justice system. For example, individuals facing repeated interactions with the criminal justice system may also be more likely to be experiencing complex mental health issues or homelessness, or to have been the victims of criminal conduct themselves.

12.4   In particular, the over representation of Aboriginal and / or Torres Strait Islander peoples in criminal justice systems across Australia is relevant to the sensitivity of Detailed Justice Data.[14] We observe that some research projects involving Detailed Justice Data may have greater impacts for Aboriginal and / or Torres Strait Islander communities, due to this over representation. Information about an individual's racial or ethnic origin is also another category of information that is recognised as 'sensitive information' under the Privacy Act and afforded a higher level of privacy protection.

12.5   Many of the stakeholders engaged in the consultation process also reflected their concerns around the particular sensitivity associated with the nature of Detailed Justice Data. In particular, they noted risks around unintended biases affecting research using such data, and the potential for biased and damaging narratives to be perpetuated if the data was to be mishandled.

12.6   Even though Authorised Users from Researchers will only have access to analytical Detailed Justice Data, and other steps will be taken in accordance with the usual PLIDA processes to ensure Data Subjects will not be individually identified in any research outcomes, the nature of Detailed Justice Data means that research projects using it may have a heightened risk of 'attribute disclosure'.

12.7   Attribute disclosure is where something can be learned about a person, even if they are not specifically identified in the relevant data. For example, outcomes from research using Detailed Justice Data may lead to a perception that all individuals within a particular community have, or are affected by, a particular attribute as a result of the research. Attribute disclosure may not involve re-identification, however there may nevertheless be a risk of harm to individuals who are known to be a part of that community, including discrimination, profiling, reputational damage or embarrassment. Attribute disclosure can be a particular risk for Aboriginal and/or Torres Strait Islander people, but it also applies for other cohorts.

12.8   This PIA has considered privacy in the context of these sensitivities inherent in Detailed Justice Data, and we observe that it means that it will be particularly important for the ABS to ensure its current privacy management strategies for PLIDA continue to be appropriate and sufficient for Detailed Justice Data.

13.   Linking Detailed Justice Data on an Enduring Basis

13.1   In summary, we have not identified additional or changed privacy risks associated with including Detailed Justice Data sets within PLIDA that will not be appropriately addressed or mitigated by existing processes, policies or technical arrangements.

13.2   We make the following comments in relation to particular issues, including as discussed with stakeholders.

---

[14] See discussion in the Australian Institute of Health and Welfare's report: *The health and wellbeing of First Nations people in Australia's prisons 2022*, available at https://www.aihw.gov.au/reports/prisoners/the-health-and-wellbeing-of-first-nations-people-i/summary

Maddocks

Consideration of public benefit, ethics, and utility

13.3   Stakeholders who were consulted generally agreed that significant benefits could be achieved through Detailed Justice Data being available for use in suitable approved research projects. In particular, stakeholders from research organisations observed that the data would be valuable for a range of projects, including those examining links with factors impacting interactions with justice systems, and how best to prevent contact with such systems. Stakeholders who were Data Custodians or other representatives of government also reflected that it would be beneficial for Detailed Justice Data to be used to help assess the efficacy of programs directed at supporting various individuals, including those leaving the justice system who may be at risk of recidivism.

13.4   As discussed in the 2022 PLIDA PIA, there are a range of privacy risks associated with adding new datasets to PLIDA. As a result of relevant recommendations in previous PIA processes, the ABS has implemented criteria that are considered before inclusion of new datasets or type of data that is proposed to be linked to PLIDA, to assess the public benefit, utility, sensitivities, and safety of the including the relevant data.

13.5   We consider that this implementation of this process, which we understand will also be undertaken in relation to Detailed Justice Data sets, will be an important mechanism to help clearly demonstrate why the inclusion of particular Detailed Justice Data in PLIDA will be appropriate.

Openness and transparency

13.6   Another important aspect of privacy (that is related to ethics) is ensuring that data handling practices are open and transparent. In the context of further Detailed Justice Data being added to PLIDA, potentially on an enduring basis, we observe that it will be important to ensure that the ABS continues to be open and transparent about the operation of PLIDA, in a manner consistent with the principles underpinning APP 1. Stakeholders also reflected that continuing openness and transparency regarding the handling of personal information for PLIDA was an important concern for them.

13.7   We support the ABS continuing to implement existing PLIDA arrangements to increase awareness about data included in PLIDA, including:

13.7.1   publishing information on its website; and

13.7.2   continuing to work with Data Custodians to improve information about PLIDA that is provided to Data Subjects at the point of the collection of their personal information.

13.8   We consider that these mechanisms are likely to continue to be appropriate to ensure that there is sufficient openness and transparency about the inclusion of Detailed Justice Data sets within PLIDA.

Managing compliance and sensitivity

13.9   Stakeholders reflected that, due to the sensitivity of Detailed Justice Data, it will be particularly important for Data Custodians to be supported with advice on the particular risks and implications of this type of data asset. In particular, the ethics of integrating projects using Detailed Justice Data and the additional restrictions that may operate on the lawful handling of Detailed Justice Data due to its sensitivity, were raised as areas of concern.

Maddocks

13.10   Data Custodians play a key role in ensuring that data can properly be included in PLIDA. For example, their role can be essential in relation to ensuring personal information:

13.10.1   has been collected and disclosed appropriately (APP 3; APP 6);

13.10.2   Data Subjects have been sufficiently notified of how their personal information may be used for PLIDA research (APP 5); and

13.10.3   personal information is of an adequate quality to be integrated with PLIDA (APP 10).

13.11   We observe that it will be important to ensure that Data Custodians are able, and feel supported, to determine whether to link particular Detailed Justice Data to PLIDA.

13.12   Previous PLIDA PIAs have recommended that the ABS take additional steps to consider whether entities (such as not for profit organisations) are appropriate to perform the role of a Data Custodian.[15] We observe that the ABS should continue to implement this recommendation in relation to entities seeking to provide Detailed Justice Data for inclusion in PLIDA, and give due consideration to the technical expertise and practical capability of those entities before they are permitted to act as Data Custodians for the purposes of Detailed Justice Data within PLIDA.

Quality of data

13.13   Stakeholders reflected that there may be a difference in quality between data collected directly from entities that are criminal justice institutions, and that that collected from other organisations that operate adjacently to those institutions. For instance, some of these entities may have varying levels of data literacy and data governance, and/or may be reliant on self-reported information, which may have a differing level of accuracy.

13.14   APP 10 requires APP entities to take such steps as are reasonable (if any) to:

13.14.1   ensure personal information collected, used, or disclosed is accurate, up-to-date and complete; and

13.14.2   in the case of uses or disclosures, to make sure this is done with regard to the purpose of the use or disclosure, and that the information is also relevant.

13.15   As such, ensuring that Detailed Justice Data is complete, accurate and up to date for the purpose of linking it to PLIDA is an important privacy consideration.

13.16   However, again we consider that the existing PLIDA processes, which do involve consideration of the quality of data before it is included in PLIDA, are likely to be appropriate.

---

[15] See, for example, **Recommendation 1** in *Australian Bureau of Statistics – Privacy Impact Assessment Update: 2024-25 Person Level Integrated Data Asset*, dated 11 April 2025 (date of publication 21 May 2025), available at https://www.abs.gov.au/about/legislation-and-policy/privacy/privacy-impact-assessments#2018

Maddocks

Security

13.17   Under APP 11.1, APP entities are required to take reasonable steps to protect personal information from misuse, interference and loss, and from unauthorised access, modification or disclosure.

13.18   Stakeholders reflected concern over the cumulative security risks associated with continuing to grow a large data asset like PLIDA, including by adding Detailed Justice Data.

13.19   As has been considered in previous PIA processes, adding further data to PLIDA, in particular information of an inherent sensitivity such as Detailed Justice Data, increases the richness and value of the data within PLIDA which is likely to also have the effect of increasing the attractiveness of attempting to gain unauthorised access to PLIDA for motivated individuals or organisations.

13.20   However, the security risks associated with PLIDA have been considered in a number of previous privacy assessments. We note that it will be important for the ABS to continue to implement security related recommendations from those assessments and we support the continued review and assessment of the security of PLIDA.

13.21   We suggest that the current measures are likely to be sufficient to address security risks associated with adding Detailed Justice Data to PLIDA.

14.   Approval of the Use of Detailed Justice Data for Research Projects

14.1   In summary, while we consider that existing processes, policies and technical arrangements will work towards addressing the identified additional or changed privacy risks associated with using Detailed Justice Data sets within PLIDA for approved PLIDA research projects, there are some areas where the ABS could consider additional best practice measures.

14.2   These areas are discussed below.

Ethical considerations

14.3   Ethics and privacy legal compliance are complexly interrelated, even though the Privacy Act only deals with ethics approval in a tangential manner.[16]

14.4   Stakeholders confirmed that the factors discussed in paragraph 12 above mean that it will be critical for ethical considerations to be considered and build into the design of research projects.

14.5   In particular, stakeholders raised questions about whether individuals affected by the type of research that may be conducted with Detailed Justice Data would have an opportunity to engage meaningfully with the approval process. This question was particularly raised in relation to whether affected communities, such as people who are or were incarcerated, or in some contexts, Aboriginal and / or Torres Strait Islander communities, would have an opportunity to access Detailed Justice Data and have a say in the research conducted using that data.

---

[16] The Privacy Act does not specifically mention ethical consideration, but rather builds in requirements which have an ethical component (e.g. requiring consent for collection and subsequent use sensitive information except in a range of limited circumstances; and requiring collection of personal information in a fair and lawful manner: see APP Guidelines, *Chapter 3: Collection of solicited personal information*, paragraph 3.62 – 3.63).

Maddocks

14.6   Stakeholders reflected that access to PLIDA data generally privileged dominant research institutions rather than working towards new partnerships with groups such as Aboriginal and / or Torres Strait Islander communities. It was observed that efforts to make the data accessible for those communities would be particularly important, noting stakeholder concerns around potential biases or potentially damaging research narratives. Having research initiatives led by affected communities, or involving them through consultation processes in the research design, was observed to be valuable to gaining important insights from research using Detailed Justice Data (such as about community needs and transition journeys). Having a strong ethical framework was considered to be an important component for research projects using Detailed Justice Data.

14.7   Currently, as part of their role in approving project proposals seeking to use PLIDA data, Data Custodians determine whether an ethics approval is required for the relevant project. For research projects requiring Aboriginal and / or Torres Strait Islander data, the ABS' standard practice is for the project to be referred to an internal Aboriginal and Torres Strait Islander Cultural Review Panel (ATSICRP) for an assessment of the project's impact on Aboriginal and/or Torres Strait Islander peoples and communities.

14.8   It is intended that these processes will continue to be applied for research projects involving Detailed Justice Data. We agree that it will be critical from a privacy best practice perspective for the intended handling of such data from an ethical perspective to be properly considered (i.e. it is not sufficient to just consider whether something *can* legally be done with Detailed Justice Data, it is also necessary to consider *should* it be done?)

14.9   We are aware that the ABS has been developing a data ethics framework that may be used to consider PLIDA projects (i.e., the Data Ethics Framework). The Data Ethics Framework allows consideration of ethical matters associated with proposed handling of data. When asked about the potential application of a Data Ethics Framework to Detailed Justice Data projects, stakeholders were generally supportive, although some observed that they would appreciate a further opportunity to review the final framework.

14.10   In relation to this, we consider that the PLIDA arrangements for the handling of Detailed Justice Data could be strengthened from a privacy and ethics perspective by the ABS implementing **Recommendation 1.**

Data Quality

14.11   Another data quality concern reflected during the stakeholder consultation process was the need to ensure that Detailed Justice Data used for specified PLIDA research projects was of sufficient quality for the research being undertaken.

14.12   As noted above, APP 10 requires APP entities to take such steps as are reasonable (if any) to:

14.12.1   ensure personal information collected, used, or disclosed is accurate, up-to-date and complete; and

14.13   in the case of uses or disclosures, to make sure this is done with regard to the purpose of the use or disclosure, and that the information is also relevant.

14.14   Stakeholders noted that Detailed Justice Data which is limited by geographic area in accordance with particular defined boundaries, may not be appropriate for certain types of research. For example, if a particular research project was looking at the impacts of incarceration on Aboriginal and / or Torres Strait Islander communities, relying on a dataset limited by state boundaries that does not reflect community or regional borders may not be appropriate because of the important differences between particular communities and the impacts of different levels of remoteness.

Maddocks

14.15   It was observed that it will be critical for Researchers to have a good understanding of the characteristics and any limitations of Detailed Justice Data before seeking to use it, or using it, for a particular research project. Otherwise, Researchers may place an inappropriate level of reliance on that data if they fail to consider those characteristics and limitation.

14.16   It was observed during the stakeholder consultations that it would provide assurance in relation to this matter if there could be better communication between Researchers and Data Custodians about the quality of Detailed Crime and Justice Data, to ensure it is used appropriately and interpreted correctly. This will mitigate the potential for unnecessary harms to be caused to individuals from research findings.

14.17   We observe that it will be important for the ABS to continue implementing the measures it has in place to ensure that Data Custodians are able to appropriately approve research projects making use of their data. However, we also consider that implementation of **Recommendation 2** would be a further best practice measure to address the potential data quality risks.

Reidentification risk

14.18   Obligations under the Privacy Act only apply to information that is 'personal information', which is defined under the Privacy Act as:

information or an opinion about an identified individual, or an individual who is reasonably identifiable:

> *(a) whether the information or opinion is true or not; and*

> *(b) whether the information or opinion is recorded in a material form or not.*

14.19   Because personal information must be about an 'identified individual', information that has undergone appropriate and robust deidentification processes will not be personal information that is subject to the Privacy Act.

14.20   Deidentification can therefore allow an entity to handle information in a way that would not otherwise be permitted under the APPs. Deidentification also generally has the potential to protect the interests of individuals, for example, by minimising unwanted attention that might be directed towards them.

14.21   When analytical data is disclosed through PLIDA to Researchers for approved research projects, it will not contain any direct identifiers about any of the Data Subjects and additional measures will have been implemented as necessary to reduce any residual reidentification risk (e.g., banding data and / or ensuring the level of granularity is not too high).

14.22   However, reidentification risk remains a relevant consideration, in particular when new types of data are introduced to PLIDA. For the purposes of the Privacy Act, the OAIC has indicated that information will need to be deidentified such that no individual is 'reasonably identifiable' from the information and the risk of reidentification is 'very low' in the relevant data access environment, for it to be considered to not be personal information.[17]

---

[17] For further OAIC discussion of de-identification, see: https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/de-identification-and-the-privacy-act

Maddocks

14.23   Detailed Justice Data has the potential to contain information about Data Subjects that is unique and specific to particular individuals, or relates to a low population area. Moreover, if Authorised Users from Researchers have specialist knowledge in a particular area or region, it is possible that their specific knowledge would enhance the likelihood that they may be able to identify a Data Subject from analytical data. There is also a potential for heightened consequences to be associated with any possible reidentification of Detailed Justice Data due to its sensitivity.

14.24   During the stakeholder consultation process, stakeholders also observed that reidentification risk was one of their key concerns in relation to the use of Detailed Justice Data. Several also observed, however, that existing PLIDA safeguards for reidentification risk were seen as positive privacy measures and gave them a high level of trust in the relevant linking and research processes. Stakeholders reflected the importance of continuing to implement necessary safeguards in this area.

14.25   We observe that the ABS' continued implementation of its reidentification risk review and minimisation processes will be vital to maintaining privacy best practice going forwards. In addition to this, we recommend the ABS implement **Recommendation 3**.

Research approval processes

14.26   Stakeholders observed that given the particular sensitivity of Detailed Justice Data, it may be beneficial if there were extra judicious requirements for the approval of research projects that would make use of such data. We observe that the concerns raised by stakeholders with regard to Data Custodians requiring extra support in relation to the linking of Detailed Justice Data were also raised in the context of approving requests for access to and use of Detailed Justice Data.

14.27   In order to mitigate this risk, we recommend the ABS consider implementing:

14.27.1   **Recommendation 1** with regard to utilising the Data Ethics Framework.; and

14.27.2   **Recommendation 3** with regard to producing guidance for Data Custodians dealing with Detailed Justice Data.

Maddocks

Part E   Summary of Privacy Compliance

15.   Introduction

15.1   Table 1 below summarises our analysis of incorporating Detailed Justice Data in PLIDA against each APP, and allocates an *APP Compliance Risk Rating* for each APP in accordance with the descriptors set out in the table in **Part B [Methodology and Assumptions]**.

15.2   This analysis does not address those elements of the APPs which reflect the ABS's broader compliance obligations.

Table 1. Summary of APP Compliance

APP	Summary
APP 1 [open and transparent management of personal information] **Compliant**	We consider that the current strategies to achieve transparency and openness in relation to data that is added to PLIDA, and in relation to its use for approved research projects is likely to be appropriate for the handling of Detailed Justice Data.
APP 2 [anonymity and pseudonymity] **Compliant**	Not relevant, as Data Subjects will not be dealing with the ABS directly for the inclusion of further Detailed Justice Data in PLIDA. As discussed in previous PIAs, it is important that the identity of Authorised Users continues to be identified.
APP 3 [collection of solicited personal information] **Compliant**	We consider that the existing measures for PLIDA are likely to be appropriate for the ABS' collection of Detailed Justice Data, in particular by ensuring that Data Custodians have the legal ability to disclose data to the ABS for inclusion in PLIDA. We observe that the ABS should continue to ensure that the entities proposed to be Data Custodians of Detailed Justice Data are appropriate to carry out that role.[18]
APP 4 [dealing with unsolicited personal information] **Compliant**	Not relevant, as all Detailed Justice Data collected by the ABS for PLIDA purposes will be solicited.

---

[18] See, for example, **Recommendation 1** in *Australian Bureau of Statistics – Privacy Impact Assessment Update: 2024-25 Person Level Integrated Data Asset*, dated 11 April 2025 (date of publication 21 May 2025), available at https://www.abs.gov.au/about/legislation-and-policy/privacy/privacy-impact-assessments#2018

Maddocks

APP	Summary
APP 5 [notification of the collection of personal information] **Compliant**	It is the responsibility of Data Custodians to ensure that appropriate notification is provided to Data Subjects when their personal information is collected for the purposes of PLIDA. We do not consider that anything further is required in relation to this APP in connection with Detailed Justice Data, provided that the ABS continues to implement its current assurance measures.
APP 6 [use or disclosure of personal information] **Improvement to meet best practice**	We consider that best privacy practices in connection with the use and disclosure of Detailed Justice Data for approved research projects may be further improved or enhanced by the implementation of **Recommendation 1** and **Recommendation 3**.
APP 7 [direct marketing] **Compliant**	Not relevant to ABS, and there will be no use of Detailed Justice Data by any organisations of any personal information for direct marketing purposes.
APP 8 [cross-border disclosure of personal information] **Compliant**	There will be no new or changed overseas data flows will be involved in the integration of further Detailed Justice Data into PLIDA. There are current PLIDA processes in place for consideration of any overseas Authorised Users for Researchers seeking access to PLIDA data.
APP 9 [adoption, use or disclosure of government related identifiers] **Compliant**	Not relevant, as inclusion of the further Detailed Justice Data in PLIDA will not involve any new or changed use of government identifiers by any organisations.
APP 10 [quality of personal information] **Improvements to meet best practice**	Whether Detailed Justice Data is sufficiently accurate, up to date, complete and relevant to justify its inclusion in PLIDA and its use for particular research purposes is a very important consideration considering its inherent sensitivity. We consider that implementation of **Recommendation 2** would be a further step to support best privacy practice, through supporting an appropriate level of reliance being placed on Detailed Justice Data by Data Custodians and Researchers with regard to the inherent characteristics of particular datasets.

Maddocks

APP	Summary
APP 11 [security of personal information] **Improvements to meet best practice**	The inclusion of further Detailed Justice Data in PLIDA is likely to contribute to the cumulative security risk associated with PLIDA as the richness of the data asset is increased. However, the ABS and the PLIDA Board have made a number of security commitments in relation to data that is added to PLIDA, and we do not consider anything additional is required in relation to this APP, provided that these commitments continue to be implemented.
APP 12 [access to personal information] **Compliant**	Once Detailed Justice Data is in PLIDA, Data Subjects will not be able to access their personal information. This has been considered in previous PIAs, and we consider that the current PLIDA processes in relation to this matter remain appropriate.
APP 13 [correction of personal information] **Compliant**	Data Subjects will not be able to request correction of their personal information in PLIDA. This has been considered in previous PIAs, and we consider that the current PLIDA processes in relation to this matter remain appropriate.

Part F   Glossary

16.   Introduction

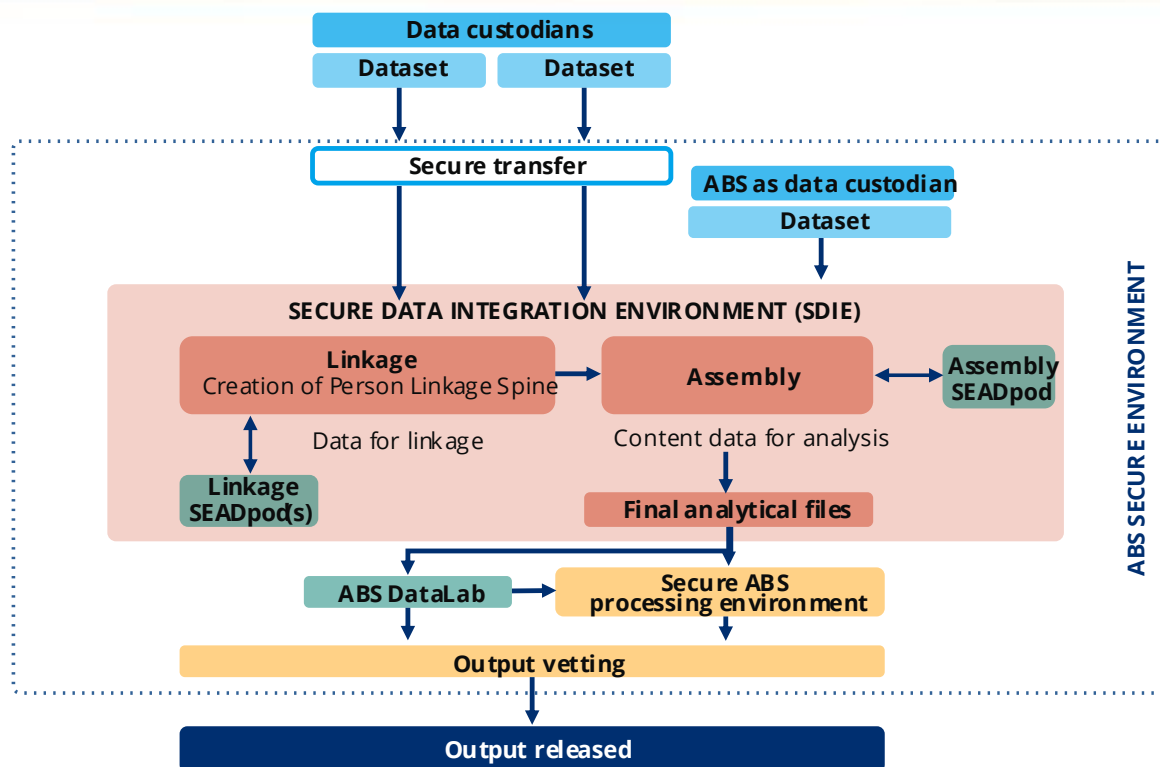16.1   In this PIA, capitalised terms have the meaning given to them in Table 2 below.

Table 2. Table of defined terms

Definitions	
ABS	means the Australian Bureau of Statistics.
APP, or Australian Privacy Principle	has the meaning given to it in the Privacy Act.
APP Code	means the *Privacy (Australian Government Agencies – Governance) APP Code 2017*.
APP Guidelines	means the OAIC's *Australian Privacy Principles guidelines*.
Archives Act	means the *Archives Act 1983* (Cth).
Authorised Users	means the individuals employed by Researchers that have been approved to access PLIDA data for approved research projects.
BEBOLD	stands for *Better Evidence, Better Outcomes, Linked Data*, and means the platform of that name containing integrated data which was established and is maintained by the BetterStart Group within the University of Adelaide.
Data Custodians	means the entities that contribute datasets to PLIDA and have a responsibility for the data within those datasets.
Data Ethics Framework	means the data ethics framework being developed by the ABS.
Data Subjects	means the individuals whose analytical data is included in Detailed Justice Data sets within PLIDA.
Detailed Justice Data	means data related to crime and / or police or justice systems in Australia, as described in paragraphs 1.5.1 and 1.5.2 of this PIA Update report.
CJDA	stands for Criminal Justice Data Asset, and means the national data asset of that name which combines datasets from State and Territory police, criminal courts, and corrective service agencies across Australia.
CoATSIS	means the ABS Centre of Aboriginal and Torres Strait Islander Statistics.
GID	means the Framework for Governance of Indigenous Data, which is a document designed to act as a stepping stone towards greater understanding of the principles of Indigenous Data Sovereignty

Maddocks

Definitions	
	and was co-designed by Australian Public Service agencies and Aboriginal and Torres Strait Islander partners).
HSDS	stands for Human Services Data Set, and means the dataset developed for the TFM project.
MADIP	stands for the Multi-Agency Data Integration Project, which was the previous name of PLIDA.
OAIC	means the ABS of the Australian Information Commissioner.
personal information	has the meaning given in section 6 of the Privacy Act.
PIA	stands for privacy impact assessment.
PIA Update	means this PIA Update process to consider the inclusion and use of Detailed Justice Data within PLIDA, as described in this report.
PLIDA	stands for Person Level Integrated Data Asset, and means the data asset of that name for which the ABS is the accredited integrating authority.
PLIDA Board	means the governance board established for the operations and strategic direction of PLIDA.
POLA Act	means the *Privacy and Other Legislation Amendment Act 2024* (Cth).
Privacy Act	means the *Privacy Act 1988* (Cth).
PTA	stands for privacy threshold assessment.
Researchers	means the research institutions from government, universities, and public policy institutes, which have been approved to access PLIDA data for research purposes.
sensitive information	has the meaning given in section 6 of the Privacy Act.
Spine	means Person Linkage Spine which acts as the central linkage infrastructure for PLIDA.
TFM	stands for Their Futures Matter, and means the NSW government project of that name aimed at improving outcomes for vulnerable children, young people and families.

Maddocks

Attachment 1   PLIDA Information Flow Diagram – Current Data Handling Practices

Figure 1. This diagram was generated by the ABS to depict the Information Flows associated with the handling of personal information for PLIDA

Attachment 2 Materials Reviewed

Further materials relied on by Maddocks in connection with the preparation of this PIA report include (this list does not include additional publicly available materials, including legislation, guidance and research materials, that we also considered as part of this PIA).

1. ABS, *Privacy Impact Assessment – Their Futures Matter – Integrating Data from the NSW Human Services Dataset with MADIP*, dated December 2021 (received by Maddocks 6 June 2025)

2. ABS, *Privacy Threshold Assessment – Linking of Better Evidence, Better Outcomes, Linked Data (BEBOLD) to Person Level Integrated Data Asset (PLIDA) for the purposes of University of Adelaide (Uoa) – BEBOLD project (2023-051) and the Life Course Data Initiative (LCDI, project 2024-001)*, dated 2025 (received by Maddocks 10 June 2025)

3. ABS, Internal ABS email discussing growing trend in requests for crime and justice related data items in PLIDA and current ABS treatment of such data, *SUBJECT: Privacy issues relating to crime and justice data*, dated 20 March 2025 (received by Maddocks 10 June 2025)

4. ABS, Internal ABS communications strategy, *Quick Guide on Broad Use Standard Release Discussion with Custodians / Clients* (received by Maddocks 10 June 2025)

5. Draft documents comprising an ABS Data Ethics Framework, being documents entitled *ABS Data Ethics Principles*, *ABS Data Ethics Principles Guide* and *ABS Data Ethics Assessment Tool* (Received by Maddocks August 2025)

6. Transcripts and notes from stakeholder consultation sessions conducted in July and August 2025, and written submissions provided to the ABS in relation to this consultation process, were also relied on in the preparation of this report. Organisations involved in the consultations (i.e., either being in attendance at a stakeholder consultation session, and/or providing written feedback after being invited to do so) included:

    - Australian Taxation Office
    - Department of Education
    - Department of Employment and Workplace Relations
    - Department of Finance
    - Department of Health, Disability and Ageing
    - Department of Home Affairs
    - Department of Industry Science and Resources
    - Services Australia
    - Department of Social Services
    - Corrections Research, Evaluation & Statistics NSW (CRES)
    - Information & Privacy Commission NSW (IPC NSW)
    - Justice Action (JA)
    - University of Adelaide (UoA)
    - Crime Statistics Agency (CSA)
    - Department of Justice and Community Safety Vic (DJCS)
    - Legal Aid NSW (LA)
    - Office of the Information Commissioner, Northern Territory (OIC NT)
    - Office of the Information Commissioner Queensland (OIC Q)
    - Barang

Maddocks

- Binarri-binyja yarrawoo

- PAMA Futures (Cape York)

- Office of the Victorian Information Commissioner

7. Answers provided by ABS to questions raised by stakeholders during consultation sessions which were 'taken on notice' by the ABS (received by Maddocks 5 September 2025)

8. Feedback from stakeholders on draft of this PIA report (received by Maddocks on 20 and 21 October 2025 and on 13 November 2025)

Maddocks