

# Australian Bureau of Statistics

Privacy Impact Assessment:

Criminal Justice Data Asset – ABS20230.026

17 March 2025



# CONTENTS

<b>1.</b>	<b>EXECUTIVE SUMMARY .....</b>	<b>4</b>
1.1	Introduction .....	4
1.2	Summary of recommendations .....	5
<b>2.</b>	<b>ABOUT THIS PIA .....</b>	<b>8</b>
2.1	What is a privacy impact assessment? .....	8
2.2	Scope of this PIA .....	8
2.3	Qualifications and assumptions.....	9
2.4	Methodology.....	9
2.5	APPs not subject to detailed privacy compliance assessment.....	10
<b>3.</b>	<b>PROJECT DESCRIPTION .....</b>	<b>11</b>
3.1	Background.....	11
3.2	Terminology .....	12
3.3	Legislative context.....	13
3.4	Collection of data from source data custodians.....	14
3.5	Data linkage using SLK-581 .....	15
3.6	Release of de-identified data to approved researchers through the DataLab (out of scope).....	16
3.7	Output of aggregated data/analysis from the DataLab (out of scope) .....	16
<b>4.</b>	<b>RELEVANT PERSONAL AND PROTECTED INFORMATION .....</b>	<b>17</b>
4.1	What is personal information and sensitive information? .....	17
4.2	Personal information involved in the Project.....	18
4.3	Protected information involved in the Project.....	19
<b>5.</b>	<b>SECURITY COMPLIANCE ASSESSMENT .....</b>	<b>20</b>
<b>6.</b>	<b>PRIVACY (APP) COMPLIANCE ASSESSMENT .....</b>	<b>24</b>
6.1	APP 1: Open and transparent management of personal information .....	24

6.2	APP 2: Anonymity and pseudonymity .....	31
6.3	APP 3: Collection of personal information .....	32
6.4	APP 4: Dealing with unsolicited information .....	34
6.5	APP 5: Collection notice and transparency .....	35
6.6	APP 6: Use and disclosure of personal information .....	36
6.7	APP 10: Data quality .....	37
6.8	APP 11: Data security .....	39
6.9	APPs 12 and 13: Data access and correction .....	41
	SCHEDULE 1 — INFORMATION FLOWS .....	42
	SCHEDULE 2 — DATA CUSTODIANS .....	47
	SCHEDULE 3 — DATA ELEMENTS .....	48
	SCHEDULE 4 — MATERIALS CONSIDERED .....	50
	SCHEDULE 5 — GLOSSARY .....	51

# 1. Executive summary

## 1.1 Introduction

- (a) The National Crime and Justice Data Linkage Project (**Project**) aims to develop a longitudinal national criminal justice data asset, known as the Criminal Justice Data Asset (**CJDA**).
- (b) The Project was initiated out of the Council of Australian Governments' *Prison to Work Report* (2016) (**Prison to Work Report**), which noted that there were '*data gaps and a patchy evidence base for what works*' to improve outcomes for prisoners and ex-prisoners.<sup>1</sup> The *Prison to Work Report* made a number of recommendations to address these shortcomings, including that:
  - (i) State and Territory governments work with the Commonwealth to '*share essential de-identified criminal justice data (including corrections, courts, police and juvenile justice) to enable the quantifying of the flow of prisoners through the system*';
  - (ii) the Commonwealth and State and Territory governments work together to '*identify and remedy data gaps*'; and
  - (iii) the Commonwealth, together with State and Territory governments, '*conduct a project linking the data for persons moving through the child protection, justice, health, welfare and employment systems*'.<sup>2</sup>
- (c) The Australian Bureau of Statistics (**ABS**) will produce the CJDA by linking datasets provided by State and Territory police, criminal courts and corrective services agencies across Australia. De-identified data from the CJDA will be made available to approved researchers, to provide opportunities for researchers to better understand how individuals interact with the criminal justice system, and to develop, monitor and evaluate criminal justice policies.
- (d) This privacy impact assessment (**PIA**) has been commissioned by the ABS to:
  - (i) identify and assess privacy and secrecy compliance risks for the ABS relating to the implementation of the Project; and
  - (ii) make recommendations for eliminating, reducing or managing those privacy and secrecy compliance risks.
- (e) Matters not in scope for this PIA are identified in section 2.2(b).

---

<sup>1</sup> Council of Australian Governments, *Prison to Work Report* (2016), pp 7, 48–53.

<sup>2</sup> *Prison to Work Report*, Finding 9.

## 1.2 Summary of recommendations

Recommendations made in this PIA to mitigate identified privacy and secrecy compliance risks for the ABS in relation to the Project, are set out below.

<b>Recommendation 1: Re-identification risk management</b>	<p>We recommend that the ABS periodically review the efficacy of the measures that the ABS has in place to manage the risks of re-identification (including any changed or increased risks over time) in the context of the Project. These periodic reviews should consider:</p> <ul style="list-style-type: none"><li>• the kind of information that is made available to researchers through the DataLab (and whether individuals may be identifiable due to unique or uncommon characteristics that enable identification;</li><li>• the kind of information that is permitted to be released from the DataLab; and</li><li>• the controls and safeguards that are in place in the DataLab, to manage re-identification risks.</li></ul>
<b>Recommendation 2: Further privacy risk assessments</b>	<p>If there are any new or material changes to the information flows identified in Schedule 1, including:</p> <ul style="list-style-type: none"><li>• the collection of additional types of personal information;</li><li>• additional or changed uses of personal information not identified in Schedule 1;</li><li>• the sharing of personal information with third parties not identified in Schedules 1 or 3; or</li><li>• as a result of changes to the Project and/or the way in which it is administered,</li></ul> <p>a privacy threshold assessment and, if required, further assessment of privacy impacts and compliance risks, should be undertaken (which could be in the form of a supplementary PIA.</p> <p>The assessment(s) should consider privacy impacts from both privacy law compliance and community expectations perspectives.</p> <p>A further secrecy compliance assessment should also be undertaken, as necessary and to the extent that there are any new or material changes to the protected information flows identified in Schedule 1.</p>

<b>Recommendation 3: Periodic reviews</b>	<p>We recommend that the ABS periodically review the operation of the Project to ensure:</p> <ul style="list-style-type: none"> <li>• methods for handling personal information remain appropriate, and align with community expectations;</li> <li>• ongoing APP compliance; and</li> <li>• opportunities to refine data handling practices and maximise privacy protection can be identified and implemented.</li> </ul>
---	--

<b>Recommendation 4: Data sharing agreements with source data custodians</b>	<p>We recommend ensuring that the terms of each MOU (or other form of data sharing agreement) between the ABS and each source data custodian address the following matters:</p> <ul style="list-style-type: none"> <li>• the data that the source data custodian will provide to the ABS;</li> <li>• the purpose for which the source data custodian will provide the relevant data to the ABS, and the purposes for which the ABS may use and disclose that data;;</li> <li>• the legal authority under which each party will collect, use and disclose the relevant data;</li> <li>• arrangements and requirements relating to the secure transfer/sharing and storage of data;</li> <li>• each party's obligations with respect to: <ul style="list-style-type: none"> <li>○ compliance with applicable privacy laws, namely: <ul style="list-style-type: none"> <li>▪ for the ABS – the Commonwealth Privacy Act and APPs; and</li> <li>▪ for data custodians – the Commonwealth Privacy Act and APPs, or an equivalent privacy law that binds the data custodian in their jurisdiction;</li> </ul> </li> <li>○ compliance with other relevant legislation that may apply to the data provided by the data custodian (e.g. secrecy provisions in legislation); and</li> <li>○ where necessary, obtaining their own legal advice and undertaking their own PIAs (or other form of privacy risk assessments) prior to sharing any data;</li> </ul> </li> <li>• obligations and processes relating to the notification and handling of data breaches and privacy complaints.</li> </ul>
--	--

<b>Recommendation 5: Governance of Indigenous Data</b>	<p>We recommend that the ABS embed and operationalise best practice for the governance of Aboriginal and Torres Strait Islander data into the CJDA. These principles are outlined in the National Indigenous Australians Agency's <a href="#">Framework for Governance of Indigenous Data</a>.</p>
--	--

**Recommendation 6:  
Transparency and  
notification**

We recommend that the ABS liaise with source data custodians to develop a strategy that supports transparency around the use of individual data for statistical purposes, including data integration. This strategy should aim to ensure that relevant individuals are informed about how their data is being collected and used, the purposes of data integration, and the measures in place to protect their privacy.

**Recommendation 7:  
Data quality and  
statistical linkage key**

We recommend that the ABS periodically review data quality, including the linkage methodology, to ensure that the data is fit for purpose for the Project.

## 2. About this PIA

### 2.1 What is a privacy impact assessment?

- (a) A PIA is defined in subsection 33D(3) of the *Privacy Act 1988* (Cth) (**Privacy Act**) as a written assessment of an activity or function that:
  - (i) identifies the impact that the activity or function might have on the privacy of individuals; and
  - (ii) sets out recommendations for managing, minimising or eliminating that impact.
- (b) Section 12 of the *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth) (**APS Privacy Governance Code**) requires Commonwealth agencies to conduct a PIA for all 'high privacy risk' projects, such as projects that involve new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals.
- (c) A PIA involves a detailed analysis of the proposed flows of personal information (as they are known at the time of the PIA), and potential privacy risks and impacts of a project. Conducting a PIA adds value to projects that involve the handling of personal information by identifying and mitigating privacy risks, ensuring compliance with legal obligations under privacy laws, and facilitating the inclusion of privacy as a key consideration in the project development ('privacy by design').
- (d) Privacy impacts may be negative (privacy invasive) or positive (privacy enhancing). A failure to properly embed privacy protection measures into a project may cause a breach of privacy laws, or limitations (e.g. technological, contractual or cost) in 'retro-fitting' a system or program design to ensure legal compliance or address community concerns about privacy.
- (e) A PIA should do more than just assess a project's likely compliance with statutory privacy principles. It should also consider the privacy control environment (i.e. the policies, procedures and structures which affect accountability for privacy compliance), and potential wider community concerns and perceptions.
- (f) Further, PIA recommendations should seek to achieve an appropriate balance between the interests of individuals affected by a project (including measures for minimising privacy intrusions and maximising privacy protection), and the achievement of the objectives of a project.

### 2.2 Scope of this PIA

- (a) On the basis of the information flows described in Schedule 1, this PIA considers the following:
  - (i) privacy compliance risks for the ABS in relation to the Project, as assessed against the Privacy Act and Australian Privacy Principles (**APPs**); and
  - (ii) secrecy compliance risks for the ABS in relation to the Project, as assessed against the *Census and Statistics Act 1905* (Cth) (**C&S Act**).

- (b) This PIA does not assess:
- (i) the collection, use, disclosure, storage or other handling of personal information by any third parties;
  - (ii) any research projects that may access and make use of the CJDA;
  - (iii) compliance with secrecy provisions other than those under the C&S Act;
  - (iv) compliance with any obligations that may apply to the ABS under the *Archives Act 1983* (Cth) (**Archives Act**);
  - (v) the ABS DataLab (**DataLab**), which is the subject of a separate PIA that has been prepared by the ABS;<sup>3</sup>
  - (vi) the existing process by which researchers register and submit project proposal for accessing ABS data (via myDATA);
  - (vii) the collection and handling of personal information relating to researchers;
  - (viii) the disclosure of statistical information by the ABS, including the disclosure of data to approved researches through the DataLab and/or the release of aggregated data outputs from the DataLab; or
  - (ix) any information flows that are not set out in Schedule 1.

## 2.3 Qualifications and assumptions

- (a) This PIA is based on the following assumptions:
- (i) at the date of this PIA report, the information flows described in Schedule 1 accurately reflect how personal and protected information is intended to be collected, stored, used and disclosed by the ABS in relation to the Project; and
  - (ii) the Australian Statistician has made all relevant delegations required under section 17 of the C&S Act to enable officers of the ABS to administer the Project.

## 2.4 Methodology

- (a) This PIA (commenced by MinterEllison, and finalised by Clayton Utz) has been undertaken by:
- (i) applying an approach based on the *Guide to undertaking privacy impact assessments (September 2021)* (**PIA Guide**) issued by the Office of the Australian Information Commissioner (**OAIC**);
  - (ii) mapping out the information flows (in consultation with the ABS) as described in Schedule 1;

---

<sup>3</sup> [Privacy Impact Assessments | Australian Bureau of Statistics \(abs.gov.au\)](https://www.abs.gov.au/privacy-impact-assessments).

- (iii) considering and relying on the material listed in Schedule 4;
  - (iv) identifying and assessing the privacy impacts and secrecy compliance risks relating to the Project, by reference to the information flows described in Schedule 1;
  - (v) preparing a draft PIA for comment by the ABS; and
  - (vi) finalising the report based on feedback received from the ABS.
- (b) MinterEllison also participated in ABS-led consultations with stakeholders. Five stakeholder consultation sessions were undertaken in November and December 2023, and February and August 2024, with the following groups:
- (i) police data custodians;
  - (ii) criminal courts and corrective services data custodians;
  - (iii) privacy regulators (state and national);
  - (iv) community legal centres (including organisations focused on youth and people with disabilities); and
  - (v) Aboriginal and Torres Strait Islander representatives.
- (c) The outcome of these consultations are summarised in a separate Consultation Report for the Project.

## 2.5 APPs not subject to detailed privacy compliance assessment

- (a) In the course of preparing this PIA, the application of the following APPs was considered, but an in-depth compliance assessment was not considered necessary in the circumstances:
- (i) **APP 7 (Direct marketing)** – This principle does not apply to the ABS as it is not an 'organisation' for the purposes of the Privacy Act and section 7A of the Privacy Act does not apply to the ABS in the context of the Project. In any event, the Project will not involve the use or disclosure of personal information for direct marketing purposes.
  - (ii) **APP 8 (Cross-border disclosure of personal information)** – This principle applies where an APP entity discloses personal information to an overseas recipient. This principle does not apply in this context because the Project will not involve any cross-border disclosures of personal information outside Australia. We are instructed that while the DataLab can be made accessible to overseas persons (subject to direct approval from the Australian Statistician and a further Cyber Security team assessment), access for this Project will be restricted to Australia only. We also note that the DataLab is out of scope for this PIA.
  - (iii) **APP 9 (Adoption, use or disclosure of government identifiers)** – This principle does not apply to the ABS as it is not an 'organisation' for the purposes of the Privacy Act, and section 7A of the Privacy Act is not applicable in the context of the Project.

### 3. Project Description

#### 3.1 Background

- (a) The Project aims to develop a longitudinal national criminal justice data asset, known as the CDJA, with a view to providing opportunities for researchers to better understand how individuals interact with the criminal justice system, and to develop, monitor and evaluate criminal justice policies.
- (b) The ABS will produce the CJDA by linking police, criminal courts and corrective services datasets provided by State and Territory agencies across Australia (also known as data custodians). These datasets are derived from existing ABS administrative crime and justice publications<sup>4</sup> and will be linked by the ABS using **SLK-581**<sup>5</sup>, which is a string of 14 letters and numbers that utilises a person's name, date of birth and sex.
- (c) We are instructed that the ABS has completed a Proof of Concept study for the CJDA, where the ABS used SLK-581 to link police offenders with criminal court defendants and adult persons held under the authority of corrective services nationally (although no data outputs were released by the ABS). In the Proof of Concept study, the ABS found that the linkage quality was fit for research purposes and preliminary analysis demonstrated the utility of the Project.
- (d) Given the results of the Proof of Concept study, the ABS is now seeking to create an enduring national data asset, which will be updated annually, and made available to approved researchers within the secure environment of the ABS DataLab.
- (e) As explained in further detail below, the Project will involve the following steps:
  - (i) the collection of data from police, criminal courts and corrective services source data custodians;
  - (ii) the linkage of police, criminal courts and corrective services datasets using SLK-581, comprising the following processes:
    - A. Librarian team process;
    - B. Linker team process; and
    - C. Assembler team process;
  - (iii) the release of de-identified data to approved researchers within the secure environment of the ABS DataLab; and
  - (iv) the release of aggregated data outputs from the DataLab.

---

<sup>4</sup> [Recorded Crime - Offenders, 2022-23 financial year | Australian Bureau of Statistics](#)  
[Criminal Courts, Australia, 2022-23 financial year | Australian Bureau of Statistics](#)  
[Prisoners in Australia, 2023 | Australian Bureau of Statistics](#)

<sup>5</sup> See the Glossary in Schedule 5 for more information.

- (f) We are instructed that these steps and processes are standard ABS procedures. We also note that the release of data and aggregated data outputs from the DataLab is out of scope for this PIA.

## 3.2 Terminology

- (a) In this PIA, the following terms are used:

- (i) **Source Linkage Data File** – a data file that contains:
  - A. the Source Record ID (also known as an original record ID – i.e. a unique identifier for an individual record in a dataset); and
  - B. the SLK-581 linkage variable;
- (ii) **Source Analytical Data File** – a data file that contains:
  - A. the Source Record ID; and
  - B. analytical data elements for individuals (e.g. age, sex, Indigenous status, offence and sentence).

A Source Analytical Data File does not contain any direct identifiers for individuals (e.g. name or date of birth);<sup>6</sup>
- (iii) **Concordance File** – a data file prepared by the Librarian team, which shows how Source Record IDs correspond to Anonymised Record IDs. Anonymised Record IDs are generated by the Librarian team. The Concordance File is provided to the Assembler team;
- (iv) **Linkage Files** – data files prepared by the Librarian team using the Source Linkage Data File, which show how encrypted SLK-581s correspond with Anonymised Record IDs. The Linkage Files are provided to the Linker team;
- (v) **Linkage Results File** – a data file prepared by the Linker team using the Linkage Files, which show how Anonymised Record IDs correspond to each other (i.e. correspond to the same individual). The Linkage Results File is provided to the Assembly team; and
- (vi) **Output Files** – data files prepared by the Assembler team using the clean Source Analytical Data Files, the Concordance File and the Linkage Results File. The Output Files contain analytical data elements from each dataset which are relevant to a particular project proposal, along with an Analysis ID. The Output Files are uploaded to the DataLab for access by approved researchers.

---

<sup>6</sup> While the information in the Source Analytical Data File does not contain any direct identifiers, we are instructed that spontaneous recognition could be possible. For example, one may know that X was caught for Y offence on Z date, and Y offence and Z date are contained in the file. ABS officers must sign an undertaking not to discuss/disclose any personal information, with penalties for unauthorised disclosure.

### 3.3 Legislative context

- (a) For the Project to be lawful and successful, the ABS and data sharing partners will need to work together to navigate various legal frameworks that apply to the Project and its participants, in a holistic way.
- (b) As a starting point, it is important to have a clear understanding of the applicable legal frameworks, as this will inform the assessment of whether (and the basis, scope and purposes for which):
  - (i) State and Territory data sharing partners can provide data to the ABS; and
  - (ii) the ABS can collect and subsequently deal with the data.

#### C&S legislation

- (c) The C&S Act governs the collection, compilation, analysis and dissemination of statistical information by the Australian Statistician.
- (d) Section 9 of the C&S Act provides that the Australian Statistician may, from time to time, collect such statistical information in relation to the matters prescribed for the purpose of that section, as they consider appropriate. Relevantly, 'crime' is one of the matters prescribed under regulation 13 (item 11) of the *Census and Statistics Regulation 2016* (Cth) (**C&S Regulations**). The ABS will collect statistical information under the authority of section 9 of the C&S Act and regulation 13 (items 11 and 38) of the C&S Regulations for the purpose of the Project.
- (e) Section 12 of the C&S Act provides that the Australian Statistician shall compile and analyse the statistical information collected under the C&S Act, and shall publish and disseminate the results of any such compilation and analysis, or abstracts of those results.
- (f) Section 13 of the C&S Act provides that the Minister may, by legislative instrument, make determinations providing for the disclosure, with the approval in writing of the Australian Statistician, of information included in a specified class of information furnished in pursuance of the C&S Act. The *Census and Statistics (Information Release and Access) Determination 2018* (Cth) (**C&S Determination**) is a determination which has been made under section 13 of the C&S Act, which sets out the requirements governing the disclosure of information provided to the Australian Statistician under the C&S Act. Relevantly, section 15 of the C&S Determination authorises the disclosure of information in the form of individual statistical records where:
  - (i) all direct identifiers, such as name and address, have been removed;
  - (ii) if the information relates to an individual, it is disclosed in a manner that is not likely to enable the identification of the individual; and
  - (iii) the disclosure recipient has given the Australian Statistical an undertaking that complies with the requirements of subsection 15(2), including that the relevant individual or organisation:

- A. will not attempt to use the information to identify particular individuals or organisations to which the information relates; and
  - B. will only use the information for statistical or research purposes.
- (g) Section 17 of the C&S Act provides that the Australian Statistician may, by signed instrument, delegate to an officer all or any of their powers under the C&S Act or any other law. We are instructed that the Australian Statistician has made all relevant delegations required under section 17 of the C&S Act to enable officers of the ABS to administer the Project.

### **Privacy laws**

- (h) As a Commonwealth government agency, the ABS is subject to the Commonwealth Privacy Act and APPs.
- (i) State and Territory government data custodians are not bound by the Commonwealth Privacy Act. Instead, they are subject to applicable privacy laws in their respective jurisdictions.
- (j) Queensland, New South Wales, Victoria, Tasmania, the Australian Capital Territory, Northern Territory and Western Australia have privacy laws which bind public sector bodies in their jurisdictions, and impose similar (though not identical) obligations as the APPs. South Australia<sup>7</sup> does not currently have privacy legislation in effect.

## **3.4 Collection of data from source data custodians**

- (a) The Project will involve the collection of data by the ABS, from police, criminal courts and corrective services data custodians in each State and Territory.
- (b) The two types of files received or created by the ABS (Source Analytical Data Files and Source Linkage Data Files) will be delivered and stored separately as part of the 'Separation Principle'. The Separation Principle means that no individual can access both the identifying data used for linkage (i.e. SLK-581 linkage variable) and the analytical data (which does not contain any direct identifiers). ABS staff working on the Project will only have access to the information that they need to perform their assigned role.
- (c) The information that will be included in each of the Source Analytical Data Files and the Source Linkage Data Files is set out in Schedule 3.

---

<sup>7</sup> While South Australia does not have privacy legislation, there is a Cabinet Administrative Instruction ([PC012 Information Privacy Principles Instructions](#), last revised in May 2020) which applies to SA public sector agencies.

## 3.5 Data linkage using SLK-581

### Librarian team process

- (a) Each Source Linkage Data File will be provided to the Librarian team, which will conduct checks for extra variables or data that should not be included in the data file (e.g. other identifiers or extra data elements). As per standard ABS processes, if unsolicited data is found in the Source Linkage Data File, a sanitised version of the file will be created, which does not contain the unsolicited data, and the original file will be securely deleted from the file system and backups.
- (b) The Librarian team will:
  - (i) apply privacy measures to anonymise personal information. This will involve:
    - A. replacing the Source Record IDs with an Anonymised Record ID; and
    - B. encrypting SLK-581s; and
  - (ii) create a Concordance File, which shows how the Source Record IDs correspond to the Anonymised Record IDs. SLK-581 data will not be present in the Concordance File.
- (c) The cleaned, standardised and anonymised Source Linkage Data Files and Linkage Files (i.e. the encrypted SLK-581 and the Anonymised Record IDs) will then be provided to the Linker team. The Concordance File will be sent to the Assembler team.

### Linker team process

- (d) The Linker team will link the Linkage Files using the encrypted SLK-581. The resulting Linkage Results File will show Anonymised Record IDs corresponding to each encrypted SLK-581.<sup>8</sup>
- (e) The linking variable (encrypted SLK-581) will be removed from Linkage Results File before being passed to the Assembler team, so that the Assembler team will only receive a file with all linked Anonymised Record IDs.

### Assembler team process

- (f) The Assembler team cleans, prepares and treats the Source Analytical Data Files (which contain the analytical data elements and Source Record ID) to ensure they are fit for purpose and only contain the information that is relevant to the particular project proposal.

---

<sup>8</sup> For example, if there are three datasets being linked, the Linkage Results File would comprise: (a) one column for each encrypted SLK-581; and (b) one column for each of the datasets (with the Anonymised Record ID for the relevant dataset appearing in their respective column).

- (g) The Assembler team will use the Concordance File to replace the Anonymised Record IDs on the Linkage Results File with Source Record IDs. The Assembler team then assembles the Output Files using the cleaned Source Analytical Data Files and the Linkage Results File with Source Record IDs.
- (h) At this point, the Assembler team will remove the Source Record ID and assign an Analysis ID<sup>9</sup> (a randomly generated synthetic ID) for each Output File.
- (i) The Output Files will be subject to another round of checks conducted by the Microdata Resource team. These are final checks to ensure that the data has been assembled correctly (based on agreed project proposal specifications) and there is no identifiable information remaining on the file.

### 3.6 Release of de-identified data to approved researchers through the DataLab (out of scope)

- (a) The Australian Statistician or delegate will provide their written approval to release the unit record information to the researchers once the appropriate legal and ABS policy conditions are met. The researchers will access and analyse the information in the secure DataLab environment.
- (b) The Microdata Resource team will only then transfer the data that is required to meet the requirements of an approved project proposal into the DataLab.
- (c) As part of standard ABS data integration and DataLab procedures, researchers can only access the data if they have been approved to access it in accordance with source data custodian requirements. In order to gain access to the data (also known as microdata), researchers are required to register and submit a project proposal via myDATA to the ABS.
- (d) In addition to having their project approved, researchers complete 'safe researcher' training and complete all relevant undertakings and declarations of compliance, before being able to access data in the DataLab. For the CJDA, access will be limited to researchers in Australia.

### 3.7 Output of aggregated data/analysis from the DataLab (out of scope)

- (a) The results of the compilation and analysis of the individual statistical records will only be output from the secure DataLab environment where the ABS has provided approval for that output. Aggregated data and/or analysis outputs can only be output from the DataLab in accordance with the project proposal.
- (b) All analysis will be checked by the ABS before output from the DataLab, to ensure that no particular person can be identified. These checks include requiring a minimum number of contributors per cell at the person level to prevent the possibility of identification.

---

<sup>9</sup> The Analysis IDs are applied after the datasets have been assembled so there is only one row per person. The ID given to each row is the Analysis ID – so it effectively replaces the linkage variable between datasets.

## 4. Relevant personal and protected information

### 4.1 What is personal information and sensitive information?

- (a) The APPs impose obligations on APP entities in relation to the collection, storage, use and disclosure of personal information, with additional requirements relating to handling 'sensitive information'.
- (b) Under the Privacy Act, personal information means *'information or an opinion about an identified individual, or an individual who is reasonably identifiable, whether the information is true or not, and whether the information or opinion is recorded in a material form or not.'*<sup>10</sup>
- (c) 'Sensitive information' is a sub-category of personal information, and is defined in section 6(1) of the Privacy Act as meaning:
  - (i) information or an opinion about an individual's:
    - A. racial or ethnic origin;
    - B. political opinions;
    - C. membership of a political association;
    - D. religious beliefs or affiliations;
    - E. philosophical beliefs;
    - F. membership of a professional or trade association;
    - G. membership of a trade union;
    - H. sexual orientation or practices; or
    - I. criminal record;that is also personal information;
  - (ii) health information about an individual;
  - (iii) genetic information about an individual that is not otherwise health information;
  - (iv) biometric information that is to be used for the purpose of automated biometric verification or biometric identification; or
  - (v) biometric templates.
- (d) Whether an individual is 'reasonably identifiable' from information needs to be considered in context and having regard to the circumstances. Relevant considerations include:

---

<sup>10</sup> Privacy Act, s 6(1) (definition of 'personal information').

- (i) the nature and amount of the information;
- (ii) the circumstances of its receipt;
- (iii) who will have access to the information;
- (iv) other information that is available to the entity that holds the information, and the practicability of using that information to identify an individual; and
- (v) if the information is publicly released, whether a reasonable member of the public who accesses that information would be able to identify the individual.<sup>11</sup>

## 4.2 Personal information involved in the Project

- (a) The Project will involve the handling of the following information:
  - (i) information about individuals who have had interactions with police, criminal courts and/or corrective services, including:
    - A. personal information (e.g. age, sex, and country of birth); and
    - B. sensitive information, namely, information about an individual's criminal record (e.g. offence and sentence), and racial or ethnic origin (e.g. Indigenous status); and
  - (ii) information about researchers seeking to access the DataLab, including:
    - A. name and contact details;
    - B. employer;
    - C. skills and qualifications; and
    - D. conflicts of interest related to the data.
- (b) Information about individuals who have had interactions with police, criminal courts and/or corrective services will be sourced from police, criminal courts and corrections data custodians. A complete list of data custodians is set out in Schedule 1, and a complete list of data elements is set out in Schedule 3.
- (c) The name and employer of each researcher is generally collected from the lead researcher who completes the project proposal. All other information about researchers is collected directly from the individual researchers themselves.
- (d) The third column of the table in Schedule 1 identifies information flows involving the handling of personal and sensitive information.

---

<sup>11</sup> APP Guidelines, paragraph B.91.

### 4.3 Protected information involved in the Project

- (a) The Project will involve the handling (i.e. divulgence and communication) of statistical information about individuals who have had interactions with police, criminal courts and/or corrective services. This information is protected by section 19 of the C&S Act (**protected information**), being '*information given under [the C&S] Act*'. As noted above, section 9 of the C&S Act provides that the Australian Statistician may collect statistical information in relation to prescribed matters, including, relevantly for this Project, statistical information in relation to crime.<sup>12</sup> For the purpose of the Project, we understand that the ABS will collect statistical information under section 9 of the C&S Act and regulation 13 (item 11) of the C&S Regulations.
- (b) The fourth column of the table in Schedule 1 identifies information flows involving the handling of protected information.

---

<sup>12</sup> C&S Regulations, regulation 13, item 11.

## 5. Secrecy compliance assessment

- (a) All data provided to the ABS is considered protected information under the C&S Act. Therefore, the handling of data in this Project will involve the handling of data that is subject to the protections under that Act, specifically, unit record level information about individuals who have had interactions with police, criminal courts and/or corrective services.
- (b) Section 19 of the C&S Act provides that a person commits an offence if:
  - (i) the person is, or has been, the Australian Statistician or an officer; and
  - (ii) the person, either directly or indirectly, divulges or communicates to another person (other than the person from whom the information was obtained) any information given under the C&S Act.
- (c) However, it is not an offence for a person to divulge or communicate information given under the C&S Act:
  - (i) in accordance with a determination under section 13; or
  - (ii) for the purposes of the C&S Act.
- (d) The Project will involve:
  - (i) the communication of protected information when the ABS receives, cleans and integrates data, via the Librarian, Linker and Assembler Teams; and
  - (ii) the divulgence of information when:
    - A. the ABS discloses linked de-identified data to approved researchers in the DataLab; and
    - B. aggregated data/analysis are output from the DataLab, as per standard ABS processes.
- (e) In our view, the communication of information (as outlined above at paragraph 5(d)(i)) is for the purposes of the C&S Act, being for the purpose of linking police, criminal courts and corrective services data to create the CJDA. This can reasonably be characterised as involving the 'compiling' of statistical information for the purpose of section 12 of the C&S Act. On this basis, we consider that the communication of information (as outlined above) is permitted under subsection 19(2) of the C&S Act.
- (f) Section 6 of the C&S Determination provides that information provided to the Australian Statistician under the C&S Act may be disclosed if:
  - (i) the general requirements contained in Part 2 of the C&S Determination are satisfied in respect of the disclosure; and
  - (ii) the disclosure is permitted by a section of Part 3 of the C&S Determination.

- (g) We are instructed that the ABS will disclose information in accordance with section 15 of the C&S Determination (which is included in Part 3 of the C&S Determination).
- (h) Part 2 of the C&S Determination relevantly sets out the following requirements for a disclosure of information under the C&S Determination:
  - (i) the disclosure of information of a personal or domestic nature relating to an individual, is done in a manner that is not likely to enable the identification of an individual (section 7 of the C&S Determination); and
  - (ii) the Australian Statistician has approved the disclosure of the information in writing (section 8 of the C&S Determination).
- (i) We are instructed that data will be disclosed by the ABS in a manner that is not likely to enable the identification of individual persons, and that that re-identification risks will be managed by the ABS in the following ways:
  - (i) personal identifiers will be kept separately to other analytical information at all times during the linkage process, in accordance with the Separation Principle;
  - (ii) the Output Files will be subject to checks by the Microdata Release team, to ensure that there is no identifiable information in the Output Files before they are uploaded to the DataLab;
  - (iii) as part of the Five Safes Framework (and specifically, Safe Outputs), the ABS has a vetting team that will check all data for re-identification risks before the data is cleared for exit from the secure DataLab environment. This includes ensuring that the data meets certain confidentiality requirements, such as having a minimum number for contributors required for each cell or statistic;
  - (iv) the ABS will limit researchers' access to data based on the research question they are seeking to answer (i.e. not all data will be released to researchers);
  - (v) researchers will be required to undertake training and sign an undertaking that they will not use the data to try and identify particular individuals from the data;
  - (vi) the ABS will not approve research projects if data for small cohorts of individuals is requested; and
  - (vii) as a requirement of the C&S Determination (section 15) and in accordance with the ABS Data Integration Principles, data will not be permitted to be used for compliance purposes.
- (j) Notwithstanding the above measures, we note that some stakeholders have expressed concerns that there may be re-identification risks that could arise in the context of the Project. We consider that risks of re-identification could potentially increase over time, as data is added to the CJDA on an annual basis (and also if CJDA data is linked with other datasets in the future).

- (k) In general, information will be considered to be 'de-identified' where the risk of an individual being re-identified in the data is 'very low' or where there is 'no reasonable likelihood of re-identification occurring'.<sup>13</sup> The OAIC has issued guidance on de-identification ([De-Identification and the Privacy Act](#)), which states that a de-identification process generally includes two steps:
- (i) the removal of direct identifiers, such as an individual's name, address or other directly identifying information; and
  - (ii) one or both of the following additional steps:
    - A. removing or altering other information that may allow an individual to be identified (for example, because of a rare characteristic of the individual or a combination of unique or remarkable characteristics that enable identification); and/or
    - B. putting controls and safeguards in place in the data access environment, which will appropriately manage the risk of re-identification.
- (l) We are instructed that information for analysis will be de-identified in accordance with the conditions outlined in the C&S Determination.
- (m) To support compliance with section 7 of the C&S Determination, we recommend that the ABS periodically review the efficacy of the measures that the ABS has in place to manage the risks of re-identification in the context of the Project, noting that re-identification risks can potentially change and increase over time (**Recommendation 1**). These periodic reviews should consider:
- (i) the kind of information that is made available to researchers through the DataLab (and whether individuals may be identifiable due to unique or rare characteristics that enable identification);
  - (ii) the kind of information that is permitted to be released from the DataLab; and
  - (iii) the controls and safeguards that are in place in the DataLab, to manage the risk of re-identification.

---

<sup>13</sup> OAIC, *De-identification and the Privacy Act*, 21 March 2018.

<p><b>Recommendation 1: Re-identification risk management</b></p>	<p>We recommend that the ABS periodically review the efficacy of the measures that the ABS has in place to manage the risks of re-identification (including any changed or increased risks over time) in the context of the Project. These periodic reviews should consider:</p> <ul style="list-style-type: none"> <li>• the kind of information that is made available to researchers through the DataLab (and whether individuals may be identifiable due to unique or uncommon characteristics that enable identification;</li> <li>• the kind of information that is permitted to be released from the DataLab; and</li> <li>• the controls and safeguards that are in place in the DataLab, to manage re-identification risks.</li> </ul>
---	---

## 6. Privacy (APP) compliance assessment

### 6.1 APP 1: Open and transparent management of personal information

- (a) APP 1 imposes obligations on APP entities to:
  - (i) take reasonable steps to implement practices, procedures and systems that will ensure the agency complies with the APPs and any binding registered APP code, and is able to deal with privacy complaints and inquiries (APP 1.2);
  - (ii) have a clearly expressed and up to date APP privacy policy about how the agency manages personal information (APPs 1.3 and 1.4); and
  - (iii) take reasonable steps to make the agency's privacy policy available free of charge (APPs 1.5 and 1.6).
- (b) This principle is aimed at increasing transparency and accountability by agencies for their personal information handling practices, and in doing so, building community trust and confidence in those practices.<sup>14</sup>

#### **Practices, procedures and systems to ensure APP compliance**

##### ***APS Privacy Governance Code and PIAs***

- (c) A PIA is a process to identify and assess APP compliance risks, and strategies to mitigate those risks. Undertaking this PIA is therefore a reasonable step to ensure that the Project is implemented in a way that complies with the APPs.
- (d) We also consider that the conduct of a PIA for the Project is consistent with the ABS' obligations under section 12 of the APS Privacy Governance Code. This provision requires an agency to conduct a PIA for all 'high privacy risk projects', being a project that involves any new or changed ways of handling personal information that are likely to have a significant impact on the privacy of individuals. The Project would be considered a 'high privacy risk project' subject to PIA requirements on the basis that it involves new or changed ways of collecting and using personal information (including sensitive information) about individuals who have had interactions with police, criminal courts and corrective services agencies.
- (e) We note that, in accordance with section 15 of the APS Privacy Governance Code, the ABS is required to include this PIA in its public facing PIA register.
- (f) Section 13 of the APS Privacy Governance Code provides that an agency may publish a PIA, or a summary version or edited copy of the PIA, on its website. While this is not a mandatory requirement, doing so can assist in promoting transparency around the information handling practices involved in the Project, as well as building public confidence in the ABS' approach to privacy protection.

---

<sup>14</sup> APP Guidelines, paragraph 1.1.

### ***Ongoing privacy review and risk management***

- (g) A PIA is a point-in-time assessment, based on the proposed project implementation approach and information flows known at the time of preparation. This PIA is based on the information flows identified in Schedule 1.
- (h) If there are any material changes to the information flows identified in Schedule 1 (i.e. changes that may raise additional privacy issues or impacts, or increased levels of privacy risk), we recommend that the ABS undertake a privacy threshold assessment (**PTA**) and, if required, further assessment of privacy impacts and compliance risks (which could be in the form of a supplementary PIA). A further secrecy compliance assessment should also be undertaken if necessary, and to the extent that there are any new or material changes to the protected information flows identified in Schedule 1 (**Recommendation 2**).
- (i) Once the Project is operational, it is possible that unanticipated privacy issues (either or both in relation to privacy compliance, and community expectations or concerns) may arise. To ensure that the Project is operating as intended and privacy issues are being appropriately managed, and to ensure ongoing APP compliance, we recommend that the Project be reviewed periodically (**Recommendation 3**).
- (j) Conducting reviews can assist in identifying any unintended or unanticipated privacy issues. It can also provide an opportunity for the ABS to review and refine data handling practices, including:
  - (i) the extent to which the collection and use of personal information is reasonably necessary in order to administer the Project; and
  - (ii) the assessment and management of re-identification risks (see also **Recommendation 1**).

### ***Data sharing arrangements with source data custodians***

- (k) To ensure there are clear privacy and data governance arrangements in place with State and Territory source data custodians, we consider there should be written data sharing agreements in place with each source data custodian for the Project. In this regard, we are instructed that the ABS proposes to enter into a Memorandum of Understanding (**MOU**) with each State and Territory source data custodian for the purpose of the Project.
- (l) We have been provided with a working draft version of an MOU which is still in the process of development. Relevantly, the draft MOU provides that:
  - (i) the parties '*acknowledge and will comply with their obligations under the Privacy Act 1988 (Cth) ... in relation to the handling of Personal Information under this MoU, including the Australian Privacy Principles*' (clause 8.1);
  - (ii) if a party receives a complaint alleging an interference with the privacy of an individual by the other party arising out of the operations of the MOU:

- A. the party receiving the complaint will immediately notify the other party of the nature of that complaint, and such details of that complaint as are necessary to minimise any (or further) interference; and
  - B. each party is to keep the other party informed as to the progress of the complaint as it relates to the other's actions in connection with the allegation of interference (clause 8.2);
- (iii) if the Privacy Commissioner directs a party to take particular action concerning the handling of Personal Information, the other party will cooperate with any reasonable request of that party to enable the party to comply with the Privacy Commissioner's direction (clause 8.3); and
- (iv) where additional state or territory privacy legislation applies, the ABS will work with the Data Custodians to ensure compliance (clause 8.4).
- (m) We understand the intent of clause 8.1 of the draft MOU is to require the parties (i.e. the ABS, and State and Territory source data custodians) to comply with the Privacy Act. As noted above, State and Territory source data custodians are not legally bound by the Commonwealth Privacy Act, and instead are subject to applicable privacy laws in their own jurisdiction.
- (n) To support compliance with APP 1.2 by the ABS, we recommend that the MOUs between the ABS and each source data custodian address the following matters, at a minimum (**Recommendation 4**):
  - (i) the data that the relevant source data custodian will provide to the ABS;
  - (ii) the purpose for which the source data custodian will provide the relevant data to the ABS, and the purposes for which the ABS may use and disclose that data;
  - (iii) the legal authority under which each party will collect, use and disclose the relevant data;
  - (iv) arrangements and requirements relating to the secure transfer and storage of data;
  - (v) each party's obligations with respect to:
    - A. compliance with privacy laws, namely:
      - 1) for the ABS – the Commonwealth Privacy Act and APPs; and
      - 2) for source data custodians – the Commonwealth Privacy Act and APPs, or an equivalent privacy law that binds the data custodian in their jurisdiction;
    - B. compliance with other relevant legislation that may apply to the data provided by the data custodian (e.g. secrecy provisions in legislation); and

- C. where necessary, obtaining their own legal advice and undertaking their own privacy risk assessments in relation to the Project prior to the commencement of the data sharing;
- (vi) obligations and processes relating to the notification and handling of data breaches and privacy complaints.

***Other data governance arrangements***

- (o) To assist in the governance of the CJDA, the ABS has formed the Joint Boards of Management (**Joint Boards**). The Joint Boards include:
  - (i) representatives from each of the National Crime Statistics Unit Board of Management, the National Criminal Courts Statistics Unit Board of Management, and the National Corrective Services Statistics Unit Board of Management, which comprise representatives from the State and Territory data custodians for the CJDA; and
  - (ii) an ABS representative.
- (p) The Joint Boards will oversee the strategic direction of the CJDA and will help to facilitate project approvals once the CJDA is operational.
- (q) During stakeholder consultations for the Project, stakeholders highlighted the importance of ensuring that the ABS' governance arrangements considered the perspectives of individuals who were directly affected by the Project or who might otherwise bring different perspectives to issues such as the protection of privacy or governance for Aboriginal and Torres Strait Islander data. Moreover, Aboriginal and Torres Strait Islander representatives recommended that ethics and cultural safety frameworks be implemented in CJDA projects, such as the Australian Institute of Aboriginal and Torres Strait Islander Studies (**AIATSIS**) Code of Ethics for Aboriginal and Torres Strait Islander Research.
- (r) Aboriginal and Torres Strait Islander representatives also highlighted the importance of presenting the data in a culturally appropriate manner and the importance of moving away from 'deficit' narratives.
- (s) We are instructed that, as part of the governance framework for the CJDA, separate PIAs may be required for individual research projects, depending on their nature and risk rating. Where a separate PIA is conducted, consultations with stakeholders will be undertaken as part of the process, to ensure that community expectations inform the risk analysis and recommendations for the PIA. We consider that the conduct of separate PIAs for individual research projects using data from the CJDA will help to support the ABS' compliance with APP 1.
- (t) To enhance the ABS' data governance arrangements, in line with community expectations, we recommend that the ABS embed and operationalise best practice for the governance of Aboriginal and Torres Strait Islander data into the Project (**Recommendation 5**).
- (u) These principles are outlined in the National Indigenous Australians Agency's [\*Framework for Governance of Indigenous Data\*](#).

## Privacy complaints and enquiries

- (v) As indicated in the [ABS Privacy Policy for Statistical Information](#), and the [ABS Privacy Policy for Managing and Operating our Business](#), the ABS has existing mechanisms and processes for receiving and dealing with privacy complaints and enquiries. We are instructed that these will apply in relation to any privacy related complaints or enquiries that arise in connection with the Project.

## Privacy policy

- (w) An APP privacy policy is intended to outline the key purposes for which personal information is collected, held, used and disclosed. It does not necessarily need to detail each information handling practice of an agency but is required to address certain matters relating to the management of personal information. A privacy policy is different to an APP 5 collection notice, which is required to provide more detailed information about a particular collection of personal information.
- (x) The ABS has two privacy policies (identified above) which are published on its website and which describes how, and the purposes for which, the ABS collects, uses and discloses personal information.
- (y) Relevant to the ABS' handling of personal information about individuals who have had interactions with police, criminal courts and corrective services agencies, the ABS Privacy Policy for Statistical Information addresses the following matters:
  - (i) the kinds of personal information that the ABS collects and holds, including demographic information (e.g. age and sex), personal characteristics, personal identifiers, and sensitive information (e.g. racial or ethnic origin, and criminal record);
  - (ii) how the ABS collects personal information, including by collecting information from data custodians that make their data available to ABS;
  - (iii) how the ABS holds personal information, including that the ABS secures all information in accordance with the Protective Security Policy Framework (**PSPF**);
  - (iv) the purposes for which the ABS collects, holds, uses and discloses personal information, namely to perform the ABS' work under the C&S Act, including data integration;
  - (v) how an individual may access or seek the correction of their personal information; and
  - (vi) how an individual may make a privacy complaint and how the ABS deals with privacy complaints.<sup>15</sup>
- (z) Relevant to the ABS' handling of researchers' personal information for the purpose of the Project, the ABS' 'Privacy Policy for Managing and Operating Our Business' addresses the following matters:

---

<sup>15</sup> [ABS Privacy Policy for Statistical Information | Australian Bureau of Statistics](#).

- (i) the kinds of personal information that the ABS collects and holds, including name, contact details, employment information, and details of personal interests supplied for the purpose of managing conflicts of interest;
  - (ii) how the ABS collects personal information, namely, that the ABS collects personal information from individuals when they use ABS services;
  - (iii) how the ABS holds personal information, including that the ABS secures all information in accordance with the PSPF;
  - (iv) the purposes for which the ABS collects, holds, uses and discloses personal information, including to assess requests to use ABS products, such as the DataLab;
  - (v) how an individual may access or seek the correction of their personal information; and
  - (vi) how an individual may make a privacy complaint and how the ABS deals with privacy complaints.<sup>16</sup>
- (aa) For the purposes of meeting its obligations under APPs 1.3 and 1.4, we consider that the ABS' privacy policy contains sufficient information relevant to the handling of personal information by the ABS in the context of the Project.

<p><b>Recommendation 2:</b></p> <p><b>Further privacy risk assessments</b></p>	<p>If there are any new or material changes to the information flows identified in Schedule 1, including:</p> <ul style="list-style-type: none"> <li>• the collection of additional types of personal information;</li> <li>• additional or changed uses of personal information not identified in Schedule 1;</li> <li>• the sharing of personal information with third parties not identified in Schedules 1 or 3; or</li> <li>• as a result of changes to the Project and/or the way in which it is administered,</li> </ul> <p>a privacy threshold assessment and, if required, further assessment of privacy impacts and compliance risks, should be undertaken (which could be in the form of a supplementary PIA.</p> <p>The assessment(s) should consider privacy impacts from both privacy law compliance and community expectations perspectives.</p> <p>A further secrecy compliance assessment should also be undertaken, as necessary and to the extent that there are any new or material changes to the protected information flows identified in Schedule 1.</p>
--	--

<sup>16</sup> [ABS Privacy Policy for Managing and Operating Our Business | Australian Bureau of Statistics.](#)

<p><b>Recommendation 3:</b> <b>Periodic reviews</b></p>	<p>We recommend that the ABS periodically review the operation of the Project to ensure:</p> <ul style="list-style-type: none"> <li>• methods for handling personal information remain appropriate, and align with community expectations;</li> <li>• ongoing APP compliance; and</li> </ul> <p>opportunities to refine data handling practices and maximise privacy protection can be identified and implemented.</p>
<p><b>Recommendation 4:</b> <b>Data sharing agreements with source data custodians</b></p>	<p>We recommend ensuring that the terms of each MOU (or other form of data sharing agreement) between the ABS and each source data custodian address the following matters:</p> <ul style="list-style-type: none"> <li>• the that the source data custodian will provide to the ABS;</li> <li>• the purpose for which the data custodian will provide the relevant data to the ABS, and the purposes for which the ABS may use and disclose that data;</li> <li>• the legal authority under which each party will collect, use and disclose the relevant data;</li> <li>• arrangements and requirements relating to the secure transfer/sharing and storage of data;</li> <li>• each party's obligations with respect to: <ul style="list-style-type: none"> <li>○ compliance with applicable privacy laws, namely: <ul style="list-style-type: none"> <li>▪ for the ABS – the Commonwealth Privacy Act and APPs; and</li> <li>▪ for data custodians – the Commonwealth Privacy Act and APPs, or an equivalent privacy law that binds the data custodian in their jurisdiction;</li> </ul> </li> <li>○ compliance with other relevant legislation that may apply to the data provided by the data custodian (e.g. secrecy provisions in legislation); and</li> <li>○ where necessary, obtaining their own legal advice and undertaking their own PIAs (or other form of privacy risk assessments) prior to sharing any data;</li> </ul> </li> <li>• obligations and processes relating to the notification and handling of data breaches and privacy complaints.</li> </ul>
<p><b>Recommendation 5:</b> <b>Governance of Indigenous Data</b></p>	<p>We recommend that the ABS embed and operationalise best practice for the governance of Aboriginal and Torres Strait Islander data into the CJDA. These principles are outlined in the National Indigenous Australians Agency's <a href="#">Framework for Governance of Indigenous Data</a>.</p>

## 6.2 APP 2: Anonymity and pseudonymity

- (a) APP 2 provides that 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 unless:
  - (i) the APP entity is required or authorised by law to deal with identifiable individuals; or
  - (ii) it is impracticable for the APP entity to deal with individuals on an anonymous or pseudonymous basis.
- (b) A person deals anonymously with an APP entity where they do not provide any personal information or identifiers, meaning that the APP entity is not able to identify the individual at the time of the dealing or subsequently.<sup>17</sup> A person deals pseudonymously with an APP entity where they use a name, term or descriptor that is different to their actual name (such as a username or an email address that does not contain the person's actual name).<sup>18</sup> APP 2 requires that both options be made available to individuals unless an exception applies.<sup>19</sup>
- (c) Anonymity and pseudonymity are important privacy concepts because they enable individuals to exercise greater control over their personal information and decide how much personal information will be shared or revealed to others.<sup>20</sup>
- (d) In our view, it is reasonably arguable that individuals who have had interactions with police, criminal courts and corrective services agencies (and whose data is collected by the ABS) will not be 'dealing with' the ABS in the context of the Project. This is because these individuals will not have any interaction with the ABS in the context of the Project. As noted above, data about these individuals will be collected by the ABS from police, criminal courts and corrective services data custodians. On that basis, APP 2 would not be applicable in the circumstances.
- (e) Even if individuals were considered to be 'dealing with' the ABS for the purposes of APP 2 (albeit indirectly, by virtue of the ABS' collection of data about these individuals), we consider that:
  - (i) it is impracticable for the ABS to deal with these individuals on an anonymous basis (that is, without any personal information or identifiers). This is because it would not be possible or practicable for the ABS to link police, criminal courts and corrections datasets without any personal information or identifiers. Therefore, the exception under APP 2.2(b) would apply; and

---

<sup>17</sup> APP Guidelines, paragraph 2.4.

<sup>18</sup> APP Guidelines, paragraph 2.6.

<sup>19</sup> APP Guidelines, paragraph 2.3.

<sup>20</sup> APP Guidelines, paragraph 2.9.

- (ii) the ABS will be dealing with these individuals on a pseudonymous basis, by using 'a name, term or descriptor that is different from the person's actual name' (i.e. SLK-581), consistent with APP 2.<sup>21</sup>

### 6.3 APP 3: Collection of personal information

- (a) APP 3 applies where an APP entity seeks to collect solicited personal information. Under APP 3, an agency must:
  - (i) only collect personal information (other than sensitive information) if it is reasonably necessary for, or directly related to, one or more of the agency's functions or activities (APP 3.1);
  - (ii) only collect sensitive information if:
    - A. the individual consents, and the information is reasonably necessary for, or directly related to, the agency's functions or activities (APP 3.3); or
    - B. an exception in APP 3.4 applies, which includes where the collection is required or authorised by law (APP 3.4(a));
  - (iii) collect personal information only by lawful and fair means (APP 3.5); and
  - (iv) only collect personal information directly from the individual, except if the individual consents to the collection from a third party, or another exception applies (APP 3.6), including where the third party collection is authorised or required by law (APP 3.6(a)(ii)).

#### APP 3.1: Collection of non-sensitive personal information

- (b) The Project will involve the collection of personal information about individuals who have had interactions with police, criminal courts and corrective services agencies, including:
  - (i) age (or year of birth);
  - (ii) sex;
  - (iii) state; and
  - (iv) country of birth.
- (c) A complete list of data elements is set out in Schedule 3. In our view, the collection of this data is reasonably necessary for the ABS' activities in undertaking data linkage to create the CJDA. Therefore, we consider that the collection of this information is consistent with APP 3.1.

---

<sup>21</sup> APP Guidelines, paragraph 2.6.

### **APP 3.3: Collection of sensitive information**

- (d) The Project will involve the collection of the following sensitive information about individuals who have had interactions with police, criminal courts and corrective services agencies:
  - (i) Indigenous status; and
  - (ii) criminal record, including offence and sentence.
- (e) A complete list of data elements is set out in Schedule 3.
- (f) In our view, the collection of sensitive information by the ABS will be authorised by section 9 of the C&S Act and regulation 13 (items 11 and 13) of the C&S Regulations. As noted above, section 9 of the C&S Act provides that the Australian Statistician may, from time to time, collect such statistical information in relation to prescribed matters as they consider appropriate. 'Crime' and 'Population and the social, economic and demographic characteristics of the population' are matters prescribed under regulation 13 (items 11 and 38) of the C&S Regulations. In these circumstances, we consider that the ABS' collection of sensitive information will be authorised by law, consistent with APP 3.4(a).

### **APP 3.5: Lawful and fair collection**

- (g) For the purposes of APP 3.5, a collection that is lawful and fair is one that:
  - (i) is not unlawful; and
  - (ii) does not involve intimidation or deception, and is not unreasonably intrusive.<sup>22</sup>
- (h) In the circumstances outlined above, we consider that the ABS' collection of personal information about individuals who have had interactions with police, criminal courts and corrective services agencies is lawful and fair, consistent with APP 3.5. In reaching this view, we note that the ABS will not collect any direct identifiers about individuals (such as name or address). As noted above, the ABS will use SLK-581 as a statistical linkage key, which is less directly identifying of a person than their name or address. We also refer to **Recommendation 4** in relation to ensuring the MOUs between the ABS and each data custodian address the legal authority under which the data custodian will lawfully provide data to the ABS. In our view, these measures will support compliance with APP 3.5.

### **APP 3.6: Direct collection**

- (i) The Project will involve the indirect collection of personal information about individuals who have had interactions with police, criminal courts and corrective services agencies. As noted above, this data will be collected by the ABS from source data custodians, and not directly from the individuals themselves.
- (j) In our view, it would be unreasonable or impracticable for the ABS to collect this data directly from individuals themselves, in circumstances where the ABS does not have any direct contact with individuals who have had interactions with police,

---

<sup>22</sup> APP Guidelines, paragraphs 3.60–3.63.

criminal courts and corrective services agencies across Australia (and in circumstances where it would not be reasonable or practicable for the ABS to make contact with these individuals). Therefore, we consider that the exception under APP 3.6(b) would apply.

## 6.4 APP 4: Dealing with unsolicited information

- (a) 'Unsolicited personal information' is information that an APP entity receives but has not 'solicited'.<sup>23</sup> An APP entity 'solicits' personal information if the entity requests another entity to provide the personal information, or to provide a kind of information in which that personal information is included.<sup>24</sup>
- (b) If an APP entity receives unsolicited personal information, it must determine whether it would have been permitted to collect the information under APP 3. If the information could not have been collected under APP 3, and the information is not contained in a Commonwealth record, the APP entity will need to destroy or de-identify that information as soon as practicable, but only if it is lawful and reasonable to do so.
- (c) In the context of the Project, it is possible that the ABS may receive unsolicited personal information from source data custodians. As noted above, if unsolicited data is found in a Source Linkage Data File, the Librarian team will create a sanitised version of the file, which does not contain the unsolicited data, and the original file will be securely deleted from the file system and backups.
- (d) In our view, unsolicited data received by the ABS will be contained in a 'Commonwealth record', being a record that is the property of the Commonwealth or of a Commonwealth institution.<sup>25</sup> Therefore, the requirement under APP 4.3 will not apply to the unsolicited data. Instead, the ABS will be required to deal with the unsolicited data in accordance with the *Archives Act 1983* (Cth) (**Archives Act**).<sup>26</sup>
- (e) We are instructed that the ABS has received advice that the deletion of the source linkage or analysis data files (in circumstances where it contains unsolicited data) is consistent with the requirements of the Archives Act. We have therefore not assessed compliance with the Archives Act for the purpose of this PIA.
- (f) We refer to **Recommendation 4** in relation to ensuring the MOUs between the ABS and each source data custodian, specify the relevant data that the source data custodian is to provide to the ABS. We consider implementing this recommendation would assist in mitigating against the risk of the ABS being provided with, and collecting, more information than it requires for the Project.

---

<sup>23</sup> APP Guidelines, paragraph 4.5.

<sup>24</sup> Privacy Act, subsection 6(1).

<sup>25</sup> Privacy Act, subsection 6(1); *Archives Act 1983* (Cth), subsection 3(1).

<sup>26</sup> APP Guidelines, paragraph 4.16.

## 6.5 APP 5: Collection notice and transparency

- (a) APP 5 requires APP entities to take reasonable steps to notify or ensure an individual is aware of certain matters at the time that it collects their personal information or, if that is not practicable, then as soon as practicable after the collection. The matters in APP 5.2 include the following:
  - (i) the identity and contact details of the entity;
  - (ii) the fact and circumstances of collection;
  - (iii) the purpose(s) of collection;
  - (iv) any third parties, or the types of third parties, to which the entity usually discloses personal information of the kind collected by the entity;
  - (v) whether the entity is likely to disclose personal information to overseas recipients; and
  - (vi) information about the entity's privacy policy, including the fact that the privacy policy contains information about how an individual can request access to or correction of their personal information, and how they can make a privacy complaint.
- (b) The 'reasonable steps' that an entity should take to comply with APP 5 depends on the circumstances, which include:
  - (i) the sensitivity of the information, with more rigorous steps being likely required when collecting 'sensitive information' (e.g. health information), or information of a sensitive nature;
  - (ii) the possible adverse consequences for the individual if they are not made aware of matters relating to the collection of their information;
  - (iii) any special needs of the individual; and
  - (iv) the practicability of giving an APP 5 notice, including time and cost involved (i.e. whether the burden would be excessive in all the circumstances, noting that an entity is not excused from taking particular steps merely because it would be inconvenient, time-consuming or impose some cost).<sup>27</sup>
- (c) Like privacy policies, collection notices provide clarity and transparency to individuals in relation to the handling of their personal information.
- (d) The 'reasonable steps' qualification in APP 5.1 acknowledges that it may be reasonable for an APP entity to not take any steps to provide a notice or ensure awareness of all or some of the APP matters, such as where:
  - (i) the individual is aware that personal information is being collected, the purpose of collection and other relevant APP 5 matters;

---

<sup>27</sup> APP Guidelines, paragraph 5.4.

- (ii) an entity collects personal information from an individual on a recurring basis in relation to the same matter; or
  - (iii) the privacy benefit would be outweighed by the impracticability of notification.<sup>28</sup>
- (e) We understand that it will not be practicable for the ABS to provide a collection notice to individuals who have had interactions with police, criminal courts and corrective services agencies, in circumstances where the ABS will not have any direct contact or interaction with these individuals. In these circumstances, we consider it arguable that the obligation to take 'reasonable steps' under APP 5 does not require the ABS to provide a collection notice to these individuals.
- (f) Nonetheless, to support compliance with APP 5, we recommend that the ABS liaise with source data custodians to develop a strategy that supports transparency around the use of individual data for statistical purposes, including data integration. This strategy should aim to ensure that relevant individuals are informed about how their data is being collected and used, the purposes of data integration, and the measures in place to protect their privacy (**Recommendation 6**).

<b>Recommendation 6: Transparency and notification</b>	We recommend that the ABS liaise with source data custodians to develop a strategy that supports transparency around the use of individual data for statistical purposes, including data integration. This strategy should aim to ensure that relevant individuals are informed about how their data is being collected and used, the purposes of data integration, and the measures in place to protect their privacy.
--	---

## 6.6 APP 6: Use and disclosure of personal information

- (a) Under APP 6, personal information collected for a particular purpose (primary purpose) must not be used or disclosed for another purpose (secondary purpose) unless the individual has given consent, or an exception in APP 6.2 applies. These exceptions include where the use or disclosure is required or authorised by law (APP 6.2(b)).

### Uses of personal information

- (b) In the context of the Project, the ABS will use personal information about individuals who have had interactions with police, criminal courts and corrective services agencies:
- (i) when the ABS National Centre for Crime and Justice Statistics (**NCCJS**) and Librarian teams clean and prepare source data files for linkage;
  - (ii) when the ABS Linker team links the data;
  - (iii) when the ABS Assembler team assembles the data; and

<sup>28</sup> APP Guidelines, paragraph 5.7.

- (iv) when the ABS Microdata Resource team undertakes final checks of the linked data to be transferred into the DataLab.
- (c) In our view, the purpose of the above uses of personal information is to create the CJDA, which is consistent with the primary purpose of collection, and therefore, consistent with APP 6.1.

#### Disclosures of personal information

- (d) As outlined in Part 5 of this PIA, the ABS has existing processes to ensure data is de-identified before being made available to researchers via the DataLab, consistent with the requirements of section 15 of the C&S Determination.
- (e) However, as also noted above, some stakeholders have expressed concerns that there may be risks of re-identification that could arise in the context of the Project. In this regard, we refer to **Recommendation 1**.

## 6.7 APP 10: Data quality

- (a) APP 10 requires the ABS to take reasonable steps to ensure that:
  - (i) the personal information collected by the agency is accurate, up to date and complete (APP 10.1); and
  - (ii) the personal information that the agency uses or discloses is (having regard to the purpose of the use or disclosure) accurate, up to date, complete and relevant (APP 10.2).
- (b) What constitutes 'reasonable steps' will depend on the particular circumstances, having regard to the following factors:
  - (i) the sensitivity of the information;
  - (ii) the nature of the entity holding the information;
  - (iii) the possible adverse consequences for an individual if the quality of the information is not ensured, with more rigorous steps being more likely to be required as the risk of adversity increases; and
  - (iv) the practicability, including time and cost involved (i.e. whether the burden would be excessive in all the circumstances, noting that an entity is not excused from taking particular steps merely because it would be inconvenient, time-consuming or impose some cost).<sup>29</sup>
- (c) The data quality requirements in APP 10 are complemented by the obligations under APP 13.1, which requires an agency to take reasonable steps to correct personal information it holds either:
  - (i) in response to a request from an individual; or

---

<sup>29</sup> APP Guidelines, paragraph 10.6.

- (ii) on the agency's own initiative where it is satisfied that, having regard to the purpose for which the information is held, the information is inaccurate, out-of-date, incomplete, irrelevant or misleading.
- (d) The APP Guidelines note that taking reasonable steps to only handle 'high quality' personal information will 'build trust and confidence'.<sup>30</sup> Conversely, a loss of faith in the accuracy of data may adversely impact on public confidence in the ABS' processes and systems.
- (e) In the course of stakeholder consultations for the Project, stakeholders expressed concern about data quality, and in particular, the linking of individuals across datasets using SLK-581.
- (f) Stakeholders noted that individuals' names can change or an alias may be used. Further, in some cases, source data custodians may incorrectly record a person's name or date of birth. Where a person's name and/or date of birth are recorded incorrectly (or have changed), there may be two or more SLK-581s for one person, and the data relating to that person may not be correctly linked.
- (g) As noted above, we are instructed that the ABS has completed a Proof of Concept study for the CJDA, where the ABS used SLK-581 to link police, criminal courts and corrective services data, and the ABS has found that the SLK-581 is suitable for use as a statistical linkage key for the CJDA. We consider that the ABS' conduct of the Proof of Concept study is a 'reasonable step' for the purpose of APP 10.
- (h) Further, as noted above, the ABS proposes to enter into an MOU (or other form of data sharing agreement) with source data custodians, which will require the parties to acknowledge and comply with relevant privacy laws.<sup>31</sup> Subject to **Recommendation 4**, State and Territory source data custodians will therefore be expected to comply with data quality principles under applicable privacy laws in their jurisdiction, that are equivalent to APP 10. We consider that this is a further 'reasonable step' for the purposes of APP 10.
- (i) To further support compliance with APP 10, we recommend that the ABS periodically review the use of SLK-581 as a statistical linkage key, including whether it continues to be fit for purpose for the CJDA, having regard to data linkage results over time (**Recommendation 7**).

**Recommendation 7:  
Data quality and  
statistical linkage key**

We recommend that the ABS periodically review data quality, including the linkage methodology, to ensure that the data is fit for purpose for the Project.

<sup>30</sup> APP Guidelines, paragraph 10.3.

<sup>31</sup> Clause 8.1 of the draft MOU provided to us states that the parties will '*acknowledge and ... comply with their obligations under the Privacy Act 1988 (Cth) ... in relation to the handling of Personal Information under this MoU, including the Australian Privacy Principles*'.

## 6.8 APP 11: Data security

- (a) APP 11 requires the ABS to take reasonable steps to ensure that any personal information it holds is protected from misuse, interference and loss, and unauthorised access, modification or disclosure. The term 'holds' includes both physical possession, as well as circumstances where an agency has control over the information.
- (b) What constitutes 'reasonable steps' will depend on a number of factors, including the amount and sensitivity of the information. The level of data security required will generally become higher as the amount and/or sensitivity of the personal information held, or the consequences for an individual in the event of a data breach, increases.
- (c) The types of security measures that an agency could implement to meet its APP 11 obligations may include the following:
  - (i) governance, culture and training;
  - (ii) internal practices, procedures and systems;
  - (iii) ICT security;
  - (iv) access security;
  - (v) contractual obligations and arrangements with third party providers;
  - (vi) data breach response plan;
  - (vii) physical security;
  - (viii) destruction and de-identification of data; and
  - (ix) compliance with data security standards.<sup>32</sup>
- (d) We are instructed that the following measures are in place to protect the security of data in the context of the Project:
  - (i) in accordance with the Separation Principle, no individual can access both the identifying data used for linkage (i.e. SLK-581 linkage variable) and the analytical data (which does not contain any direct identifiers). ABS staff working on the Project will only have access to the information that they need to perform their assigned role;
  - (ii) the ABS will apply the 'Five Safes Framework' to manage disclosure risks, comprising Safe People, Safe Projects, Safe Settings, Safe Data and Safe Outputs;<sup>33</sup> and

---

<sup>32</sup> APP Guidelines, paragraph 11.8. See also the OAIC's *Guide to securing personal information*.

<sup>33</sup> [Five Safes framework | Australian Bureau of Statistics \(abs.gov.au\)](https://www.abs.gov.au/five-safes-framework).

- (iii) the ABS' data integration systems and processes conform to the Information Security Manual and the PSPF.<sup>34</sup>
- (e) Further, we are instructed that the following measures are in place to protect the security of data in the DataLab:
  - (i) data encryption at rest, to mitigate against unauthorised access to microdata;
  - (ii) Azure Storage Accounts to securely hold individual research products and allow querying from authorised users;
  - (iii) cloud servers (including back-up servers) hosted exclusively in Australia, with access only authorised for use in Australia, unless approved by the ABS;
  - (iv) closed network virtual machines to provide secure, isolated research spaces for the analysis of microdata;
  - (v) secure access through multi-factor authentication and workspace segmentation, which prevents data from being shared between research projects;
  - (vi) a DataLab Product Storage Account protected with Microsoft Defender, providing threat detection against malicious or unusual behaviour;
  - (vii) all researchers are required to complete training before accessing the DataLab;
  - (viii) researchers are also required to sign an undertaking that they will not share their login details for the DataLab; and
  - (ix) researchers will have access to linked data in the DataLab only for the duration of their project. Project proposals have a maximum two-year limit, following which researchers may apply for an extension.
- (f) Additionally, all ABS Librarian, Linker and Assembler activity occurs in an isolated IT environment – the ABS Secure Data Integration Environment (**SDIE**). We are instructed that:
  - (i) the SDIE has no external connectivity (i.e. no email, internet, etc) to mitigate risk of data exfiltration;
  - (ii) baseline security clearance is required to obtain access to the SDIE;
  - (iii) each functional role has separate access-controlled data holdings within the SDIE; and
  - (iv) the SDIE has undergone an assessment under the Information Security Registered Assessors Program (**IRAP**), and all ABS systems and procedures were certified as compliant under the Australian Government Information Security Manual (**ISM**).

---

<sup>34</sup> [Keeping integrated data safe | Australian Bureau of Statistics \(abs.gov.au\)](https://www.abs.gov.au/keeping-integrated-data-safe).

- (g) We consider that the above measures support the ABS' compliance with APP 11 in the context of the Project.

## 6.9 APPs 12 and 13: Data access and correction

- (a) Under APP 12, individuals must be given access to their own personal information (subject to certain exceptions).
- (b) APP 13 requires APP entities to take reasonable steps, on request by an individual, to correct any personal information they hold to ensure it is accurate, relevant, up to date, complete and not misleading, having regard to the purpose for which it is held.
- (c) The ABS privacy policies refers to existing personal information access and correction procedures.
- (d) In the context of this Project, we are instructed that:
  - (i) it would not be reasonably practicable for the ABS:
    - A. to identify data as it relates to a specific individual; or
    - B. even if this were possible, to correct data received from a source data custodian, having regard to the purpose for which it is collected and held by the ABS; and
  - (ii) any access or correction requests made by individual data subjects will be directed by the ABS to the relevant source data custodian(s).

## Schedule 1 — Information flows

Step	Description	Personal Information Flow	Protected Information Flow
<b>1. Data collection</b>			
<b>1(a)</b>	<p>The Project will involve the collection of data by the ABS, from police<sup>35</sup>, criminal courts<sup>36</sup> and corrective services<sup>37</sup> data custodians in each State and Territory.</p> <p>The two types of files received or created by the ABS (Source Analytical Data Files and Source Linkage Data Files) will be delivered and stored separately as part of the 'Separation Principle'.</p> <p>The Separation Principle means that no individual can access both the identifying data used for linkage (i.e. SLK-581 linkage variable) and the analytical data (which does not contain any direct identifiers)<sup>38</sup>. ABS staff working on the Project will only have access to the information that they need to perform their assigned role.</p> <p>The information that will be included in each of the Source Analytical Data Files and the Source Linkage Data Files is set out in Schedule 3.</p>	<p><b>APP 3</b></p> <p>ABS will <b>collect</b> personal information (including sensitive information) from data custodians.</p> <p><b>APP 6</b></p> <p>ABS will <b>use</b> personal information (including sensitive information) for a secondary purpose when as approved by data custodian such as data linking.</p>	<p>ABS will <b>collect</b> protected statistical information in accordance with C&amp;S Act and the C&amp;S Regulations.</p> <p>ABS will <b>communicate</b> (between ABS officers) protected statistical information for compilation and analysis purposes in accordance with the C&amp;S Act.</p>
<b>2. Librarian team processes</b>			
<b>2(a)</b>	Each Source Linkage Data File will be provided to the Librarian team, which will conduct checks for extra variables or data that should not be included in the data file (e.g. other identifiers or extra data elements).	<b>APP 6</b>	ABS will <b>communicate</b> (between ABS officers) protected statistical

<sup>35</sup> [Recorded Crime - Offenders, 2022-23 financial year | Australian Bureau of Statistics](#)

<sup>36</sup> [Criminal Courts, Australia, 2022-23 financial year | Australian Bureau of Statistics](#)

<sup>37</sup> [Prisoners in Australia, 2023 | Australian Bureau of Statistics](#)

<sup>38</sup> While the information in the analytical data does not contain any direct identifiers, we are instructed that spontaneous recognition could be possible if an ABS officer knew other information. For example, if they knew X was caught for Y offence on Z date and Y date and Z offence are contained in the file. ABS officers must sign an undertaking not to discuss/disclose personal information.

Step	Description	Personal Information Flow	Protected Information Flow
	As per standard ABS processes, if unsolicited data is found in the Source Linkage Data File, a sanitised version of the file will be created, which does not contain the unsolicited data, and the original file will be securely deleted from the file system and backups.	ABS will <b>use</b> personal information when it checks data files.	information for compilation and analysis purposes in accordance with the C&S Act.
<b>2(b)</b>	<p>The Librarian team will:</p> <ul style="list-style-type: none"> <li>▪ apply privacy measures to anonymise personal information. This will involve: <ul style="list-style-type: none"> <li>○ replacing the Source Record IDs with an Anonymised Record ID; and</li> <li>○ encrypting SLK-581s;<sup>39</sup> and</li> </ul> </li> <li>▪ create a Concordance File, which shows how the Source Record IDs correspond to the Anonymised Record IDs. SLK-581 data is not present in the Concordance File.</li> </ul> <p>The cleaned, standardised and anonymised Source Linkage Data Files (i.e. the encrypted SLK-581 and the Anonymised Record IDs) – Linkage Files, are then provided to the Linker team, and the Concordance File is provided to the Assembler team.</p>	<p><b>APP 6</b></p> <p>ABS will <b>use</b> personal information when it encrypts, anonymises and transfers the data files.</p>	ABS will <b>communicate</b> (between ABS officers) protected statistical information for compilation and analysis purposes in accordance with the C&S Act.
<b>3. Linker team processes</b>			
<b>3(a)</b>	<p>The Linker team will link together the processed Linkage Files using the encrypted SLK-581. The resulting Linkage Results File shows how Anonymised Record IDs correspond to each encrypted SLK-581.<sup>40</sup></p> <p>The linking variable (encrypted SLK-581) is removed from the Linked Results File prior to being passed to the Assembler team, so that the Assembler team will only receive a file with all linked Anonymised Record IDs.</p> <p>The proposed linkage method will not create or use a spine. Note this may be revised as part of future linkage methodology reviews.</p> <p>The dataset will grow each year as new data are added. No data will be purged between years – the Criminal Justice Data Asset will grow as a time series.</p>	<p><b>APP 6</b></p> <p>ABS will <b>use</b> personal information when it links and transfers the data files.</p>	ABS will <b>communicate</b> (between ABS officers) protected statistical information for compilation and analysis purposes in accordance with the C&S Act.

<sup>39</sup> The encrypted SLK-581 will appear in each split SLK file.

<sup>40</sup> For example, if there are three datasets being linked, the Linkage Results Files would comprise: (a) one column for encrypted SLK-581; and (b) one column for each of the datasets (with the Anonymised Record ID for the relevant dataset appearing in each column).

Step	Description	Personal Information Flow	Protected Information Flow
<b>4. Assembler team processes</b>			
<b>4(a)</b>	<p>The Assembler team cleans, prepares and treats the Source Analytical Data Files to ensure they are fit for purpose. Processing of the data will include:</p> <ul style="list-style-type: none"> <li>▪ anonymising any unique identifiers;</li> <li>▪ ensuring the files only contain (analytical) information that is relevant to the particular project proposal; and</li> <li>▪ applying confidentiality treatments.</li> </ul>	<p><b>APP 6</b></p> <p>ABS will <b>use</b> personal information when it processes data files.</p>	No protected statistical information communicated or divulged at this point.
<b>4(b)</b>	<p>The Assembler team will use the Concordance File to replace the Anonymised Record IDs on the Linkage Results File with Source Record IDs.</p> <p>The Assembler team then assembles the Output Files using the cleaned Source Analytical Data Files and the Linkage Results File with Source Record IDs.</p> <p>At this point, the Assembler team will remove the Source Record ID and assign an Analysis ID<sup>41</sup> (a randomly generated synthetic ID) for each Output File. Records can be matched across the Output Files using the Analysis ID.</p>	<p><b>APP 6</b></p> <p>ABS will <b>use</b> personal information when it assembles the data files.</p>	No protected statistical information communicated or divulged at this point.
<b>4(c)</b>	The Output Files are subject to another round of checks conducted by the Microdata Resource team. These are final checks to ensure that the data has been assembled correctly (based on agreed project proposal specifications) and there is no identifiable information remaining on the file.	<p><b>APP 6</b></p> <p>ABS will <b>use</b> personal information when it reviews and transfers the final data files.</p>	ABS will <b>communicate</b> (between ABS officers) protected statistical information for compilation and analysis purposes in accordance with the C&S Act.
<b>5. Release of data into the DataLab</b>			

<sup>41</sup> Analysis IDs are applied after the datasets have been assembled so there is only one row per person. The ID given to each row is the Analysis ID – so it effectively replaces the linkage variable between datasets.

Step	Description	Personal Information Flow	Protected Information Flow
5(a)	<p>Once the Output Files have been through the final round of checks, they are loaded into the ABS DataLab which may form a new product module.<sup>42</sup></p> <p>Modules are approved extracts of the de-identified linked data (microdata<sup>43</sup>) that are loaded to DataLab. These often include commonly requested data items, so that linkage doesn't have to be duplicated.</p> <p>The Assembler/Microdata Resource teams will release only the data/module that is required to meet the requirements of an approved project proposal (i.e. this may mean that only data from certain regions or between certain dates).</p>	<p><b>APP 6</b></p> <p>ABS will <b>use</b> personal information it loads data files into the DataLab.</p>	<p>ABS will <b>communicate</b> (between ABS officers) protected statistical information for compilation and analysis purposes in accordance with the C&amp;S Act.</p>
5(b)	<p>Approved researchers can access the product if the Australian Statistician or delegate has approved the release in writing, the researcher and a senior responsible officer have provided an undertaking, all direct identifiers have been removed, and if information relating to a person is not disclosed in a manner that is likely to enable the identification of that person. Furthermore, any access by researchers must be done in accordance with any conditions or requirements agreed between the ABS and the source data custodian.</p> <p>In order to gain access to the de-identified microdata for statistical or research purposes in the DataLab environment, researchers must complete a number of steps, including having an approved 'safe project' (via registering and submitting a project proposal in myDATA), be located in Australia when accessing microdata, completing 'safe researcher' training and completing all relevant undertakings and declarations of compliance.</p> <p>Approved users are only given access to the microdata relevant to their project. Functional separation means that a person cannot have access to the data linking environment (NGI) and the DataLab at the same time.</p> <p>Authorised researchers will access the data/module for analysis within the ABS DataLab.</p>	<p><b>Out of scope for this PIA</b></p>	<p><b>Out of scope for this PIA</b></p>

<sup>42</sup> A module is a collection of variables from a data source that are grouped together. All MADIP modules are access-controlled in the DataLab – access is granted only to projects that are approved by the relevant data custodian(s) to access the module.

<sup>43</sup> Microdata is the unit record data that provides detailed information about people, households, businesses or other types of entities. It includes data created from ABS surveys and the Census, person centred and business centred administrative data, and integrated data (Australian Bureau of Statistics Cloud DataLab PIA, June 2020).

Step	Description	Personal Information Flow	Protected Information Flow
<b>6. Outputs of data from the DataLab</b>			
<b>6(a)</b>	<p>Analytics findings (outputs) are used to create reports and products for relevant stakeholders. Outputs must be in accordance with the project proposal.</p> <p>Only aggregated data can be output from the DataLab (no unit record files) and all outputs are checked by the ABS for potential confidentiality risks before being released from the DataLab. These checks include requiring a minimum number of contributors per cell to prevent the possibility of identification. There are also penalties for unauthorised disclosure of information, further reducing the likelihood of any disclosive data being released.</p>	<b>Out of scope for this PIA</b>	<b>Out of scope for this PIA</b>

## Schedule 2 — Data custodians

<b>Corrective Services (for the <i>Prisoners in Australia</i> publication)</b>	<p>Corrective Services NSW</p> <p>ACT Corrective Services</p> <p>Department of Justice Tasmania – Corrective Services</p> <p>Department of Attorney-General and Justice NT – Corrective Services</p> <p>Crime Statistics Agency/Corrections Victoria</p> <p>QLD Corrective Services</p> <p>SA Department for Correctional Services</p> <p>WA Department of Justice</p>
<b>Criminal Courts (for the <i>Criminal Courts, Australia</i> publication)</b>	<p>Department of Justice NSW</p> <p>Justice and Community Safety Directorate, ACT</p> <p>Department of Justice Tasmania</p> <p>Department of Attorney-General and Justice NT</p> <p>Crime Statistics Agency/Court Services Victoria</p> <p>Department of Justice and Attorney-General, Qld Courts</p> <p>Courts Administration Authority SA</p> <p>WA Department of Justice</p>
<b>Police (for the <i>Recorded Crime – Offenders</i> publication)</b>	<p>NSW Police Force</p> <p>ACT Policing</p> <p>Tasmania Police</p> <p>Northern Territory Police</p> <p>Victoria Police</p> <p>Queensland Police Service</p> <p>South Australia Police</p> <p>Western Australia Police</p>

## Schedule 3 — Data elements

**Note 1:** Data in **blue bold** text is 'sensitive information' as defined under the Privacy Act (i.e. criminal record information, and information about racial or ethnic origin).

**Note 2:** We are instructed that not all of the data elements listed in the tables below will be included in the first iteration of the Project, although they may be included in subsequent iterations.

<i>Prisoners in Australia</i>	
File type	Data elements
Source Analytical Data File	Source Record ID State Sex Half year of birth <b>Legal Status<sup>44</sup></b> <b>Type of sentence</b> <b>Most serious offence (ANZSOC)</b> <b>Detention start date</b> <b>Detention end date</b> <b>Detention end reason</b> <b>Aggregate sentence</b> Country of birth <b>Indigenous Status</b> <b>Previous known adult imprisonment</b>
Source linkage file	SLK-581 Source Record ID

---

<sup>44</sup> This refers to the type of warrant or court order issued against a person (e.g. sentenced and awaiting appeal, convicted but awaiting sentence, unfit to plead, etc.). It is used to distinguish between sentenced and unsentenced prisoners.

<b><i>Criminal Courts, Australia</i></b>	
<b>Source Analytical Data File</b>	Source Record ID State Sex Half year of birth Date of initiation Date of finalisation Sentence type Offence (ANZSOC) Method of initiation Method of finalisation FDV flag Indigenous Status Court level Sentence quantum unit Sentence quantum
<b>Source linkage file</b>	SLK-581 Source Record ID

<b><i>Recorded Crime – Offenders</i></b>	
<b>Source Analytical Data File</b>	Source Record ID State Sex Half year of birth Date of action Offence (ANZSOC) Method of proceeding FDV flag Indigenous Status
<b>Source linkage file</b>	SLK-581 Source Record ID

## Schedule 4 — Materials considered

### ABS Documents and Materials

- ABS National Crime and Justice Data Linkage Project – Proof of Concept Summary (undated)
- CJDA Data Flows (undated)
- CJDA Privacy Consultations – Pre-Material (undated)
- CJDA Privacy Consultations – Slides (undated)
- CJDA Process Flow (undated)
- Data Integration Plan: Proof of Concept for Crime and Justice Data Integration (undated)
- Draft Memorandum of Understanding in relation to provision of data and data integration activities as part of the National Crime and Justice Data Linkage Project and the Criminal Justice Data Asset (October 2023)
- Item 7: National Crime and Justice Data Linkage Project Update (3 May 2023)
- National Centre for Crime and Justice Statistics – Structure – 2022/23 (undated)
- Privacy Impact Assessment: Proof of Concept for Crime and Justice Data Integration (undated)
- Use of the SLK-581 in the Criminal Justice Data Asset (undated)
- Various information and comments provided by ABS in relation to draft versions of the PIA and information flows

### OAIC Resources

- Australian Privacy Principles Guidelines (December 2022)
- De-identification and the Privacy Act (21 March 2018)
- Guide to Undertaking Privacy Impact Assessments (September 2021)

### Legislation

- *Census and Statistics Act 1905* (Cth)
- *Census and Statistics (Information Release and Access) Determination 2018* (Cth)
- *Census and Statistics Regulation 2016* (Cth)
- *Privacy Act 1988* (Cth)
- *Privacy (Australian Government Agencies – Governance) APP Code 2017* (Cth)

## Schedule 5 — Glossary

Term/Acronym	Definition
<b>ABS</b>	Australian Bureau of Statistics
<b>AIATSIS</b>	Australian Institute of Aboriginal and Torres Strait Islander Studies
<b>APPs</b>	Australian Privacy Principles, which are set out at Schedule 1 of the Privacy Act.
<b>APS Privacy Governance Code</b>	<i>Privacy (Australian Government Agencies – Governance) APP Code 2017</i> (Cth)
<b>Archives Act</b>	<i>Archives Act 1983</i> (Cth)
<b>CJDA</b>	Criminal Justice Data Asset, which is a longitudinal national criminal justice data asset that will be produced by the ABS by linking police, criminal courts and corrective services data provided by State and Territory data custodians across Australia.
<b>C&amp;S Act</b>	<i>Census and Statistics Act 1905</i> (Cth)
<b>C&amp;S Determination</b>	<i>Census and Statistics (Information Release and Access) Determination 2018</i> (Cth)
<b>C&amp;S Regulations</b>	<i>Census and Statistics Regulation 2016</i> (Cth)
<b>DataLab</b>	ABS DataLab, which is the system used by the ABS to enable approved researchers to access data for approved projects.
<b>MOU</b>	Memorandum of Understanding
<b>myDATA</b>	Portal for managing research projects accessing ABS Microdata within DataLab ( <a href="https://mydataportal.abs.gov.au">https://mydataportal.abs.gov.au</a> )
<b>NCCJS</b>	National Centre for Crime and Justice Statistics
<b>OAIC</b>	Office of the Australian Information Commissioner
<b>Personal information</b>	As defined in the Privacy Act
<b>PIA</b>	Privacy Impact Assessment
<b>PIA Guide</b>	<i>Guide to undertaking privacy impact assessments</i> , published by the OAIC.
<b>Prison to Work Report</b>	Council of Australian Governments, <i>Prison to Work Report</i> (2016)
<b>Privacy Act</b>	<i>Privacy Act 1988</i> (Cth)
<b>Project</b>	National Crime and Justice Data Linkage Project, which aims to develop a longitudinal national criminal justice asset, known as the Criminal Justice Data Asset.
<b>Protected information</b>	Information that is protected by section 19 of the C&S Act.
<b>Sensitive information</b>	As defined in the Privacy Act (a subcategory of personal information).

Term/Acronym	Definition																					
SLK-581	<p>A string of 14 letters and numbers which will be used as a statistical linkage key for the purpose of the Project. SLK-581 comprises, in order, from left to right:</p> <ul style="list-style-type: none"><li>the second, third and fifth letters of a person's surname (three letters);</li><li>the second and third letters of the person's given name (two letters);</li><li>all eight digits in the person's date of birth (DDMMYYYY) (eight digits); and</li><li>code for sex (1 for male, and 2 for female) (one digit).</li></ul> <p>For example, 'Jane Smith born on 1 January 1990' would be represented with an SLK of 'MIHAN010119902'.</p> <p>The SLK-581 ignores all non-alphabetic characters in the person's names and there are set rules for dealing with short names and/or missing values:</p> <table><tr><th>Component</th><th>Issue</th><th>Rule</th></tr><tr><td rowspan="3">Surname</td><td>Is missing</td><td>Use 999 as the three 'letters'</td></tr><tr><td>Is 3 or 4 letters long</td><td>Use 2 as the third 'letter'</td></tr><tr><td>Is 1 or 2 letters long</td><td>Use 2 and 2 as the second &amp; third 'letters'</td></tr><tr><td rowspan="2">Given name</td><td>Is missing</td><td>Use 99 as the two 'letters'</td></tr><tr><td>Is 1 or 2 letters long</td><td>Use 2 as the second 'letter'</td></tr><tr><td>Date of birth</td><td>Is missing</td><td>Use 01011900 as the eight digits</td></tr><tr><td>Sex</td><td>Is missing</td><td>Use 9 as the single digit code</td></tr></table>	Component	Issue	Rule	Surname	Is missing	Use 999 as the three 'letters'	Is 3 or 4 letters long	Use 2 as the third 'letter'	Is 1 or 2 letters long	Use 2 and 2 as the second & third 'letters'	Given name	Is missing	Use 99 as the two 'letters'	Is 1 or 2 letters long	Use 2 as the second 'letter'	Date of birth	Is missing	Use 01011900 as the eight digits	Sex	Is missing	Use 9 as the single digit code
Component	Issue	Rule																				
Surname	Is missing	Use 999 as the three 'letters'																				
	Is 3 or 4 letters long	Use 2 as the third 'letter'																				
	Is 1 or 2 letters long	Use 2 and 2 as the second & third 'letters'																				
Given name	Is missing	Use 99 as the two 'letters'																				
	Is 1 or 2 letters long	Use 2 as the second 'letter'																				
Date of birth	Is missing	Use 01011900 as the eight digits																				
Sex	Is missing	Use 9 as the single digit code																				