



The PLIDA Governance Guide

v1.1

2026



Contents

Introduction	3
What is the purpose of this document?	3
What is data integration?	3
What is the Person-Level Integrated Data Asset or PLIDA?	4
What PLIDA can and cannot be used for	6
Benefits for data custodians	6
Costs for data custodians	7
Governance Principles	8
Co-governance	8
Privacy by Design	10
How do these protocols ensure FAIR principles are met?	13
PLIDA Board	14
Can I be a member of PLIDA Board?	14
Data Custodian responsibilities	15
What is my role as a PLIDA data custodian?	15
Data Linkage Process	20
Person Linkage Spine	22
Data Assembly	23
PLIDA Modular Products	23
Core Modules	24
Access to the PLIDA through ABS DataLab	25
Project approval processes	25
Researcher onboarding process	30
Releasing data from the Datalab	33
Retention and destruction of data	35
Attachments	37
Legislative authority	37
Accredited Data Service Provider documentation	37
How is data in PLIDA kept safe?	37
PLIDA Data Item List	39
ABS Data Storage Environments	39
ABS Data Breach Protocol	39
ABS Security	40

Introduction

What is the purpose of this document?

[Guidance for Data Custodians | Australian Bureau of Statistics](#)

Welcome new or prospective data custodian! This document is a collection of information about Person Level Integrated Data Asset (PLIDA) governance.

These guidelines describe the PLIDA Operating Model, governance protocols set by legislated protections and accreditations, and historical decisions by the Australian Statistician informed by public consultation and PLIDA Board advice. Changes to the Operating Model require [delegated] Australian Statistician approval, PLIDA Board endorsement and public consultation.

The document is an introduction for new data custodians to understand the processes the ABS employs to manage their data safely and securely and to understand their role in the data integration journey. When signing a data sharing arrangement, typically a Letter of Exchange with the ABS, you are agreeing to these governance protocols. The document provides links to the ABS website and references to process flows. The ABS maintains Standard Operating Procedures that underpin each process described here. This document supports an organisation's own privacy and ethics approvals for data sharing into PLIDA.

This document is not designed to inform data custodians that want to supply data but do not permit re-use of that data. While many of these governance protocols apply, data custodians wanting custom integrations should contact the ABS.

What is data integration?

[Data integration | Australian Bureau of Statistics](#)

Data integration is the process of combining data from two or more sources at the unit level (e.g. person and/or business). The ABS integrates data to enhance the data available for informing Australia's important decisions.

Integrated data is used to gain insights into our society, economy and environment. These insights support important research and improve government policies and services in areas such as health, education, infrastructure, and business.

The ABS works as a trusted partner with government, research institutions and business on data integration projects that have a clear public benefit. The data we integrate comes from the Census and surveys we run, and from other government agencies.

PLIDA provides the ability to integrate your data with other datasets in a safe and secure environment, while allowing you and other custodians to maintain control of the data.

What is the Person-Level Integrated Data Asset or PLIDA?

[Person Level Integrated Data Asset \(PLIDA\) | Australian Bureau of Statistics](#)

PLIDA is a secure data asset combining information on health, education, government payments, income and taxation, employment, and population demographics to create a comprehensive picture of Australia over time. It is part of the ABS Integrated Data suite and connects to business and location data (see diagram).

PLIDA was initiated in 2015 and provides whole-of-life insights about various population groups in Australia, such as interactions between their characteristics, use of services like healthcare and education, and outcomes like improved health and employment.

There are now 47 datasets that are part of the core PLIDA product that are available for re-use with notable developments in health, wealth and housing domains. In comparison, there were only 9 datasets in 2017. The ABS has linked another 59 datasets for specific projects making 106 in total in PLIDA. This includes a wide range of State and Territory data and some new private sector datasets such as insurance data, many of which are not available for re-use.

As an Accredited Data Service Provider, the ABS collects and combines the data, provides access to authorised researchers, and protects privacy and keeps information secure at all times⁶.

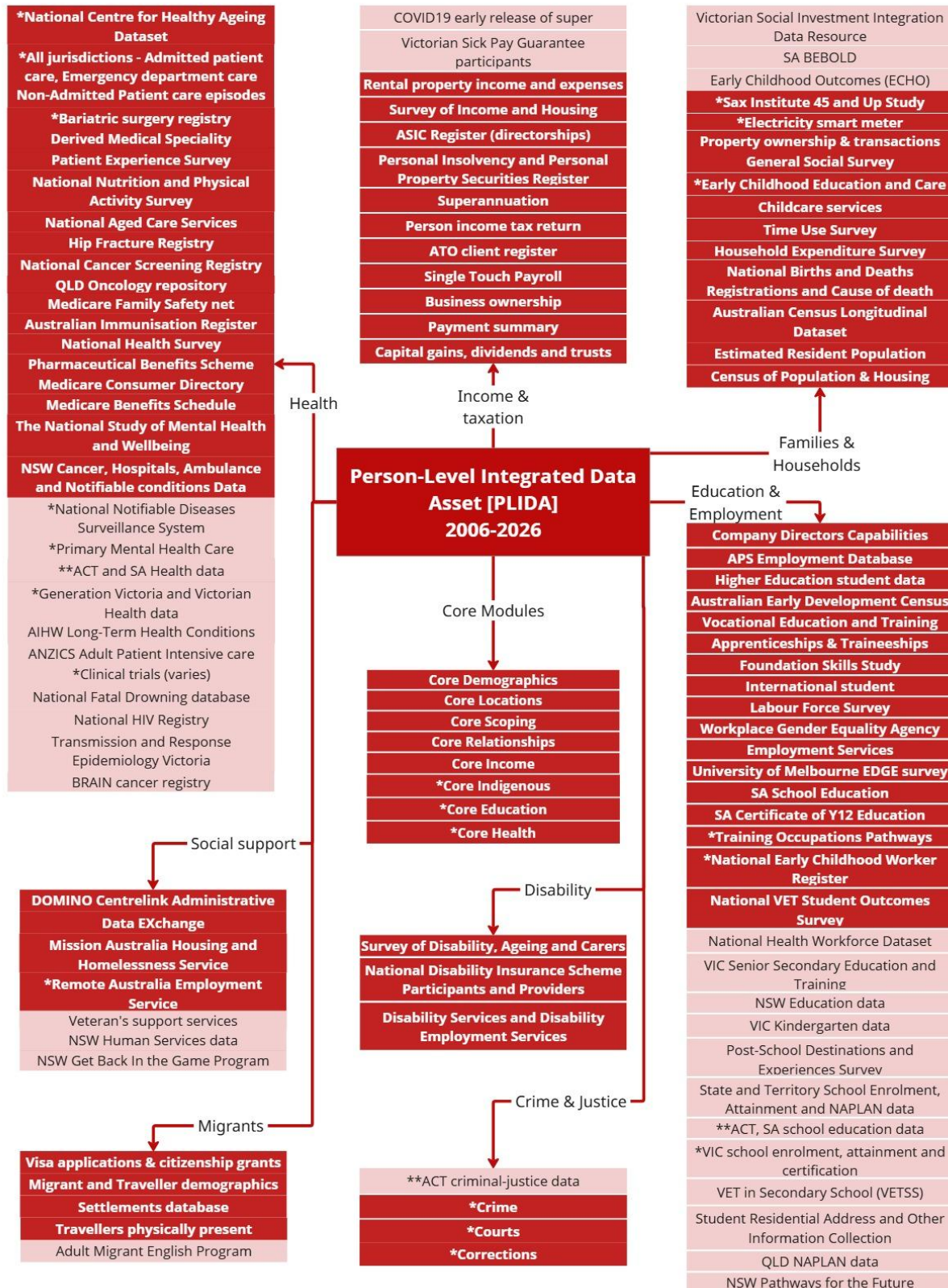
Figure 1. Person-Level Integrated Data Asset

PLIDA is not a single, integrated dataset – the data structure is a set of linkable files based on unique individual identifiers.

Dark bars indicate the dataset is available for re-use. Light bars indicate the data is not available for re-use

An * indicates that the data supply is in negotiation or data integration is underway.

An ** indicates being linked to PLIDA for the purposes of the Life Course Data Initiative and access will be limited to approved LCDI projects during the pilot phase.



What PLIDA can and cannot be used for

[Five Safes framework | Australian Bureau of Statistics](#)
[Using DataLab responsibly | Australian Bureau of Statistics](#)

Permissible uses of PLIDA include

1. Research and analysis for approved project purposes, including:
 - Answer policy questions
 - Program evaluation
 - Empirical research
 - Inform decisions relating to the expenditure of government funding.
2. Statistical purposes, including supporting the production of official statistics.

While there are clear benefits to data integration, there is also a responsibility for stakeholders of data integration projects to preserve privacy and confidentiality through policies and procedures.

Data integration projects will only proceed where they provide significant benefit to the public, are only conducted for statistical and research purposes (not for compliance or regulatory purposes), minimise any potential impact on privacy and confidentiality and are transparent – the datasets and research purposes are published on the ABS website. The 'Safe projects' section of the [Five Safes framework | Australian Bureau of Statistics](#) webpage mentions '*no capacity to be used for compliance or regulatory purposes*'. The [Using DataLab responsibly | Australian Bureau of Statistics](#) webpage under "DataLab undertakings" also mentions that researchers will '*only use the information for statistical or research purposes*'.

Benefits for data custodians

PLIDA makes better use of information that has already been collected. By combining administrative datasets, survey datasets and the Australian Census, PLIDA enhances the value of existing public data resources.

- *We save you significant time and effort.* When you link your data to PLIDA or access the data we save you over \$100m and 12 years of work to set up similar research infrastructure.
- *The data is pre-linked NOT pre-approved.* Data custodians always retain control over data access. Conditions of use are upheld by legally binding undertakings from individuals and organisations.
- *As we grow you grow.* We significantly enrich your data with a range of demographic and outcome information over time. We do this in the most secure environment that preserves privacy with care and diligence. We have a solid track record in privacy, safe and secure platforms and governance. As new data becomes available from other sources your data can be further enriched. You only need to measure one 'thing', we can help you measure everything else.
- *We can take the pressure off your organisation.* Once linked, you can redirect data access requests to the ABS enforcing a *supply once, use many times* approach. We manage data requests on your behalf, reducing time and effort and proliferation of your data. Approved projects access data through our secure DataLab. This is a subsidized and high capability service that saves people the effort of building this technical and governance infrastructure themselves. You get to review access requests and see draft publications coming out of DataLab.
- *Research opportunity.* As a data custodian, you also get access to the same DataLab services.
- *Collaboration opportunity.* As a researcher you can use our DataLab as a common forum for collaboration with academics and others to join or deliver your projects.

Costs for data custodians

[Data integration service](#) | [Australian Bureau of Statistics](#)

As an organisation that provides data, data custodians need to

- Enter into a data sharing agreement,
- Provide data and metadata as agreed, and
- Where required, consider access requests from other organisations, and
- Where required, review and comment on draft publications from approved researchers.

Governance Principles

Co-governance

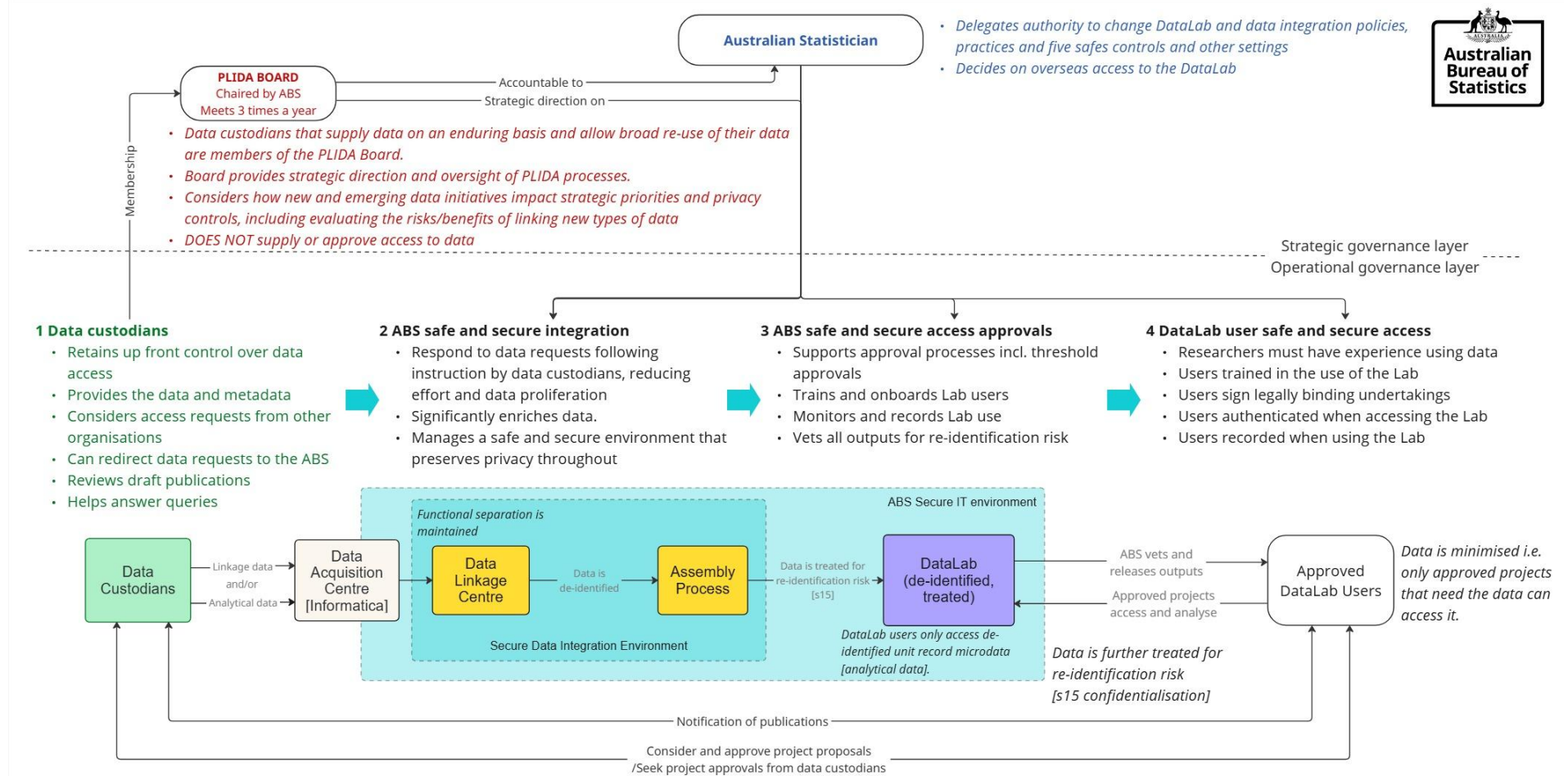
The success of PLIDA as a sustainable asset is built on a foundation of co-governance and partnership with data custodians.

The ABS maintains a wide range of PLIDA datasets or *modules* – linking data on healthcare, education, government payments, personal income tax, housing and population. There are now 45 datasets that are part of the core PLIDA Modular Product but the ABS has linked or is linking more than 80 other modules for specific projects.

Access to each of these modules is controlled by a data custodian – directly, or by delegation. This means there are 120+ examples of data custodians contributing to PLIDA co-governance by considering and approving access on a *project-by-project* basis. This includes some State and Territory and private sector data custodians.

The below diagram provides an overview of PLIDA co-governance. Data custodians supply a dataset and metadata via secure file sharing. Keeping the linkage and analytical data separated at all times, the ABS undertakes linkage and assembly work to turn the dataset into a pre-linked and de-identified PLIDA Module in the PLIDA Modular Product. Any Safe Data controls are applied at this stage. All data integrations are undertaken in secure cloud-based infrastructure [Secure Environment for Analysing Data](#) (SEAD) and the [Australian National Data Integration Infrastructure](#) (ANDII). Once delivered, information on the new PLIDA Module is findable in myDATA, the ABS' client relationship management system, for approved researchers to request. The relevant Data Custodian is notified of new access requests and is provided with a range of information on research aims, public interest, ethical and cultural guidance to inform a decision. If approved, the actual PLIDA Module is provisioned in the ABS DataLab for that specific project. The ABS manages Safe Output controls and releases de-identified and confidentialised data to the researchers in the project. Once the researchers are ready to publish they must notify ABS and data custodians, giving data custodians the opportunity to comment on findings and interpretation.

Figure 2. PLIDA co-governance in action



Privacy by Design

*[PLIDA/MADIP Privacy Impact Assessments | Australian Bureau of Statistics](#)
[Privacy in PLIDA | Australian Bureau of Statistics](#)*

The ABS and the PLIDA Board are committed to upholding the privacy, confidentiality and security of information in the PLIDA. The ABS embeds Privacy by Design principles throughout the governance and operation of the PLIDA, ensuring privacy protections are proactively considered and systematically applied. This approach reflects the ABS's obligations under the Privacy Act 1988, the Australian Privacy Principles (APPs), and the Australian Government Agencies Privacy Code.

Privacy by Design in PLIDA is not a single process but a layered framework that integrates privacy safeguards at the system, asset, and project levels. These protections are supported by formal privacy tools, risk assessments, and transparency measures that ensure PLIDA operates securely, ethically, and in alignment with community expectations.

Embedded Privacy Protections

Privacy protections in PLIDA are embedded across three levels:

System Level

At the system level, privacy safeguards are built into the data integration infrastructure and governance arrangements. This includes secure technical environments, functional separation of roles to prevent unauthorised access, and periodic system-wide PIAs to identify and mitigate emerging risks.

Asset Level

At the asset level, privacy controls support the safe use and expansion of PLIDA. The recurring PLIDA Privacy Impact Assessment Update—conducted every two to three years—assesses changes to the asset, including new datasets and expanded outputs, ensuring continued compliance with the Privacy Act 1988 and the Australian Privacy Principles (APPs). Safe Data Risk Assessments are also used to evaluate reidentification risks.

Project Level

At the project level, privacy protections are tailored to individual data integration activities. All new proposals undergo Privacy Threshold Assessments (PTAs), with full PIAs conducted for projects involving higher privacy risks or sensitive data. Additional transparency measures include public disclosure of the proposal, a call for public feedback, and targeted consultations.

Privacy Tools and Processes

The ABS uses a suite of privacy tools and processes to ensure that PLIDA operates in accordance with our privacy obligations. This includes:

1. ABS Privacy Policies

The ABS Privacy Policies set out the ABS's personal information handling practices, including how personal information is collected, stored, used, and disclosed. These policies apply across all ABS activities and provide the foundation for privacy compliance in PLIDA operations.

2. PLIDA Privacy Statement

The [PLIDA Privacy Statement](#) outlines the specific privacy practices applied to PLIDA. It describes how personal information is managed within the asset, including safeguards around data integration, access controls, and the use of de-identified data for research and statistical purposes.

3. Privacy Threshold Assessments (PTAs)

PTAs are conducted for all new PLIDA data linkage proposals. They help determine whether a full Privacy Impact Assessment (PIA) is required based on the nature of the data, intended use, and potential privacy risks.

4. Privacy Impact Assessments (PIAs)

PIAs are undertaken at the system, asset, and project levels. They identify and assess privacy risks, recommend mitigation strategies, and ensure compliance with legislative and ethical standards. A recurring PLIDA PIA Update is conducted every two to three years to evaluate changes to the asset and maintain alignment with best practices.

5. Additional Transparency Measures

When a project proposes linking a new type of data with PLIDA, enhanced transparency measures are applied. These may include:

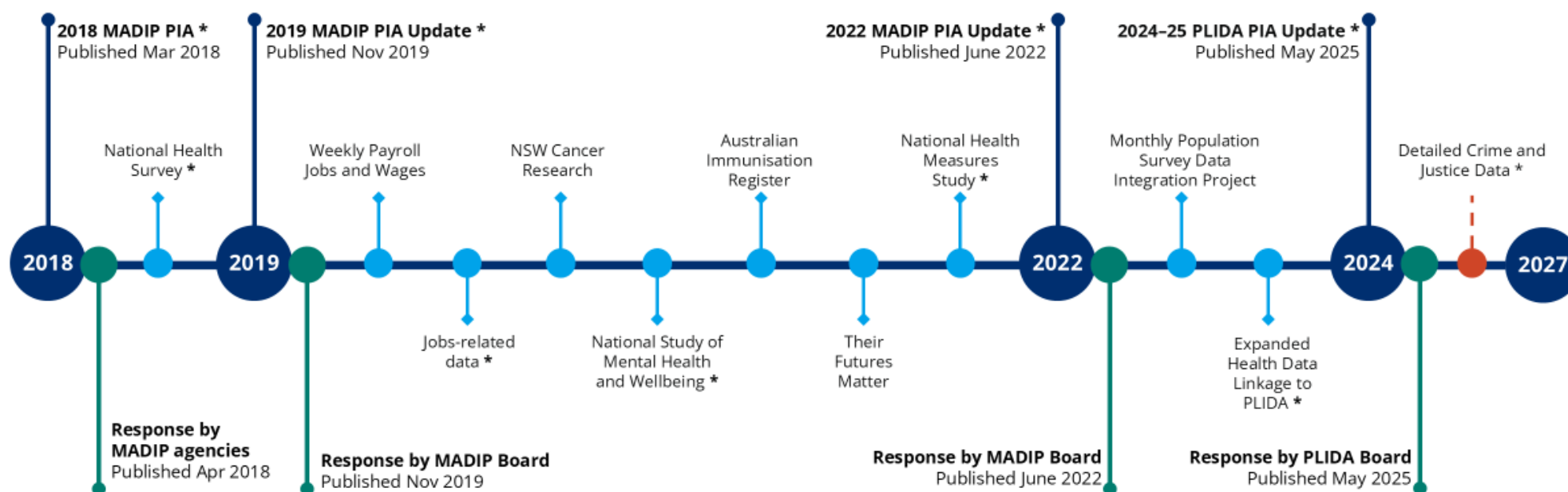
- Public notification of the proposal
- An invitation for public feedback
- Targeted stakeholder consultation

Final decisions and supporting justifications are published on the ABS website.

During the term of the Letter, the ABS will apply privacy by design practices, which include:

- conducting privacy threshold assessments on all new PLIDA data linkage proposals and projects
- conducting privacy impact assessments where a proposal or project is found to have a medium to high privacy risk or requires additional transparency measures. The ABS also conducts periodic updates of the independent privacy impact assessment for PLIDA
- using the seven High Level Principles for Data Integration to conduct any linkage of supplied data to PLIDA. These Principles are the established protocols for the safe and secure integration of Commonwealth data for research and statistical purposes.
- applying the Five Safes Framework
- applying the Separation Principle which means personal identifiers are stored separately from other information, and no one can view both personal identifiers and analytical information at the same time
- implementing functional separation (or roles) in all data integration projects. This means that staff undertaking data linkage projects only have access to the information that they need to perform their assigned role
- deleting personal identifiers (such as name and address) once the data is integrated to PLIDA and there is no longer a business need for the data. The ABS will retain an encoded version for any future linking.
- not making any linkage information available to authorised users for research purposes.
- an ongoing program of security audits and system accreditations.

Privacy Impact Assessments for MADIP/PLIDA



All documentation available on the [ABS Privacy Impact Assessments](#) webpage

Project-specific PIAs involving PLIDA data

Consultation undertaken

Currently undertaken

How do these protocols ensure FAIR principles are met?

Findable – Information about your linked dataset will be seen in forms in the myDATA system, in ABS communications and on the ABS website. We are transparent about what data we link to PLIDA.

Accessible – Your linked data will be available for researchers to request in the myDATA system. Once approved, the data will be made available to projects in our secure DataLab. Only confidentialised/aggregated data is allowed out of the DataLab.

Interoperable – PLIDA is not a single, integrated dataset. It is a set of discrete pre-linked files *or Modules* with identifiers that enable integration with other PLIDA Modules. Only analytical information is made available to researchers in a de-identified format.

Re-useable - The ABS has a *supply-once, use-many-times* approach to data integration. Data are linked to the Person Linkage Spine and re-used in projects where approved by data custodians.

PLIDA Board

[PLIDA Board | Australian Bureau of Statistics](#)

The PLIDA Board is the governance body responsible for the design of operations and strategic direction of PLIDA. The Board is a decision-making authority accountable to the Australian Statistician.

The PLIDA Board is chaired by an SES Band 2 officer from the Australian Bureau of Statistics (ABS). Meetings are triannual. The Board reports to the Australian Statistician.

The PLIDA Board provides strategic direction and oversight of the PLIDA and develops the PLIDA Strategy which outlines the vision and purpose of PLIDA. The PLIDA Board DOES NOT supply or approve access to data.

The PLIDA Board considers how new and emerging data initiatives impact strategic priorities and evaluates the risks and benefits of linking additional types of data to the asset. This is informed by public consultation through Privacy Impact Assessments.

The PLIDA Board was established as a forum for PLIDA data custodians to discuss and shape the direction and operations of PLIDA.

Can I be a member of PLIDA Board?

Yes.

Not all 120 data custodians are members of PLIDA Board. Data custodians that supply data on an enduring basis and allow broad re-use of their data are members of PLIDA Board. However, you don't need to be a data custodian to be a PLIDA Board member. You can be an observer to the Board.

Current members of the PLIDA Board are listed on the [PLIDA webpage](#). For more information about membership, contact mydataportal@abs.gov.au.

Data Custodian responsibilities

Guidance for Data Custodians | Australian Bureau of Statistics

What is my role as a PLIDA data custodian?

You will sign a data sharing arrangement (DSA) with the ABS. There are multiple forms that DSAs can take but the two most common formats for public sector entities are Memoranda of Understanding (MoU) and Letters of Exchange (LoE). Note that neither formats are legally binding. DSAs describe three expectations:

1. Data supply

Data supply is negotiated in bilateral arrangements between ABS and data custodians. Data custodians are responsible for the preparation of source data and metadata that is shared. ABS has procedures in place to remediate supply of unsolicited data if this occurs. Data supply is described in the [PLIDA data supply guidelines](#).

The ABS works with prospective data custodians to ensure that the data sharing agreement identifies appropriate legal authorisation for data supply (for example, by legislative authorisation, data sharing legislation, or other legal mechanism). It is the responsibility of each data custodian to ensure that they have legal authority or a legal mechanism to supply the data to the ABS and that the supply of the data complies with the *Privacy Act 1988* (Cth) or other applicable privacy legislation (for regulated entities). In circumstances where data has been provided to the ABS on the basis of consent of the data subject, data custodians are responsible for managing the withdrawal of consent by individual data subjects. The ABS updates datasets when custodians provide refreshed data.

PLIDA data custodians provide content data up front, avoiding complex negotiations, resource-intensive duplication of data supply events and delays to approved research and statistics projects. This is important for research and statistical work that requires regular publication or timely results.

What does a data sharing agreement look like?

A Letter of Exchange (LoE) template is provided on the [ABS website](#). The LoE describes the mechanisms that allow for data sharing from the custodian and collection by the ABS.

The usual steps involved are:

- ABS drafts initial document using information provided in the Data Integration Request
 - o If desired, the ABS can use the data custodian's own data sharing arrangement template but will require additional time to review and include standard required clauses (e.g. ABS security measures, privacy clauses, data breach handling etc)
 - o Details in the draft include: name of dataset(s), data reference period(s), timing of supply, name of agency supplying data, method of data transfer, access arrangements for the data (e.g. available for reuse, strictly limited for a specific project), legal mechanism that enables data supply and/or on-sharing of data, notes regarding any additional data custodian requirements, privacy measures (e.g. separation principle), security and data breach measures.
- This draft will be sent to the data custodian for initial review and further discussion as needed.
 - o Legal advice can be sought (from either party) where required to ensure that the content aligns with relevant legislation and policies
- Once both parties agree on the content, the document proceeds to signing. Typically the ABS signs first if it is on their template but this is not a firm requirement.
- If the data will be transferred using ABS' enterprise solution (Informatica), a questionnaire will also be sent around this stage (if not earlier) to collect key information about the number and size of files expected. This gets sent to a technical team for them to complete system set up to enable

the file transfer. Instructions and access codes are sent to the data custodian to explain how to complete the file transfer. These instructions can also be found on the ABS website: [Submitting data files to the ABS | Australian Bureau of Statistics](#)

Conditions

Data custodians can request mutually acceptable conditions about how their data will be used in PLIDA, such as its re-use, ethics, safe output and other approval requirements. Conditions may derive from legal or non-legal sources e.g. policies. The conditions cannot limit the powers of the Australian Statistician under the *Census and Statistics Act 1905*.

What data is collected from data custodians?

The ABS collects two broad types of information for PLIDA:

1. **Linkage information** - which usually includes personal identifiers such as name, sex/gender, address, and date of birth. This information is only used to link the datasets together; it is not used for analytical purposes.
2. **Analytical information** - which includes variables of interest for analysis, such as occupation, income and health services use. Some linkage data may be used for analytical purposes with appropriate confidentiality treatments applied (for example, sex/gender, address).¹⁴

The ABS restricts access to personal identifiers for the purpose of data integration. It uses the internationally recognised best practice: the Separation Principle.

The separation principle requires that personal identifiers (e.g. name, address, date of birth) and analytical information (e.g. occupation, income, health services use) is kept separate at all times (i.e. these two types of data are never used at the same time or seen together).

What are the different supply options for PLIDA?

Datasets can either be a *reuseable* or *not-reuseable* link to PLIDA. Linkages that are not-reuseable are still findable through the Data Integration Register.

- **Reuseable:** The data will be integrated with PLIDA and is requestable by any approved researcher for any approved project strictly in accordance with approval procedures set by the data custodians, who maintain authority over access and usage¹⁶. The data sharing agreement permits access and use without requiring renegotiation or resupply. It is ABS preference to establish reuseable supply and access arrangements as it supports 'share once, use many' outcomes. The ABS prioritises data integration for re-use.
- **Not-reusable:** The data is to be used for a specific project only with no option to request access by other researchers or projects. The data sharing agreement does not permit re-use.

Can I require additional or non-standard governance processes over and above what the ABS already delivers?

Yes.

If a data custodian has a specific approval condition, the ABS can advise researchers of those requirements and refer projects to that data custodian to take the project or researchers through those steps. Once the data custodian is satisfied that those conditions are met, they notify the ABS of approval. This process would be by mutual agreement and written into the data sharing agreement.

If a data custodian wants the ABS to adopt and deliver a non-standard or new protocol or process, the ABS must follow a number of steps. The new process or protocol should be costed and agreed with the data custodian following consultation with researchers and impacted data custodians, a public

consultation through the Privacy Impact Assessment process and ultimate approval by the PLIDA Board and the Australian Statistician. This new process would be written into this and other ABS documentation.

Non-standard governance requests add cost and complexity to the ABS data integration program.

2. Access approvals

[Home](#) | [myDATA](#) | [Australian Bureau of Statistics](#)

Access to data within PLIDA is controlled by data custodians. The PLIDA Board does not approve access to data. Approval is sought from custodians for each project seeking to use their data. Access is subject to approval by PLIDA data custodians which is facilitated through the myDATA platform.

Once a PLIDA Module is created, it is listed as available for request in the myDATA platform. Additional requirements or conditions that are agreed in the data sharing agreement are visible in the myDATA platform so that researchers understand any additional steps they must undertake e.g. ethics committee approval. In parallel, each data custodian is set up in the myDATA system. This enables custodians to consider requests from projects that request access to their Module in the ABS DataLab project proposal form.

Data needs are determined following consultation between the ABS and researchers (the data users). Researchers can then request access to the Module by completing the ABS DataLab project proposal in myDATA for detailed and integrated microdata and completing any additional requirements set out in the data sharing agreement.

Requests for approval to access each Module are automatically forwarded to the relevant data custodian(s). The role of data custodian can be fulfilled in the organisation by the person or role that the custodian chooses to nominate. Data custodians are given 20 business days to review and approve project proposals on a case-by-case basis.

Only once a project is approved, and relevant module access requests are approved, will the Module be loaded into the specific project folder in the ABS DataLab.

It is recommended that custodians consider using the PLIDA threshold model of assessment to reduce the burden of assessing project-by-project requests. Under the threshold model, access to PLIDA microdata in lower-risk projects is subject to approvals by the ABS in its stewardship role and the relevant data custodians are advised of each approval.

The below diagram shows the general approval process. See page 25 for more information on project approvals.

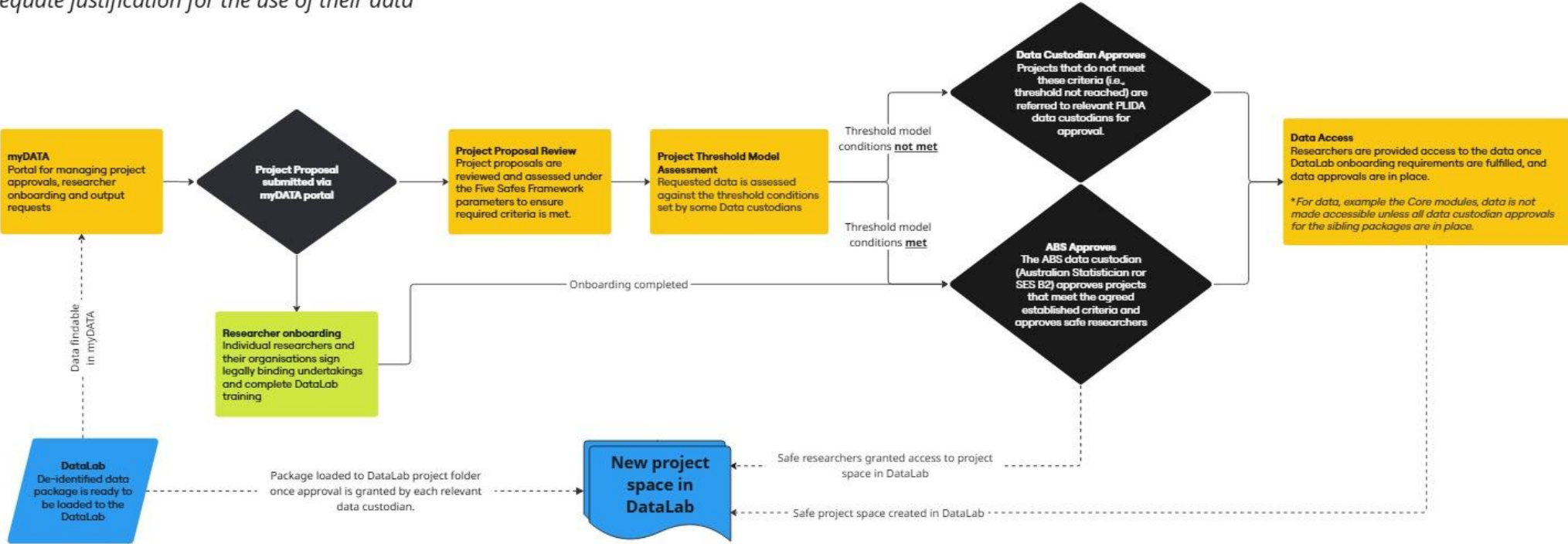
Figure 3. Data custodian approval process flow

Data Custodian Approval Process for PLIDA Modular Products (PMPs)

(as part of the ABS Data Integration process flow)



**Data custodians retain up front control over who accesses their data, and provide approvals based on adequate justification for the use of their data*



3. *Researcher support*

Where possible the ABS supports all technical queries of researchers. Occasionally, the ABS asks data custodians to help respond to highly technical questions. Data Custodians are given the opportunity to review draft publications produced by researchers. See also page 33 for more information.

Data Linkage Process

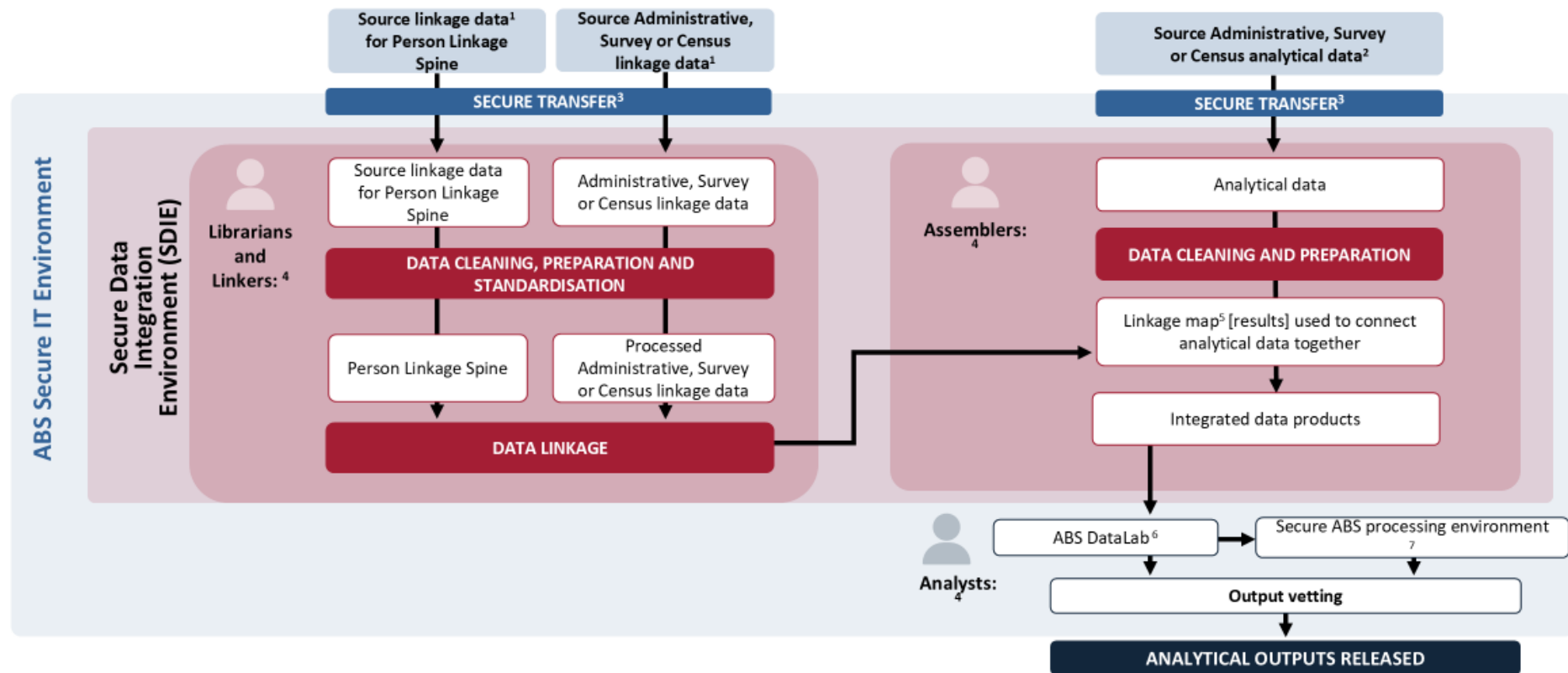
ABS data linkage uses probabilistic and deterministic linkage methods to create a pre-linked PLIDA Module. Information is combined via linking person-level datasets to the Person Linkage Spine (the 'Spine'), a key piece of linking infrastructure that serves as a base dataset representing the 'ever-resident' population of Australia. For more information on the Person Linkage Spine, how it was built and an assessment of its quality, see the attached paper Person Linkage Spine Methodology and Quality Assessment.

- Linkage results provide a way to combine selected source datasets into assembled analytical files which are then accessed in a safe, controlled environment. The data is brought back together using encrypted identifiers to enable efficient assembly for approved projects.
- The receipt of analytical data and personal identifiers occurs via separate files delivered to separate areas of the ABS.
- Personal identifiers are always **stored securely and separately** from the analytical information.
- No-one can access both personal identifiers and analytical information at the same time. Each person working with the data is assigned a role, and is **only able to access the information necessary to perform that role.**
- Datasets provided to the ABS are maintained separately and only integrated with other datasets when required for a specific project purpose.
- Raw personal identifiers are destroyed -upon completion of the data linkage process. Anonymised/processed data is retained.

The diagram below shows the data linkage process as a data flow.

Figure 4. PLIDA data flow

PLIDA Data Flow



- Linkage data:** usually includes personal identifiers such as name, address and date of birth, or other identifiers like Australian Business Numbers. Note, some data items may be approved for both linkage and analytical use.
- Analytical Data:** variables of interest for analysis, such as occupation, income and health services use, or business type and industry.
- Secure transfer:** data is supplied to the ABS via an accredited secure transfer method as agreed with data custodians.
- Functional roles (librarians/linkers, assemblers and analysts):** The ABS applies the separation principle at all stages of the data process, ensuring that linkage data and analytical data are kept separate at all times. ABS officers are assigned to a specific functional role and are only able to access information necessary to perform their role. Refer to Figures 2, 3 and 4 for more information on the different roles undertaken by ABS staff.
- Linkage map:** Maps the links between IDs across datasets. IDs are generated by the ABS. Linkage maps contain no personal information. Refer to Figure 2.
- ABS DataLab:** a secure analytical cloud environment for users to undertake complex analysis of detailed microdata for statistical research or modelling. The ABS uses a series of controls as part of the Five Safes Framework to mitigate the risk of disclosure in the DataLab.
- Secure ABS processing environment:** a location within the secure ABS IT environment where PLIDA data can be used by the ABS for approved projects. Access by ABS officers only in this location.

Person Linkage Spine

[Person linkage spine | Australian Bureau of Statistics \(abs.gov.au\)](https://abs.gov.au/person-linkage-spine)

The Person Linkage Spine is central to our data linking methods. Instead of linking datasets one-to-one for individual projects, we can link all datasets to the Spine once and then combine datasets via the Spine as needed for multiple projects. The Spine enables more efficient and higher quality linkage. By keeping the Spine separate from the main body of the data, we also improve privacy and security.

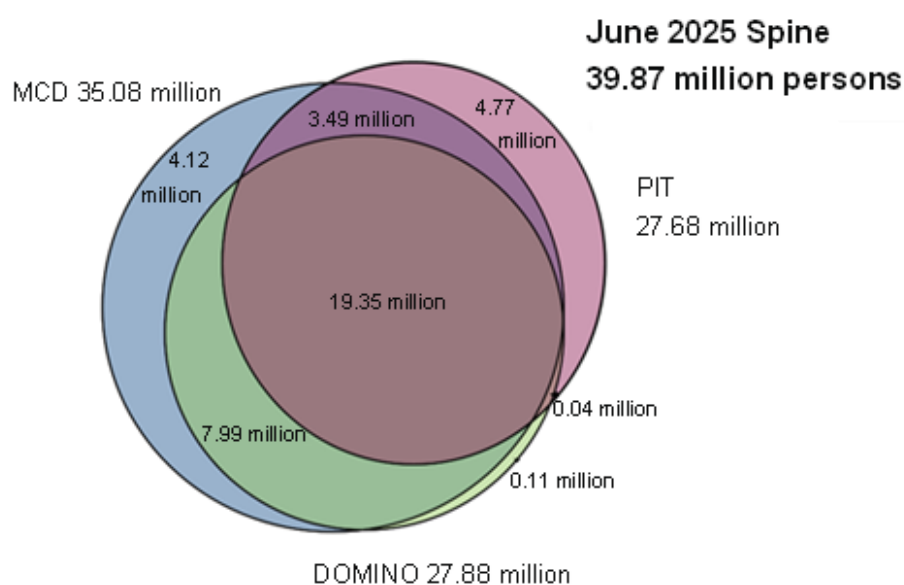
The Spine is based on the combined population from three core datasets:

- Medicare Consumer Directory (MCD) - Services Australia
- DOMINO Centrelink Administrative Data (DOMINO CAD) - Department of Social Services
- Personal Income Tax (PIT) - Australian Taxation Office

The Spine aims to cover all people who were resident in Australia at any point during a given reference period. The current Spine covers January 2006 to June 2025.

- The Spine comprises 39.87 million unique persons

Figure 5. Person Linkage Spine data sources and counts



Data Assembly

Five Safes framework | Australian Bureau of Statistics

Assembly work is required to make integrated datasets available in the DataLab. Before being loaded into the DataLab, all tables in a dataset will go through a series of data quality and confidentiality checks and treatments. Treated data is packaged into DataLab products along with mapping files that enable the data to be joined with other PLIDA data. At a minimum the removal of direct identifiers (such as name and address) must be applied to data before it is released in the DataLab. Further statistical disclosure controls should also be applied, depending on how the data will be released.

Data suppression is already deployed in the DataLab by custodians who desire additional data confidentiality protections over and above the ABS' risk posture. In addition to the data suppression that a custodian applies, the ABS conducts an additional 'Safe Data' process on all new datasets prior to it being made available in the DataLab. This is effectively an ethical hack process that identifies the prevalence of unique individuals who may be easily identifiable in the public domain and recommends additional measures to suppress the dataset further (e.g. top coding, data ranging). The process is also a final gate in detecting other personal identifiers in obscure fields or provided in error (for example, names or contact information in free text fields, or incorrectly reported/logged data such as names included in a postal address field).

PLIDA Modular Products

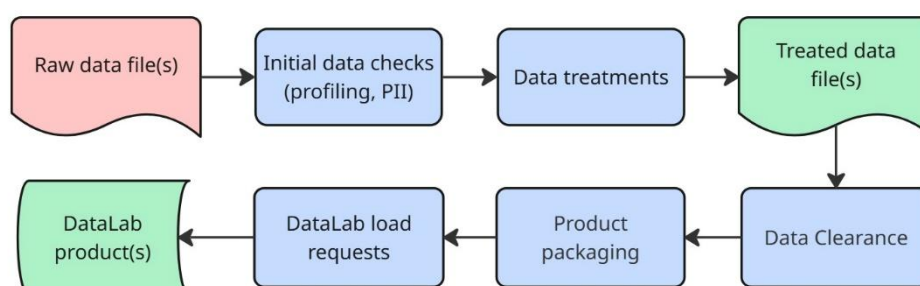
Microdata: Person Level Integrated Data Asset (PLIDA) | Australian Bureau of Statistics

From the linkage and assembly process above we create a detailed microdata product called the PLIDA Modular Product or PMP from your dataset. The PMP is a collection of discrete modules corresponding to different datasets (for example, modules relating to Personal Income Tax, the Medicare Benefits Schedule and Higher Education) from which users select according to their research needs.

All access to PLIDA data is via a PMP made available to approved researchers in the [ABS DataLab](#). Researchers can request access to a PMP by completing the ABS DataLab project proposal for detailed and integrated microdata. Access is subject to approval by each PLIDA data custodian which is facilitated through the myDATA platform.

Modules are requested and approved individually. Only the modules needed for an approved project are provided to the researchers.

Figure 6. PLIDA PMP assembly process



Core Modules

In addition to single-source PLIDA modules, the ABS can (with approval) combine parts of your dataset with others. These are called Core Modules.

The Core Modules are curated by the ABS and are designed to support users to access key information from different data sources in the one place without having to access each data source individually. As part of the development of these modules, we work closely with you to update supply and access governance, and document information about the data to feed into explanatory materials that will aid in data useability.

For example, the *Core Relationships Module* consolidates partner relationships and parent-child relationships from existing and new datasets into one table. The Core Modules pull key information from a range of different datasets in PLIDA and make them available in the one place.

Access to the PLIDA through ABS DataLab

[*Accessing integrated data | Australian Bureau of Statistics
DataLab | Australian Bureau of Statistics*](#)

The ABS provide authorised users with access to the linked data through the ABS DataLab environment.

DataLab is hosted in Microsoft Azure and meets PROTECTED level security standards, as prescribed in the ISM. The DataLab environment is subject to IRAP certification, security audits, robust IT security testing, and patching delivering the Safe Settings aspect of the Five Safes Framework.

Additional security protections applied to DataLab include:

- data encryption at rest to mitigate against unauthorised access to microdata
- Azure Storage Accounts to securely hold individual research products and allow querying from authorised users
- cloud servers (including backup servers) hosted exclusively onshore with access only
- authorised for use in Australia unless approved by the ABS
- closed network virtual machines to provide secure isolated research spaces for the analysis of microdata
- guarded access through multi-factor authentication and workspace segmentation inhibiting data sharing between projects
- a DataLab Product Storage Account protected with Microsoft Defender providing threat detection against malicious/unusual behaviour.

Project approval processes

Standard approval process

[*DataLab User Guide | Australian Bureau of Statistics*](#)

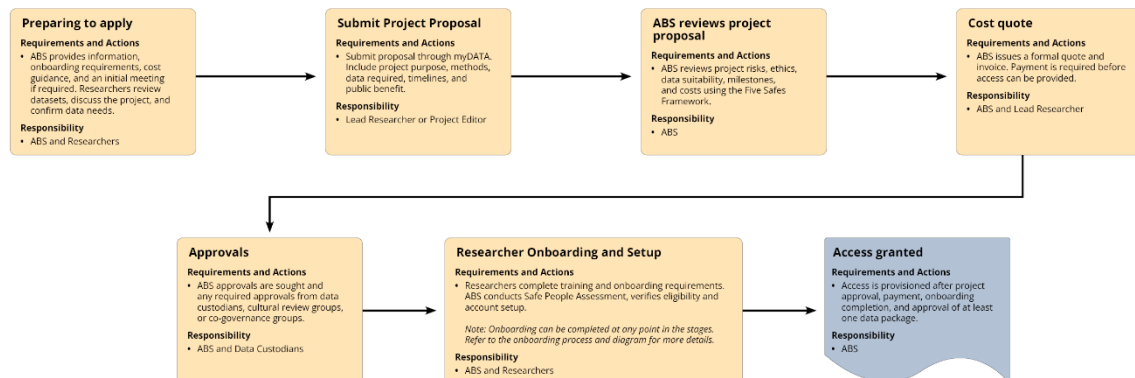
Projects seeking access to PLIDA data follow a structured approval process to ensure compliance with governance requirements and data custodian conditions. All requests are submitted through the myDATA platform as part of the ABS DataLab project proposal process.

Each proposal is assessed against the Five Safes framework and reviewed by relevant data custodians. Approval is granted only when the project demonstrates public value, meets privacy and security standards, and satisfies any additional conditions set by custodians.

For projects requesting access to existing integrated data, public benefit is considered as part of the proposal review activity undertaken by ABS staff following new project submission. The project proposal form specifically requires researchers to detail how the research will provide public benefit as part of the description of project outcomes and objectives. The core principle of the public benefit assessment considers whether the increase in privacy risk that comes with expanding access to or volume of data is outweighed by the value of the additional insights that the integrated dataset could generate. This assessment balances risk against the potential for improved evidence to inform policy, service delivery, research and broader public outcomes.

Refer to Access Approvals for detailed steps on page 17.

Figure 7. ABS DataLab project access process flow



Threshold models of approval

Data custodians can choose to assess each project or have agreed threshold approval standards with the ABS. The ABS also provides an up-front pre-approval service via the *Threshold model* that advises project proponents of their obligations and any restrictions on the data. In this way ABS prevents data custodians from being overloaded with project proposals that are unlikely to be approved.

The ABS Threshold Model takes a risk-based approach centred on the internationally recognised Five Safes Framework, whereby the ABS can approve projects below a risk threshold (i.e., threshold not reached or conditions met) on behalf of data custodians. Those requests above the threshold will be submitted to data custodians for consideration. (i.e., threshold reached or conditions not met).

Where the ABS approves projects on a data custodian's behalf, data custodian are notified of each approval event. This saves the data custodian up to 90% of project assessments depending on how the threshold is implemented.

Adopting the threshold model for assessment is agreed upon between the ABS and data custodians, and captured in the Data sharing agreement instrument.

Register of approved PLIDA projects

[*PLIDA/MADIP Research Projects | Australian Bureau of Statistics*](#)

Details of approved research projects are published on the ABS website. Data Custodians can check which projects they have approved through their myDATA account.

Offshore project approvals

The Australian Bureau of Statistics (ABS) supports DataLab access outside Australia as an ongoing and cost-recovered service. This initiative supports international collaboration and enables secure access to PLIDA by overseas researchers and organisations. In the Data sharing agreement, the data custodian must indicate if international access to their data is allowable under their legislation.

Sensitive data or topics

Sensitive data is defined under the *Privacy Act 1988*, or as defined by a data custodian in a data sharing agreement. If a project requests access to sensitive data such as health or genetic information or information about racial or ethnic origin then the project must go through additional steps:

1. Where Aboriginal, Torres Strait Islander, Māori and Pasifika people or communities are concerned, the project is subject to cultural review.
2. Where the data custodian mandates formal Human Research Ethics Committee (HREC) approval, the project must provide evidence this has occurred and must provide evidence that ethical concerns have been addressed in a Data Ethics Assessment.
3. Where the data custodian does not mandate HREC approval, the project must still provide evidence that ethical concerns have been addressed in a Data Ethics Assessment.

Cultural review

If a project is materially concerned with the lives of Aboriginal and/or Torres Strait Islander, Māori and Pasifika people or communities in Australia, the project is subject to a cultural review.

This process involves referral of the project proposal to a ABS Cultural Review Panel for consideration. The cultural review process includes an assessment of each project within a matrix against the following criteria:

The project must clearly address why Indigenous data are necessary to answer the research question(s), consider how research outcomes may affect the indigenous community, and demonstrate sufficient input from relevant indigenous communities or people to confirm alignment with indigenous research priorities. Consideration of an ethics review by an Aboriginal and Torres Strait Islander HREC should also be discussed.

The ABS is actively engaged with the [Governance of Indigenous Data \(the GID\) Framework](#), whose vision is for Aboriginal and Torres Strait Islander people to have greater agency over how their data are governed within the Australian Public Service so that their priorities and aspirations are reflected.

As the GID framework is further embedded within operations, the cultural review process will continue to evolve, with scope for wider review and consultation to be included.

Human Research Ethics Committee (HREC) approvals

As a condition in a data sharing agreement, data custodians may require that a project obtain approval from an HREC before data can be released into the ABS DataLab. Where this is the case, the ABS facilitates the process by:

- tracking whether approved DataLab projects have obtained HREC approval;
- recording the name of the approving HREC;
- referring researchers to the appropriate HREC, where nominated by the data custodian.

When HREC Approval is Required

Use of an HREC aims to balance the benefits of projects with any risks that the project may cause harm, inconvenience or discomfort to individuals. HREC approval supports the data custodian approval process. Ethics committees will consider a number of aspects before granting approval, including whether projects:

- have research merit and integrity;
- select participants fairly;
- minimise the burden imposed;
- respect the privacy of participants; and
- respect the confidentiality of the information.

Where a data custodian requires a project/s to be approved by a specific HREC, this should be referred to in the data sharing agreement. This may include a specialist data linkage ethics committee in accordance with the exemptions from the National Mutual Acceptance scheme <https://www.medicalresearch.nsw.gov.au/national-mutual-acceptance/>. The ABS will refer researchers to the data custodian to complete any HREC approval steps and ensure HREC approval for a project is obtained before final approval for the project to proceed.

Data Ethics Assessment

In cases where HREC approval is not required but the project is accessing sensitive data, a *Data Ethics Assessment* is required. The data ethics assessment ensures consistent, transparent, and proportionate ethics practices across DataLab projects alongside cultural review, privacy, security and governance controls already in place. The data ethics assessment does not itself constitute an ethics review nor is equivalent to an HREC.

The ABS and PLIDA data custodians already provide substantial privacy, security and governance protections embedded within PLIDA, DataLab and custodian approval processes. The data ethics assessment requires researchers to provide additional assurances on the ethical aspects of a

proposed project that they uniquely control (public benefit and accountability, cohort impacts, and interpretation risks). This information provides clearer ethical context for data custodian project approval decisions.

Researcher onboarding process

[*Using DataLab responsibly | Australian Bureau of Statistics*](#)
[*Safe researcher training | Australian Bureau of Statistics*](#)
[*Conditions of use | Australian Bureau of Statistics*](#)

During the term of the Letter, the ABS will ensure that the linked data is used safely, responsibly and in line with data custodian approval. Access to the DataLab environment is available only to these types of users:

- government employees (including the ABS)
- government contractors and individuals sponsored by government
- academics
- researchers from public policy research institutes

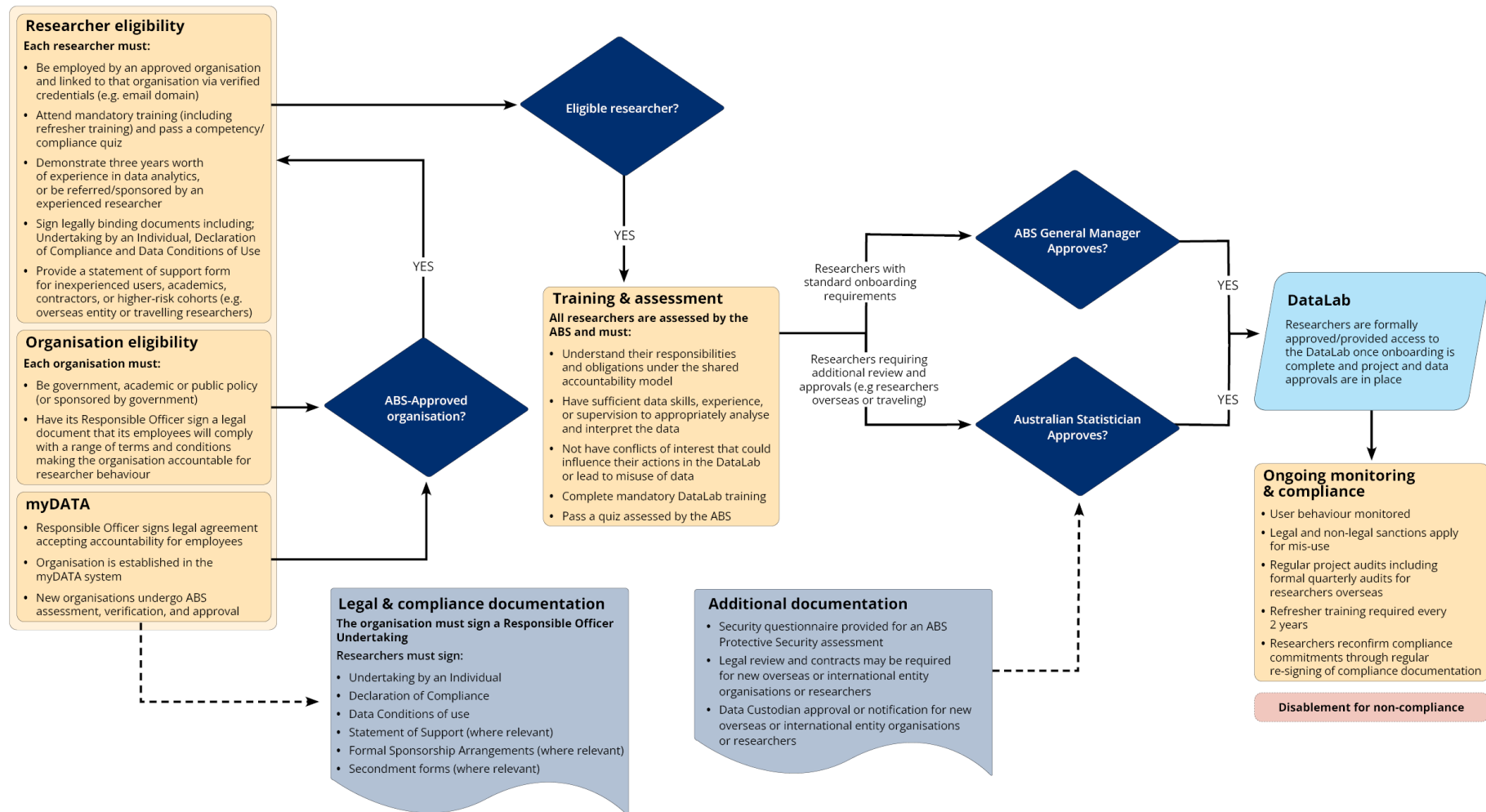
The [DataLab User Guide](#) outlines the requirements users must meet before access is granted. Authorised users requesting access to the linked data must:

- Conduct Safe Researcher Training and meet the conditions of use. [DataLab safe researcher training](#) provides an overview of the mandatory training and schedule.
- Meet the [requirements to become an authorised user](#).
- Agree to [use DataLab responsibly](#) and to protect the confidentiality of data.
- [Apply for access](#) to components of the Life Course Dataset that are project relevant. This involves data custodian approval processes to authorise access for that project.

The diagram below shows the general process.

The PLIDA Governance Guide

Figure 8. ABS DataLab researcher onboarding process



Offshore or overseas researcher access

The Australian Bureau of Statistics (ABS) supports DataLab access outside Australia as an ongoing and cost-recovered service. This initiative supports international collaboration and enables secure access to PLIDA by overseas researchers and organisations. In the Data sharing agreement, the data custodian must indicate if international access to their data is allowable under their legislation.

Custodianship and governance arrangements

Data custodians retain full custodianship of their data, ensuring that project access aligns with its governance frameworks and legal obligations. Where allowable, data custodians must approve all overseas projects involving foreign entities (see.

All applications are assessed under the Five Safes Framework, with additional controls tailored to overseas access risks. This ensures that data access and use remains safe.

Each overseas researcher undergoes a security and risk assessment by ABS security teams. Final approval is granted by the Australian Statistician ensuring high-level oversight and accountability. Applicants must provide:

1. A clear justification for overseas access.
2. Evidence of public value and benefit to Australia.
3. Organisational support, including endorsement from a senior leader or Responsible Officer.
4. Detailed information for a security risk evaluation (e.g., researcher location, access method).

Releasing data from the Datalab

[DataLab Clearance | Australian Bureau of Statistics](#)
[Using DataLab responsibly | Australian Bureau of Statistics](#)

Data confidentialisation process (output vetting)

During the term of the Letter, the ABS will require authorised users to request clearance of outputs from DataLab. This process ensures that all outputs released from DataLab maintain the confidentiality of individuals in accordance with the DataLab Clearance Rules.

PLIDA processes already include a range of technical and non-technical measures to ensure the risk of re-identification remains low. This includes the role of the ABS Disclosure Review Committee, making assessments against the Five Safes Framework, considering the risk of re-identification and recommending steps to minimise disclosure risk.

During the term of the Letter, to request clearance of outputs from the DataLab, users must use the clearance request tile in the myDATA portal. This process ensures that all outputs released from the DataLab are confidentialised in accordance with ABS legislation. The DataLab Clearance rules assist researchers to produce confidentialised outputs.

Output confidentialisation rules are robust and built to handle sensitive data like health data. This is the final check on the information before it is made public, which aims to reduce the risk of disclosure to a minimum. ABS statistical experts check all outputs for inadvertent disclosure before the data leaves the DataLab environment.

Research output review process

[Authorised users must provide any publication report and presentation](#) to the DataLab clearance team a minimum of 2 weeks prior to wider release. The DataLab clearance team then notifies relevant data custodians. This ensures the publication complies with any other requirements of the data custodian. Authorised users are sent any comments provided by data custodians on their publications.

When project teams use integrated data, they are required to **notify the ABS at least two weeks before publishing** any outputs. This requirement is part of the ABS's broader framework for data governance, confidentiality, and responsible data use. Any publication, report and presentation that references BLADE or PLIDA data needs to be provided to the ABS a minimum of 2 weeks prior to wider release. This is a requirement of our Data Custodians. This process does not seek approval from custodians but is in place to give custodians visibility of project outputs, provide comments and brief Ministers, as required. The governance team circulate to the project teams any comments or feedback received from custodians on circulated publications.

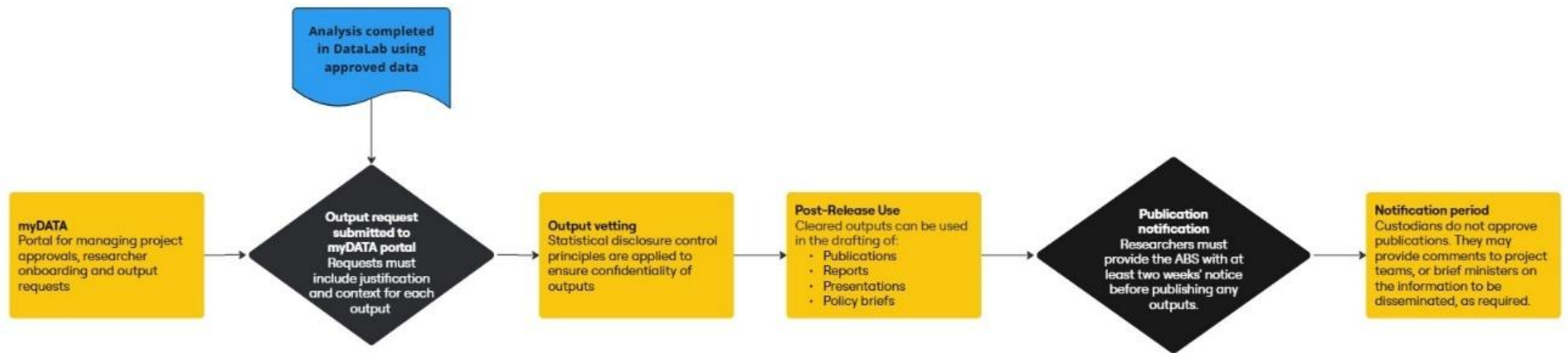
Below condition on the Project Proposal in myDATA is required to be read and acknowledged by every Project lead before a new project is accepted:

13.3 Acknowledgement of two-week notice of publication period (Required for projects requiring access to PLIDA and/or BLADE microdata).

Write the full name of the Project Lead to acknowledge you understand the above stated requirement that: you must provide two weeks written notice to the ABS (email mydataportal@abs.gov.au) of any pending publication of work from this project, including presentations at academic conferences.

Figure 9. Output vetting and publication process

Output vetting and publication process for DataLab



Retention and destruction of data

[DataLab | Australian Bureau of Statistics](#)
[DataLab user privacy notice | Australian Bureau of Statistics](#)

The ABS Deletion and Retention Policy is designed to support data governance and privacy across data integration infrastructure, systems, and services. ABS policy reflects our commitment to responsible data stewardship and aligns with recommendations from Privacy Impact Assessments (PIAs).

Custodianship and Governance

The ABS retains custodianship of all personal information collected through its services, ensuring compliance with the *Archives Act 1983 (Cth)* and relevant Records Disposal Authority (RDA) guidelines. While RDAs establish minimum retention periods, data destruction is only mandated under specific conditions, such as those related to security classification.

The **ABS Data Retention & Recordkeeping Policies** subsection **Retention of Personal Identifiers for Statistical Purposes Policy** govern the handling of personal identifiers. These identifiers include any received through input data, datasets, metadata, or unsolicited sources, and may be used in production design, research, or development activities.

The *Records Authority* and *Archives Act* define the requirements, roles, and responsibilities for the retention of in-scope personal identifiers.

Project Data in the DataLab

During the active phase of a project, all data is securely stored in its original form and is accessible only to authorised users.

Upon project closure, researcher data and personal information are archived 30 days post-closure unless otherwise specified. Archived data is retained for up to five years or until it no longer meets one or more of the following business needs:

- Facilitating collaboration
- Evaluating system usage
- Auditing processes
- Supporting reporting functions (e.g., systems, user behaviour, outputs)
- Enabling project governance and approval processes
- Supporting analysis for new product development
- Investigating potential or actual breaches, including legal and non-legal sanctions

All microdata and personal information are stored in certified secure cloud environments hosted in Australia, in accordance with the *Privacy Act 1988* and the ABS legislative framework. These environments meet the 'Protected' classification level, with risks mitigated through structured governance and secure system design.

Researcher Personal Information

As the administrator of the DataLab, the ABS collects personal information necessary to provide access.

This policy incorporates principles from the **Five Safes Framework**, specifically:

- **Safe People** – Only authorised personnel handle personal information
- **Safe Settings** – Data is accessed within controlled environments

Personal information is **retained** to:

- Authenticate and distinguish users
- Govern access to authorised data
- Support project governance and system audits
- Enable collaboration, reporting, and breach investigations

Deletion:

- Data is securely stored on certified Australian cloud infrastructure
- Personal information is archived 30 days after project closure
- Data is deleted after five years unless it continues to meet defined business needs
- Annual reviews are conducted by designated staff to assess ongoing relevance

Attachments

Legislative authority

[*PLIDA data and legislation | Australian Bureau of Statistics*](#)

The ABS collects data for PLIDA under the authority of the *Census and Statistics Act 1905*. This means:

- Information cannot be released in a manner likely to enable the identification of an individual or organisation
- ABS and seconded officers are legally bound to uphold the confidentiality of PLIDA information
- The ABS is required to publish and disseminate compilation and analyses of statistical information and to maintain the confidentiality of information collected⁹.

The ABS collects data for PLIDA from a range of different data custodians¹⁰. Legislative authority for sharing may come from the data custodian's:

- establishing legislation
- legislation relating to the original collection of the data
- specific data sharing legislation
- other legislation.

Accredited Data Service Provider documentation

[*ABS Accredited Data Service Provider \(ADSP\) Information*](#)

The ABS has been an Accredited Integrating Authority since April 2012. A copy of the application made by the ABS, verified by an independent auditor, is available on [Data.gov.au](#). This accreditation was maintained when the ABS became an Accredited Data Service Provider in July 2023 under the *Data Availability and Transparency Act 2022*. This ABS's accreditation under this scheme was renewed in February 2025.

How is data in PLIDA kept safe?

[*Keeping integrated data safe | Australian Bureau of Statistics*](#)

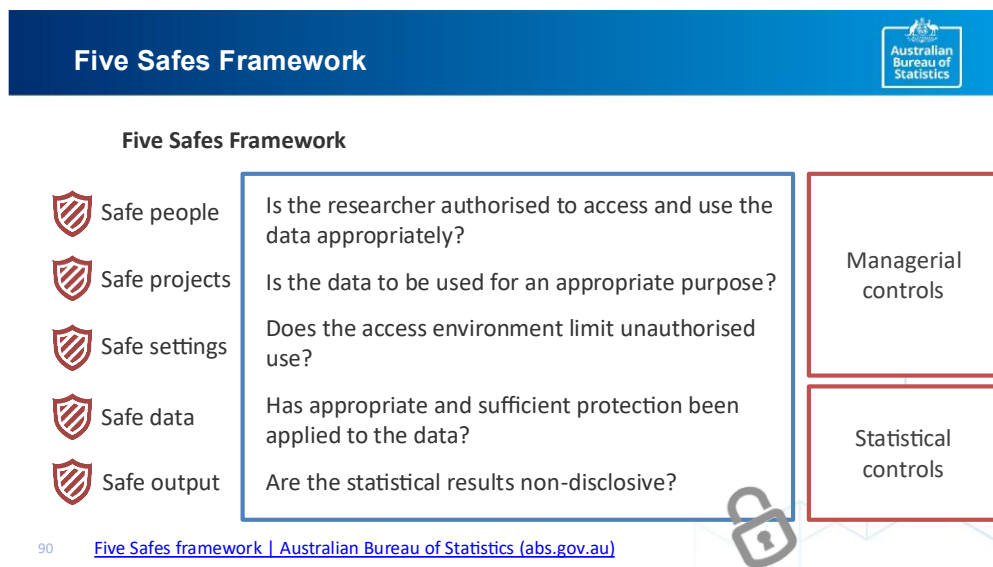
The ABS protects privacy and is committed to keeping PLIDA data safe and secure. PLIDA data is protected by the secrecy provisions of the *Census and Statistics Act 1905*. This means that the ABS cannot release PLIDA data in a way that is likely to identify an individual. For more information about how we protect your privacy, please see [Keeping integrated data safe](#) and [Privacy at the ABS](#).

The ABS enforces a robust framework of protections for PLIDA which includes⁹:

- **Legislative protections:** PLIDA is compliant with all relevant legislation including the *Census and Statistics Act*, which applies to data brought into the ABS for the purposes of the data integration. The secrecy provisions of this Act offer strong legislative protections which

ensure personal information remains strictly confidential. This means the ABS is obligated under legislation to ensure the information we bring in 'cannot be released in a manner which is likely to enable a person or organisation to be identified'. The penalty for breach of these provisions is up to 2 years imprisonment and/or fine of \$25,200.

- **Privacy protections:** The ABS takes a 'privacy by design' approach. PLIDA complies with the Privacy Act 1988 and with the legislative requirements of each party whose data is involved, and is consistent with the Australian Privacy Principles (APPs).
- **Policies and standards:** The ABS also adheres to the Australian Government standards for information, personnel, and physical security, including using the separation principle and data minimisation.



Safe data handling practices - the ABS has adopted the Five Safes Framework to enable secure access to data for authorised users only. These include:

1. Safe people – researchers must undergo training and be approved by all data custodians
2. Safe projects – research proposals are assessed by ABS and data custodians. (For example, a project seeking to monitor compliance is not in the public interest will not be approved.)
3. Safe settings – the ABS uses secure IT and physical environments for access and storage.
4. Safe data – the data is deidentified before researchers are allowed access (meaning names and addresses are removed)
5. Safe outputs – analytical outputs (such as data tables) are vetted by the ABS before being released to researchers. This ensures no data is released in a manner likely to enable the identification of an individual or organisation.

PLIDA Data Item List

The latest PLIDA Data Item List - Can be found at the bottom of this webpage:

[Microdata: Person Level Integrated Data Asset \(PLIDA\) | Australian Bureau of Statistics](#)

ABS Data Storage Environments

During the term of the Letter, the linkage (Linkage Data) and analytical (Family File) data will be transferred separately to the ABS using secure file transfer protocols, where the data is encrypted using robust encryption standards to prevent interception and unauthorised access. This ensures that even if the data is intercepted it cannot be read or tampered.

Upon receiving the data, the ABS will store the supplied data in its restricted secure data integration environments. These environments have had Multiple Independent Security Registered Assessors Program (IRAP) assessments completed. Each of these environments provide the ABS with additional layers of control to reduce residual risks relating to the privacy and confidentiality of data supplied to it.

ABS Data Breach Protocol

A data breach occurs when data that is held by the ABS is lost, accessed, disclosed, or used without authorisation. This includes incidents involving:

- unauthorised access or disclosure;
- accidental release or loss of data;
- cyber-attacks or system compromises;
- receipt of unsolicited data;
- breaches involving data shared externally by the ABS.

The ABS has a formal Data Breach and Incident Response Plan (DBIRP) that outlines procedures for identifying, containing, assessing, remediating, notifying, and reviewing data incidents. The Plan ensures compliance with the Privacy Act 1988, the [Notifiable Data Breaches \(NDB\) Scheme](#), and the Data Availability and Transparency Act 2022 (DATA Scheme).

What Data Custodians Can Expect

In the unlikely event of a data breach involving data provided by a custodian, the ABS will:

1. **Notify the Custodian Immediately**
The ABS will provide written notification detailing the nature of the breach, the data involved, and any known impacts.
2. **Contain and Remedy the Breach**
The ABS will take all necessary steps to contain the breach and prevent further unauthorised access or disclosure. This includes technical containment, forensic investigation, and mitigation actions.
3. **Provide Reasonable Assistance**
The ABS will support the custodian in responding to the breach, including:
 - Coordinating communications;
 - Sharing incident documentation;
 - Assisting with legislative or contractual reporting obligations.
4. **Comply with Legislative Obligations**
The ABS will assess whether the breach meets the threshold for notification under the NDB Scheme and, if so, notify:
 - The Office of the Australian Information Commissioner (OAIC);
 - Affected individuals;
 - The Office of the National Data Commissioner (ONDC), if DATA Scheme data is involved.
5. **Coordinate Multi-Entity Responses**
Where a breach involves multiple entities, the ABS will work with affected parties to determine lead responsibilities and ensure a coordinated response, including consistent public messaging.
6. **Review and Improve**
Following the incident, the ABS will conduct a post-incident review to identify root causes, assess response effectiveness, and implement improvements. Custodians may be invited to participate in this review if their data was involved.

Custodian Responsibilities

Custodians should:

- Ensure their own internal data breach protocols are compatible with ABS processes;
- Review any relevant Data Sharing Agreements, MoUs, or Letters of Exchange for notification obligations;
- Be prepared to engage in joint incident response and public communication if required.

ABS Security

The ABS's data integration systems and processes:

- comply with Australian Government standards for information, personnel and physical security;
- conform to the IT security arrangements set out in the [Information Security Manual](#) (ISM) produced by the Australian Signals Directorate; and
- comply with the [Australian Government Protective Security Policy Framework](#) (PSPF).

During the term of the Letter, the ABS will maintain security practices to protect all the data supplied to it, including:

- all information technology systems will conform with technical security requirements defined by the ISM;

- strict physical security controls will cover access to ABS premises as per the Australian Government PSPF;
- all ABS officers must comply with personnel security arrangements, which may include:
 - undergoing security checks on engagement;
 - signing an Undertaking of Fidelity and Secrecy under the C&S Act; and
 - obtaining a baseline security clearance prior to access being granted to the ABS's secure data integration processing environments.
- maintaining a secured internet gateway, which is reviewed annually by the Australian Signals Directorate;
- conducting regular protective security risk reviews to ensure security arrangements remain effective; and
- ongoing security audit and review programs covering computer systems and the physical environment.



www.abs.gov.au