Australian Bureau of Statistics

The PLIDA Governance Guide

February 2026

Contents

Introduction

Purpose of this document

Welcome, new or prospective data custodian! This document provides key information about the governance of the Person Level Integrated Data Asset (PLIDA).

These guidelines are a combination of legislated protections and accreditations and reflect historical decisions made by the Australian Statistician, informed by public consultation and advice from the PLIDA Board. Changes to this document 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 data safely and securely. It helps data custodians 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 includes links to the ABS website and references to process flows. The ABS also maintains Standard Operating Procedures that underpin each process described here. These can be shared if requested. These guidelines support your organisation's own privacy and ethics approvals for sharing data into PLIDA.

Please note: This document is not intended for data custodians who do not permit data re-use. While many governance protocols still apply, custodians seeking custom integrations should contact the ABS directly.

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 provides insights into our society, economy and environment. These insights support important research and help 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 ABS surveys, and from other government agencies.

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

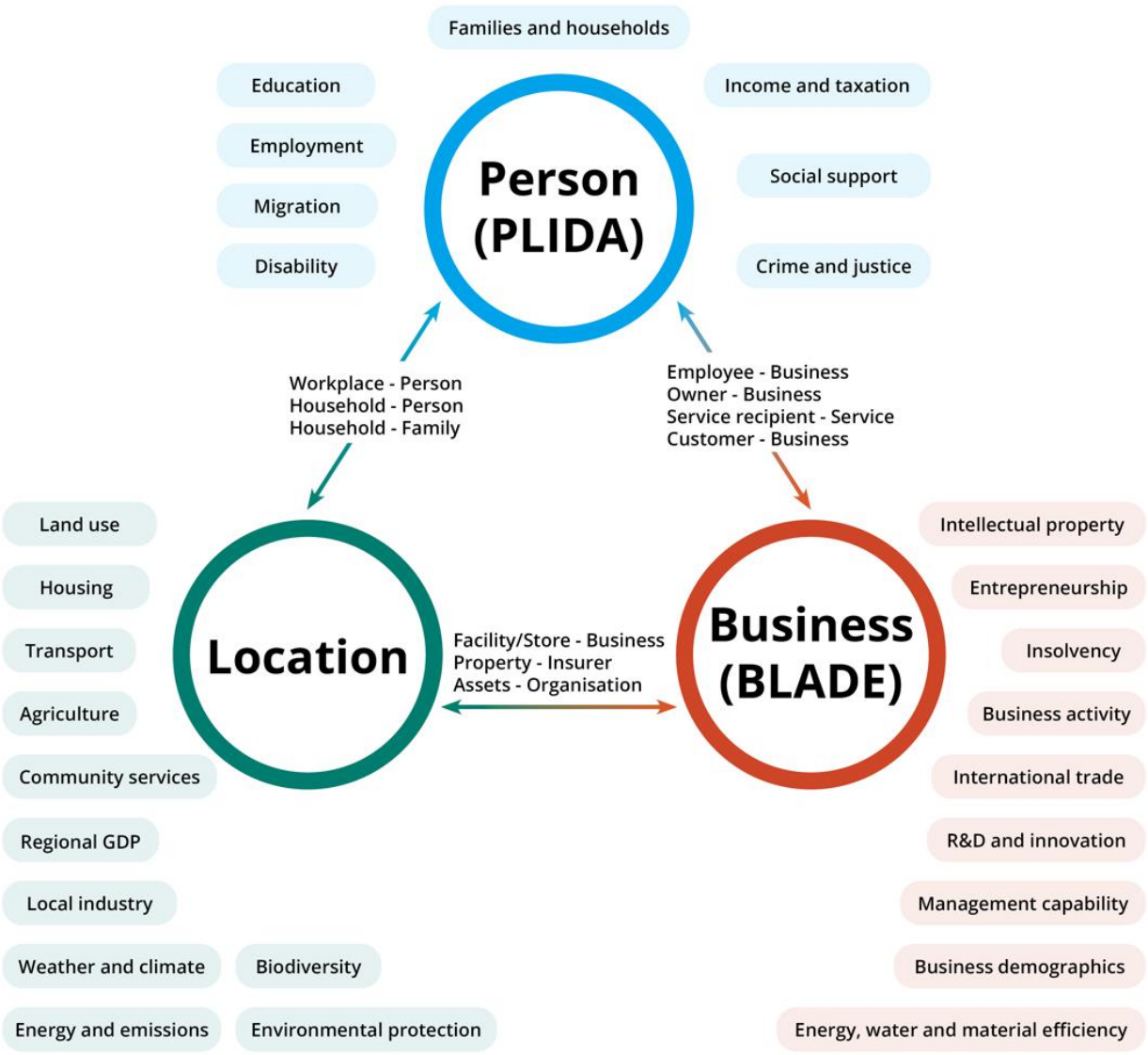
What is the Person Level Integrated Data Asset or PLIDA

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 provide a comprehensive picture of Australia over time.

Initiated in 2015, PLIDA delivers whole-of-life insights about various population groups in Australia, including their characteristics, use of services such as healthcare and education, and outcomes like improved health and employment.

As an Accredited Data Service Provider, the ABS collects and integrates these datasets, provides access to authorised researchers, and protects privacy and keeps information secure at all times.



What PLIDA can and cannot be used for

Five Safes framework | Australian Bureau of Statistics
Using DataLab responsibly | Australian Bureau of Statistics
Data integration project register | Australian Bureau of Statistics

Permissible uses of PLIDA include:

1. Research and analysis for approved project purposes, such as:
    - Addressing policy questions
    - Conducting program evaluations
    - Undertaking empirical research
    - Informing decisions related to the allocation 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, minimise any potential impact on privacy and confidentiality, and are ethical and transparent.

Data integration projects are assessed by ABS to ensure they:

- Provide significant benefit to the public
- Are only conducted for statistical and research purposes (not for commercial gain or compliance, or regulatory purposes)
- Minimise any potential impact on privacy and confidentiality
- Are transparent – the datasets and research purposes are published on the ABS website
- Do not involve unethical use of data, or request information that is not aligned with the stated project objectives
- Do not use datasets in ways that conflict with legal or policy requirements, or exceed obligations agreed upon by data custodians or the ABS.

For more information about project assessments, responsible data use, and current data integration initiatives, please refer to the links above.

The ABS currently uses PLIDA data in a range of its own publications, including Census-related outputs that are publicly available. A PLIDA TableBuilder product is also in development and is expected to be available by mid-2026.

Benefits for data custodians

PLIDA enables better use of information that has already been collected. By combining administrative datasets, survey datasets and the 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 existing data we can save you over $100m and 10-12 years of work required to set up similar research infrastructure.
- The data is pre-linked but 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. The ABS has a solid track record in maintaining 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. You can redirect data access requests to the ABS. 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 subsidised and high capability service that saves people the effort of building this technical and governance infrastructure themselves.
- Research opportunity. As a data custodian, you also get access to the same DataLab services, with options for a subsidy to some custodians who conduct DataLab projects and support ongoing, broad access including re-use (to be negotiated as part of the data sharing agreement).
- Collaboration opportunity. As a researcher you can also use our secure DataLab system to work with approved project team members in a safe and secure way, you can collaborate with others to join or deliver your projects. Data custodians are also provided with access to researchers’ draft publications to keep abreast of how the data is being used.

Governance Principles

PLIDA operates under a rigorous governance structure designed to ensure security, cultural integrity, privacy, and ethical compliance. Key components include:

- Five Safes framework assessment
- Cultural reviews undertaken by the ABS Centre of Aboriginal and Torres Strait Islander Statistics (CoATSIS)
- Privacy assessments (including Privacy Threshold Assessments and Privacy Impact Assessments)
- Tracking ethics approvals for projects that require review, ensuring compliance and transparency
- Approval by data custodians.

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 currently 37 datasets that form the core PLIDA Modular Product, and the ABS has linked, or is in the process of linking, more than 80 additional datasets for specific projects.

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

The diagram below provides an overview of PLIDA co-governance.

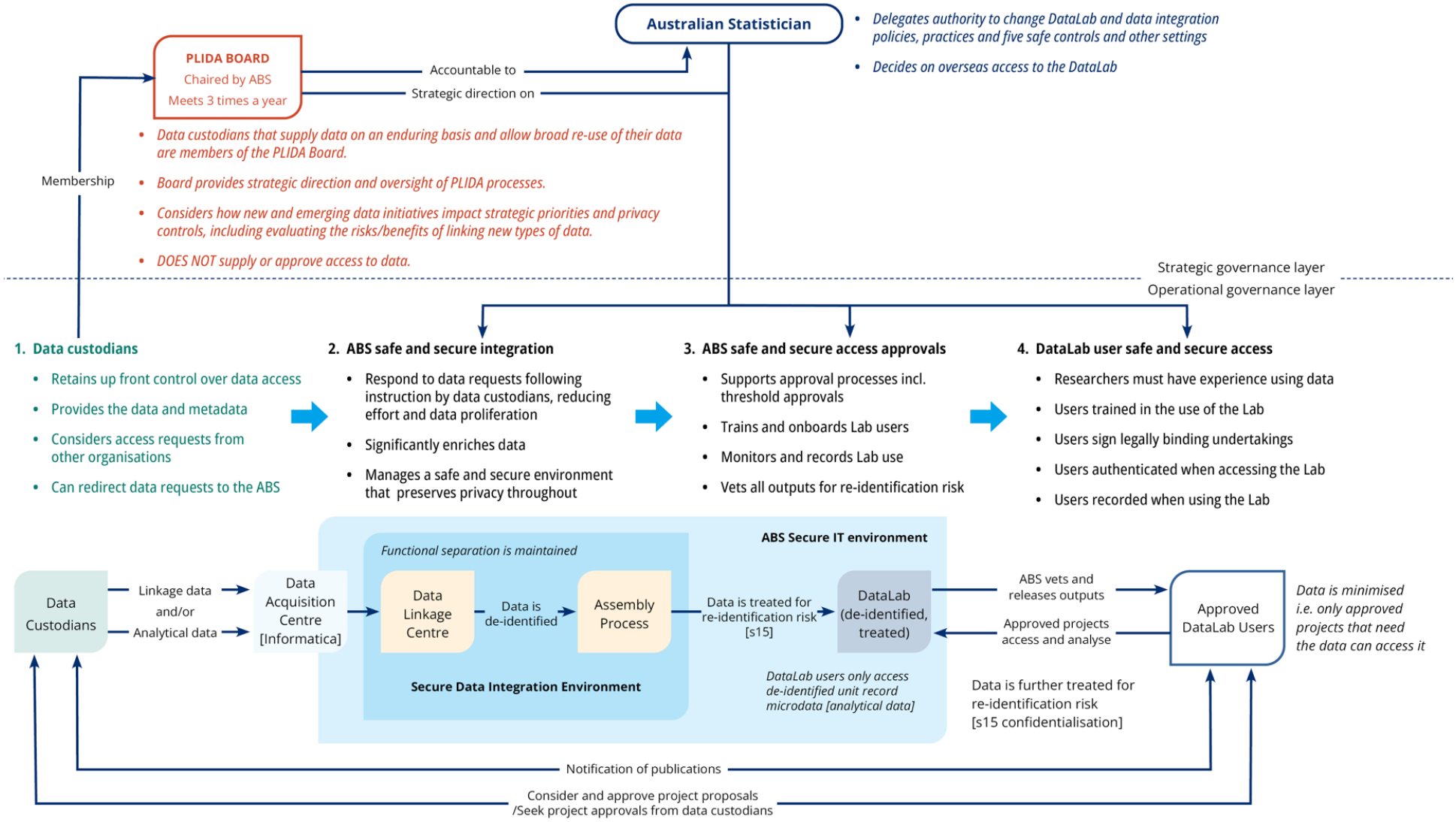
Data custodians supply datasets and metadata via a secure file sharing platform. Keeping the linkage and analytical data separated at all times, the ABS undertakes linkage and assembly work to transform the dataset into a pre-linked and de-identified PLIDA Module in the PLIDA Modular Product. Any Safe Data controls are applied at this stage.

All new data integrations will be undertaken in a secure cloud-based infrastructure: the Secure Environment for Analysing Data (SEAD) and/or the Australian National Data Integration Infrastructure (ANDII).

Once delivered, information on the new PLIDA Module is findable in myDATA for approved researchers to submit access requests. The Data Custodian is notified of new access requests. If approved, the 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. Before publishing, researchers must notify both the ABS and data custodians, giving custodians the opportunity to review and comment on findings and interpretations.

An overview of PLIDA co-governance



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 at all stages. This approach reflects the ABS's obligations under the *Privacy Act 1988* (Privacy Act), 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:

1. 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 Privacy Impact Assessments (PIAs) to identify and mitigate emerging risks.

2. 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 and the Australian Privacy Principles (APPs). Safe Data Risk Assessments are also used to evaluate reidentification risks.

3. 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 notification of the proposed integration, 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

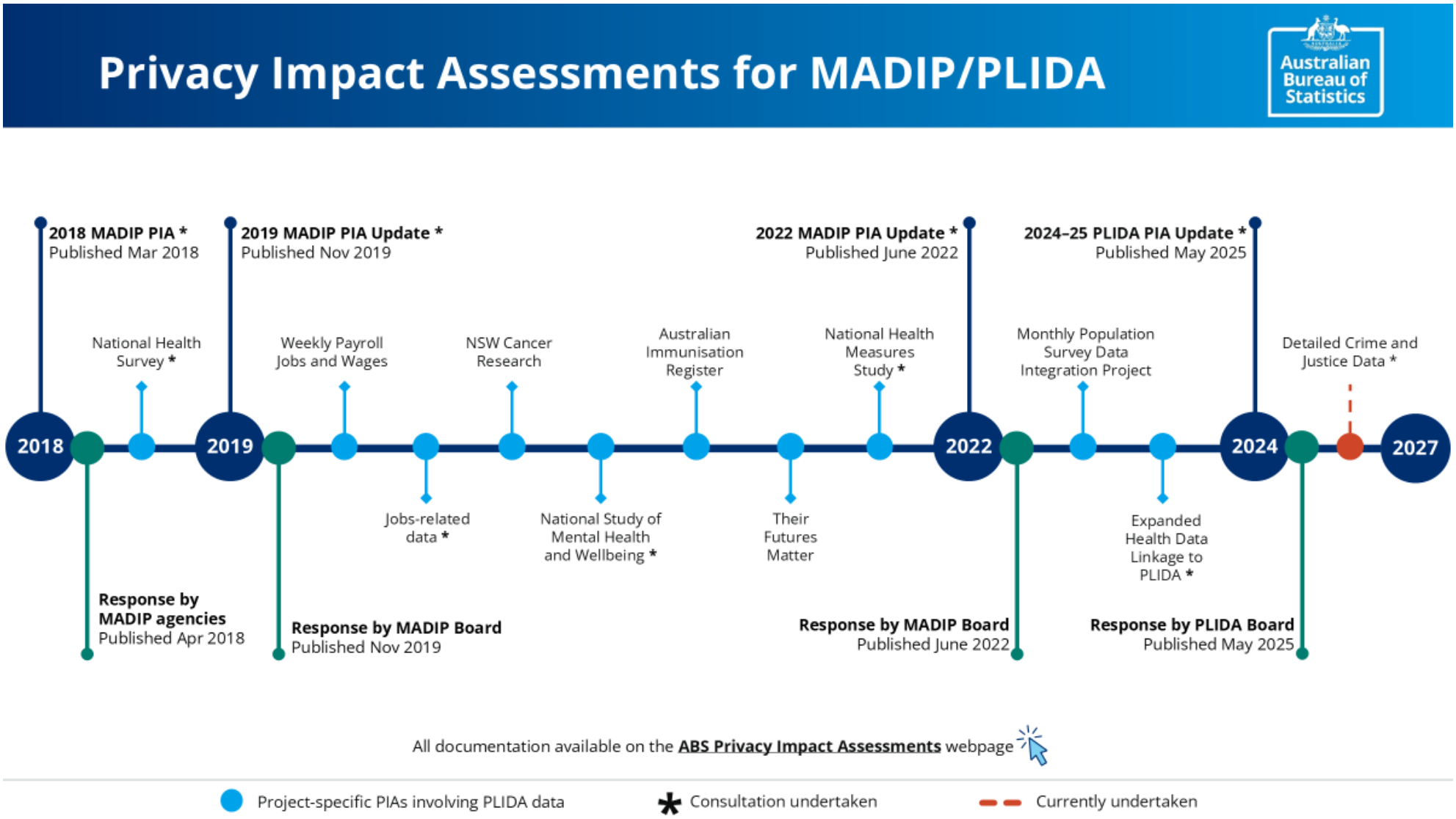
The PLIDA Privacy Statement outlines the specific privacy practices applied to PLIDA. It describes how personal information is managed within the asset, including safeguards around data integration, access controls, and the use of de-identified data for research and statistical purposes.

3. Privacy Threshold Assessments (PTAs)

The ABS is required to review re-identification risk when a new type of linkage or a new type of data asset is requested to be linked. 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.


Privacy Impact Assessments for MADIP/PLIDA
Australian Bureau of Statistics
2018 MADIP PIA *
Published Mar 2018
2019 MADIP PIA Update *
Published Nov 2019
2022 MADIP PIA Update *
Published June 2022
2024–25 PLIDA PIA Update *
Published May 2025
National Health Survey *
Weekly Payroll Jobs and Wages
NSW Cancer Research
Australian Immunisation Register
National Health Measures Study *
Monthly Population Survey Data Integration Project
Detailed Crime and Justice Data *
2018
2019
2022
2024
2027
Response by MADIP agencies
Published Apr 2018
Response by MADIP Board
Published Nov 2019
Jobs-related data *
National Study of Mental Health and Wellbeing *
Their Futures Matter
Response by MADIP Board
Published June 2022
Expanded Health Data Linkage to PLIDA *
Response by PLIDA Board
Published May 2025
All documentation available on the ABS Privacy Impact Assessments webpage
Project-specific PIAs involving PLIDA data
Consultation undertaken
Currently undertaken

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 of Exchange (LoE), the ABS will apply privacy-by-design practices, which include:

- Conducting PTAs for all new PLIDA data linkage proposals and projects
- Conducting PIAs where a proposal or project is assessed as having a medium to high privacy risk or requires additional transparency measures. The ABS also conducts periodic updates of the independent PIA for PLIDA
- Applying the seven High Level Principles for Data Integration to 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 always stored separately from other information, and no individual 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.
- Ensuring linkage information is never made available to authorised users for research purposes
- Maintaining an ongoing program of security audits and system accreditations.

Protocols ensure FAIR principles are met

These governance protocols are designed to uphold the internationally recognised FAIR principles - Findable, Accessible, Interoperable, and Reusable, ensuring that integrated data is managed transparently and securely. Applying FAIR principles to PLIDA maximises the value of data by improving discoverability, enabling safe access, and supporting efficient reuse for research and policy development.

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

Accessible –Your linked data will be available for researchers to request through myDATA. Once approved, the data will be made available to projects in the secure ABS DataLab. Only confidentialised or aggregated data can leave or exit the DataLab.

Interoperable – PLIDA is not a single, integrated dataset. It consists of discrete pre-linked files *or Modules* with identifiers that enable integration with other PLIDA Modules. Researchers can only access analytical information in a de-identified format.

Reusable – The ABS applies a *supply-once, use-many-times* approach to data integration. Data linked to the Person Linkage Spine can be re-used in projects where approved by data custodians, reducing duplication and improving efficiency.

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 meets three times a year, and reports directly to the Australian Statistician. The Board is chaired by an SES Band 2 Officer from the ABS.

The PLIDA Board provides strategic direction and oversight of 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, and supplying data does not inherently result in board membership.

The PLIDA Board oversees the PLIDA Working Group, the PLIDA Technical Advisory Group, and other working groups as required. It considers advice from these groups and may seek input from other forums when necessary.

The PLIDA Board reviews how new and emerging data initiatives impact strategic priorities and assesses the risks and benefits of linking additional types of data to PLIDA. These decisions are 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.

PLIDA Board membership

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 can become members of PLIDA Board. However, you do not need to be a data custodian to be a PLIDA Board member or observer.

ABS is open to additional members of the Board. To nominate a representative of a data custodian for PLIDA Board membership, please email mydataportal@abs.gov.au expressing interest. Nominations are considered by the Australian Statistician. Alternatively, the Australian Statistician may invite membership.

Once a membership application is approved, appointment is immediate, and the membership will remain ongoing. The ABS Secretariat will contact the new Board member to provide an orientation briefing on the Board. The Board member will be invited to the next available meeting, and will receive meeting papers and recent minutes.

The PLIDA Board structure and terms of reference of the Board are available on the PLIDA Board webpage. Membership and associated voting rights can be included in a data sharing agreement with prior agreement from the Australian Statistician.

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

What is my role as a PLIDA data custodian

As a PLIDA data custodian, you will enter into a Data Sharing Arrangement (DSA) with the ABS. This arrangement outlines key expectations for both parties. For public sector entities, DSAs typically take one of two formats:

- Memorandum of Understanding (MoU)
- Letter of Exchange (LoE).

Neither format is legally binding, meaning they can be terminated if circumstances change. DSAs are deliberately non-prescriptive because ABS activities are governed by legislation, including:

- *Australian Bureau of Statistics Act 1975* (ABS Act)
- *Census and Statistics Act 1905* (Census and Statistics Act)
- *Privacy Act 1988* (Privacy Act).

These Acts are referenced in DSAs.

The ABS will destroy data when directed or required under the DSA or the *Archives Act*. Analytical information is not retained indefinitely - once deleted, data cannot be reverified. Retention and destruction decisions follow the DSA.

What does a Data Sharing Agreement (DSA) look like

A Letter of Exchange (LoE) template can be found as a separate download at the bottom of this webpage. The LoE describes the mechanisms that allow for data sharing from the custodian and collection by the ABS.

The usual steps involved are:

1. **Drafting:** The ABS prepares an initial draft document using information provided in the Data Integration Request.
    - If desired, the ABS can use the data custodian's own DSA template but will require additional time to review and include standard required clauses (e.g. ABS security measures, privacy clauses, data breach handling etc)
    - Draft details include:
        - Dataset name(s), data reference period(s), timing of supply
        - Name of agency supplying data, method of transfer, access arrangements for the data (e.g. available for reusable or project-specific)
        - Legal mechanism enabling data supply and/or on-sharing of data
        - Additional custodian requirements, dispute resolution terms, identified Liaison officers in both organisations
        - Privacy measures (e.g. Separation Principle), security and data breach measures.
    - A Data Item List detailing the contents and format of the to be supplied data must be attached to the agreement, therefore this information needs to be confirmed before the final agreement can be signed.
2. **Terms:** For ongoing arrangements, the DSA would include a clause for termination as well as regular review points. Usual terms cover the following:
    - The agreement will be effective from the date of signing with an agreed length of time, unless terminated earlier:

- by the Parties at any time by mutual arrangement; or
  - by either party giving the other party 30 working days written notice
  - an agreed review clause specifying the frequency that the agreement would be reviewed (e.g. every 3 years).

3. **Review and signing:** The draft agreements will be sent to the data custodian for initial review and further discussion as needed. 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.

4. **Technical setup**: If the data will be transferred using the ABS's 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.

PLIDA data custodians provide information 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.

Intellectual property rights are covered in the data sharing agreements. Each data custodian shall continue to own the Intellectual Property (IP) of their Background IP. The ownership of all Project IP created by a project (the creator) will be the property of the creator unless otherwise agreed in writing.

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.

Information about data supply including how to prepare and validate data for linkage is described in the PLIDA Data Supply Guidelines available for download on the Guidance for data custodians page.

What data is collected from data custodians

The ABS collects two broad types of information for PLIDA:

- **Linkage information** - data as supplied by the data custodian as per the DSA and LoE, and 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.
- **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).

The ABS restricts access to personal identifiers for the purpose of data integration and applies the internationally recognised best practice known as 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) are kept separate at all times (i.e. these two types of data are never used at the same time or seen together).

Different supply options for PLIDA

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

- **Reusable:** The data will be integrated with PLIDA and can be requested 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 usage.
  The data sharing agreement permits access and use without requiring renegotiation or resupply. It is the ABS's preference to establish reusable 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.

Additional or non-standard governance processes over and above what the ABS already delivers

The ABS governance model and processes are designed to apply to all data accesses and are co-designed with data custodians. Non-standard governance controls should be negotiated with the ABS.

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 LoE.

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 PIA 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.

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. Access is subject to approval by PLIDA data custodians which is facilitated through the myDATA platform. Researchers from data custodian organisations are not treated any differently from other researchers.

Once a PLIDA Module is created, it is listed as available for request in the myDATA platform. 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.

Researchers can then request access to the Module by completing the ABS DataLab project proposal in myDATA for detailed and integrated microdata.

Requests for approval to access each PLIDA Modular Product (PMP) 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.

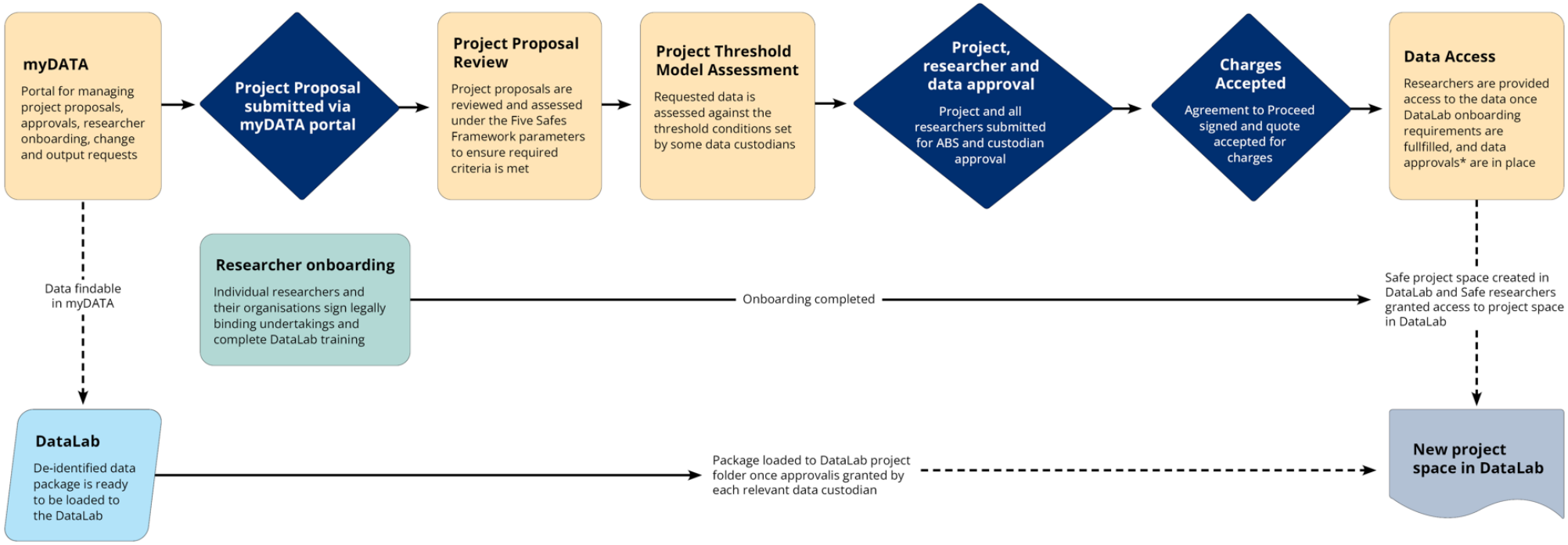
Instances may arise where custodians are asked to re-approve a project or approve changes to a project. These include but are not limited to:

- Major changes in project scope, aims, objectives, methodology or expected outcomes
- Relevant changes to ethics and access to sensitive data
- Access outside of Australia, including overseas projects involving overseas entities.

Data needs are determined following consultation between the ABS and researchers (the data users). Approval is sought from custodians for each project seeking to use their data. It is recommended that custodians consider using the PLIDA threshold model 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.

The below diagram shows the approval process.

Data Custodian Approval Process for PLIDA Modular Products (PMPs)
as part of the ABD Data Integration process flow



*Where data in a package requires multiple custodian approvals, data access will not be granted until all custodians have approved.

Researcher support

Where possible, the ABS supports technical queries from researchers. Occasionally, the ABS asks data custodians to help respond to highly technical questions.

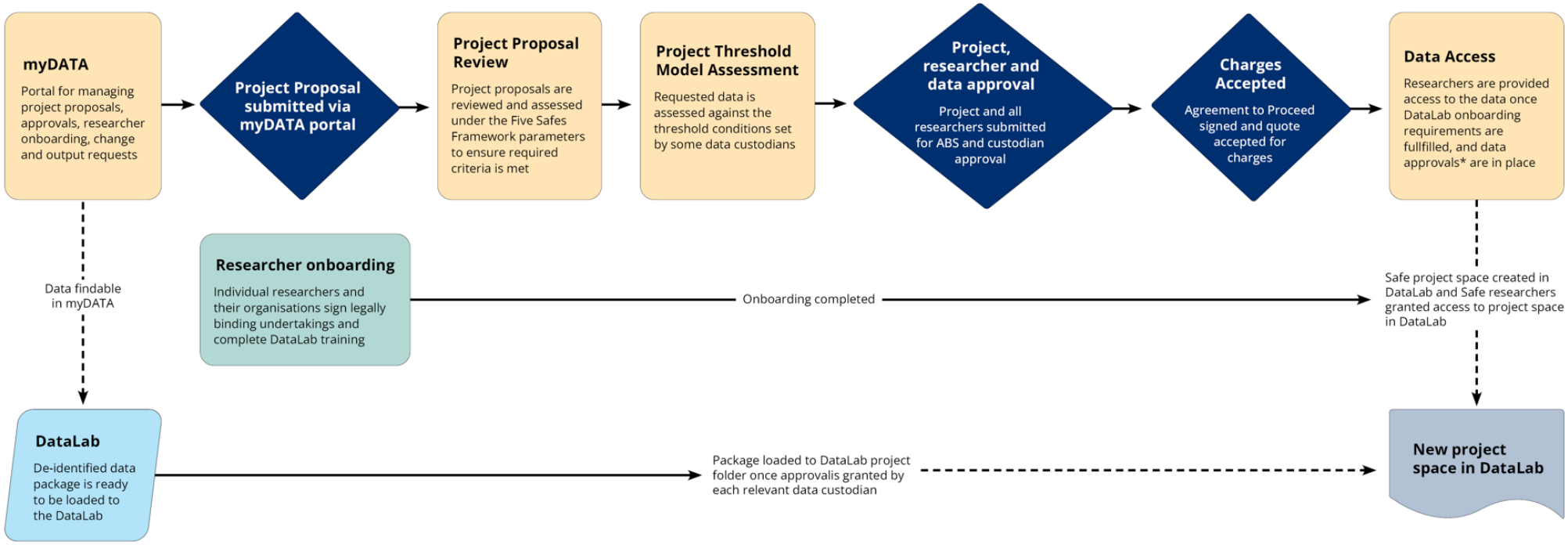
Data Custodians are also given the opportunity to review draft publications produced by researchers prior to official release.

Enduring Multipurpose Programs (EMPs)

The ABS is piloting EMPs under the oversight of the PLIDA Board. These EMPs are designed to streamline aspects of governance controls for government agencies. These include:

- Reduced timeframes and real-time analyses.
- Projects can implement changes without requiring custodian re-approvals or lengthy timeframes, enabling faster responses to urgent ministerial or policy questions. Researchers can request datasets upfront without linking them to specific research questions, provided they align with the project's broad purpose – Data custodians are generally inclined to approve these. However, any additional dataset requests beyond the initial scope will still require custodian approval.
- Projects offer a broad scope rather than focusing on detailed research questions. They allow early access to data and enable the release of outputs without the standard two-week custodian review. Publication notification is only waived when the vetted output is shared with Ministerial Officers and other government agencies.
- While some 'Safe project' criteria have been softened, there are new strengthened 'safe people' criteria such as SES project sponsorship to offset this.
- Overseas access is not supported.

Data Custodian Approval Process for PLIDA Modular Products (PMPs)
as part of the ABD Data Integration process flow



*Where data in a package requires multiple custodian approvals, data access will not be granted until all custodians have approved.

Data Integration Process

Data integration is carried out in clear steps or phases. These are outlined below.

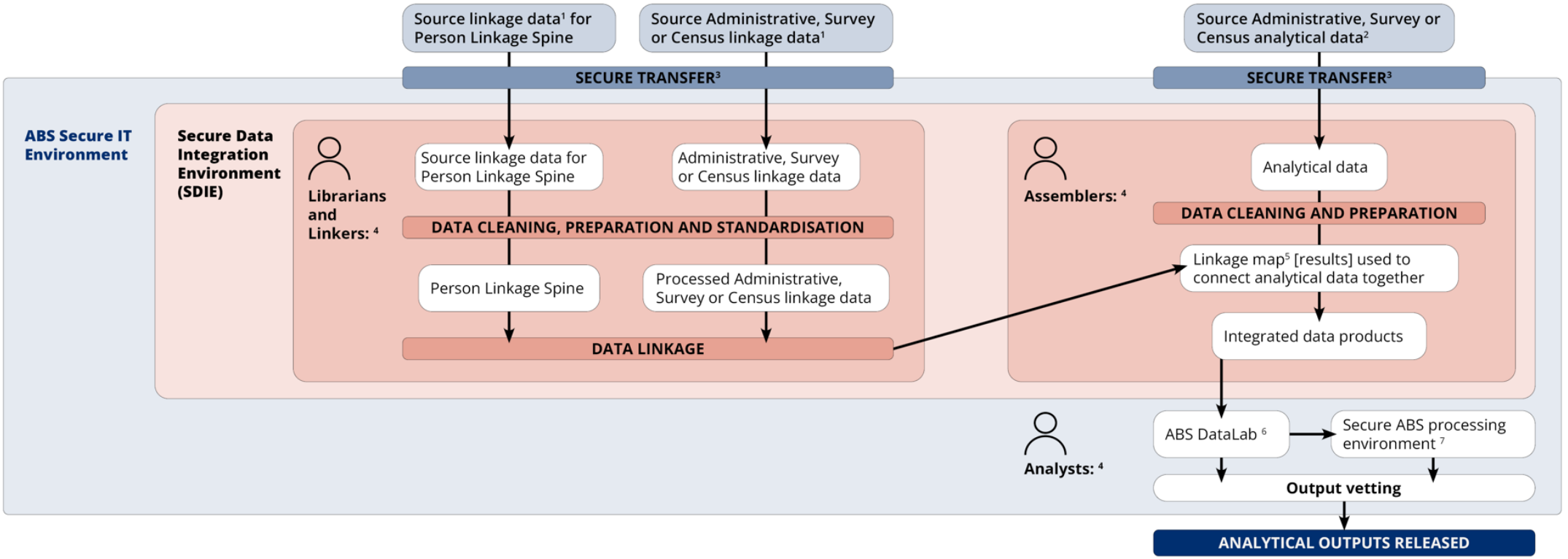
Data linkage

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.

- 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.

PLIDA Data Flow



1. **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.
2. **Analytical Data:** variables of interest for analysis, such as occupation, income and health services use, or business type and industry.
3. **Secure transfer:** data is supplied to the ABS via an accredited secure transfer method as agreed with data custodians.
4. **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.
5. **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.
6. **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.
7. **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)

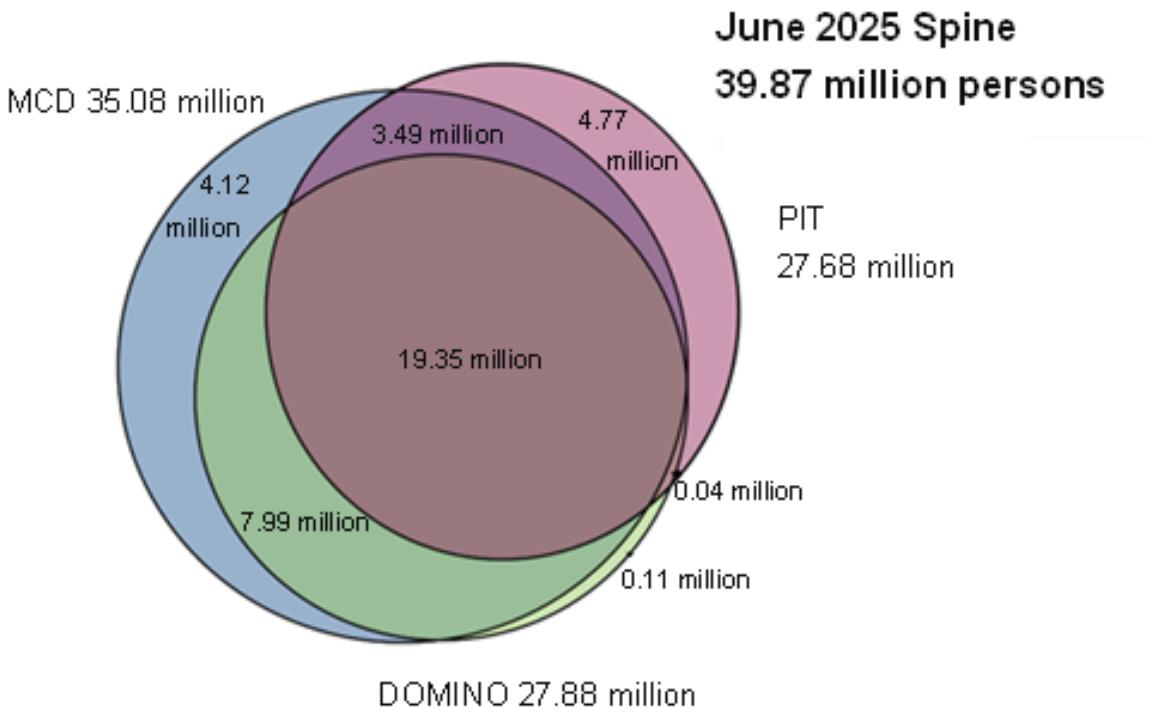
The Person Linkage Spine is central to our data linking methods. Instead of linking datasets one-to-one for individual projects, we can link all datasets to the Spine once and then combine datasets via the Spine as needed for multiple projects. The Spine enables more efficient and higher quality linkage. 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 current Spine comprises 39.87 million unique persons.



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 undergo 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 may 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 process acts as an ethical hack process to identify the prevalence of unique individuals who may be easily identifiable in the public domain and recommends additional measures to further suppress the dataset (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).

Data approval and loading into DataLab

The Statistician holds ultimate responsibility for approving the release of data, taking into account advice provided by the Chief Methodologist. To support this process, the Disclosure Review Committee (DRC) was established to advise the Chief Methodologist on disclosure risks and appropriate mitigation strategies related to the dissemination of data.

Under ABS policy, all proposed data releases must be reviewed by the DRC. In assessing disclosure risk, the committee considers not only the data itself but also the circumstances and environment in which the data will be accessed. The DRC uses the Five Safes Framework as a guiding approach for these assessments.

To ensure confidentiality, the DRC applies key principles including Legality, Risk Management, Comprehensive Assessment, and Continuous Improvement. These principles help the committee evaluate disclosure risks and ensure compliance with Commonwealth legal requirements under the Census and Statistics Act. Additionally, the DRC implements measures to mitigate risks such as data matching and recognition.

PLIDA data products

The ABS makes various PLIDA products available to approved researchers to help support their analysis.

PLIDA Modular Product

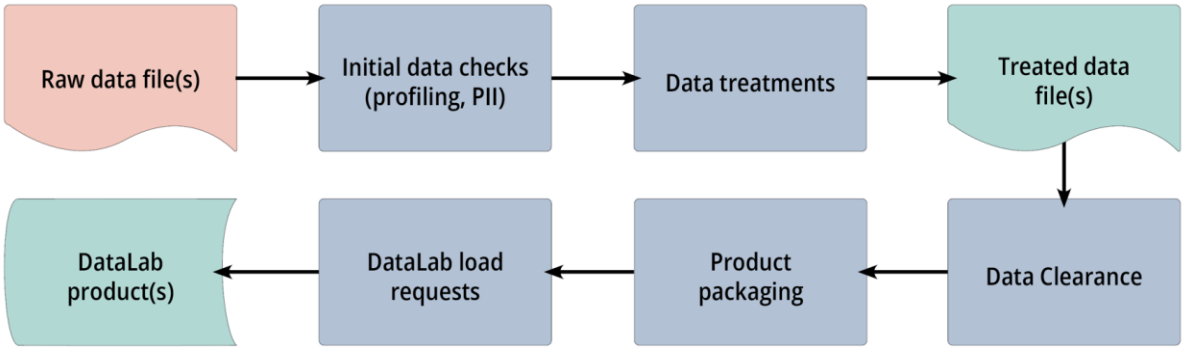
Microdata: Person Level Integrated Data Asset (PLIDA) | Australian Bureau of Statistics

From the linkage and assembly process described above, the ABS creates a detailed microdata product from your dataset, which is added to the PLIDA Modular Product (PMP). 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) that researchers can select based on their project needs.

All access to PLIDA data is via the PMP, which is made available to approved researchers in the ABS DataLab. Researchers request access to specific modules by completing the ABS DataLab project proposal for detailed and integrated microdata in myDATA. Access is subject to approval by each PLIDA data custodian which is facilitated through the myDATA platform.

Modules are approved individually by their respective custodians. Only the modules required for an approved project are provided to researchers.

The diagram below illustrates the process for the creation of the PLIDA Modular Product.



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, eliminating the need to access each 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 for 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 a single table. The Core Modules draw key information from a range of different datasets in PLIDA and make them available in the one place.

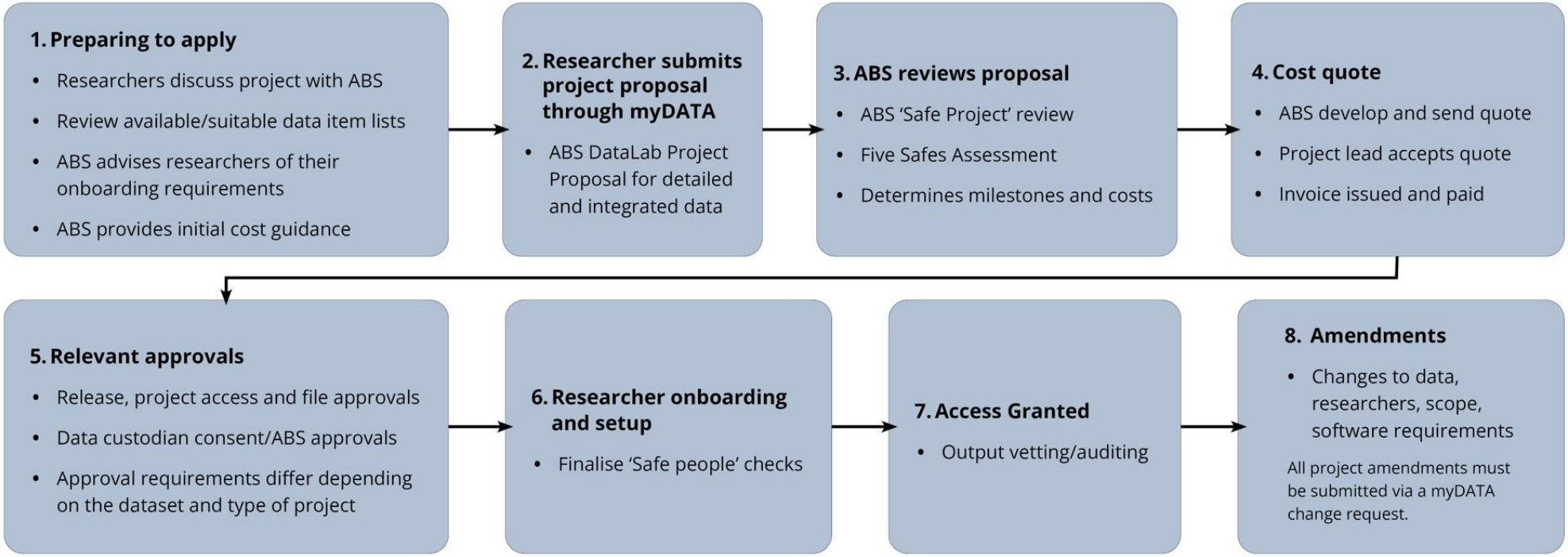
PLIDA Data Item List

The latest PLIDA Data Item List can be found here: Microdata: Person Level Integrated Data Asset (PLIDA) | Australian Bureau of Statistics.

Access to PLIDA through the ABS DataLab

Accessing integrated data | Australian Bureau of Statistics
DataLab | Australian Bureau of Statistics

ABS standard access process – microdata in the DataLab



Access to PLIDA through the ABS DataLab

During the term of the LoE, the ABS will provide authorised users with access to the linked data through the ABS DataLab environment. Jurisdictions access their own and other Commonwealth PLIDA data through this mechanism.

DataLab is hosted in Microsoft Azure and meets PROTECTED level security standards, as prescribed in the Information Security Manual (ISM). The DataLab environment is subject to Independent Risk Assessor Program (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.

Cost

There are charges associated with DataLab. The ABS currently uses a partial cost recovery model to assist with maintaining service levels and implementing necessary system, administration and infrastructure updates. The ABS does not seek to make a profit from DataLab or any other integration service.

For more information, see: Charges | Australian Bureau of Statistics.

The data integration service is fully cost-recovered Data integration service | Australian Bureau of Statistics.

Why cost recovery?

Section 12 (3) of the Census and Statistics Act authorises the Statistician to charge fees for certain outputs. Specifically, it states:
"The Statistician may make charges for results and abstracts published and disseminated under this section."

In accordance with the Australian Government Charging Framework (AGCF), the ABS can apply commercial charges to the provision of data services. These charges may be authorised by the Australian Statistician as the accountable authority under the *Public Governance, Performance and Accountability Act 2013* (PGPA Act).

To continue to enable expanded access for government, academics and public policy researchers it is essential that the Data Integration program cost recover. Cost recover supports users to access data in the DataLab, enhanced infrastructure to deliver improved and sustainable access, and streamlining processes to reduce administrative overhead while delivering appropriate governance to uphold ABS's legislative responsibilities and ensure trust in the ABS is maintained.

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 LoE, 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.

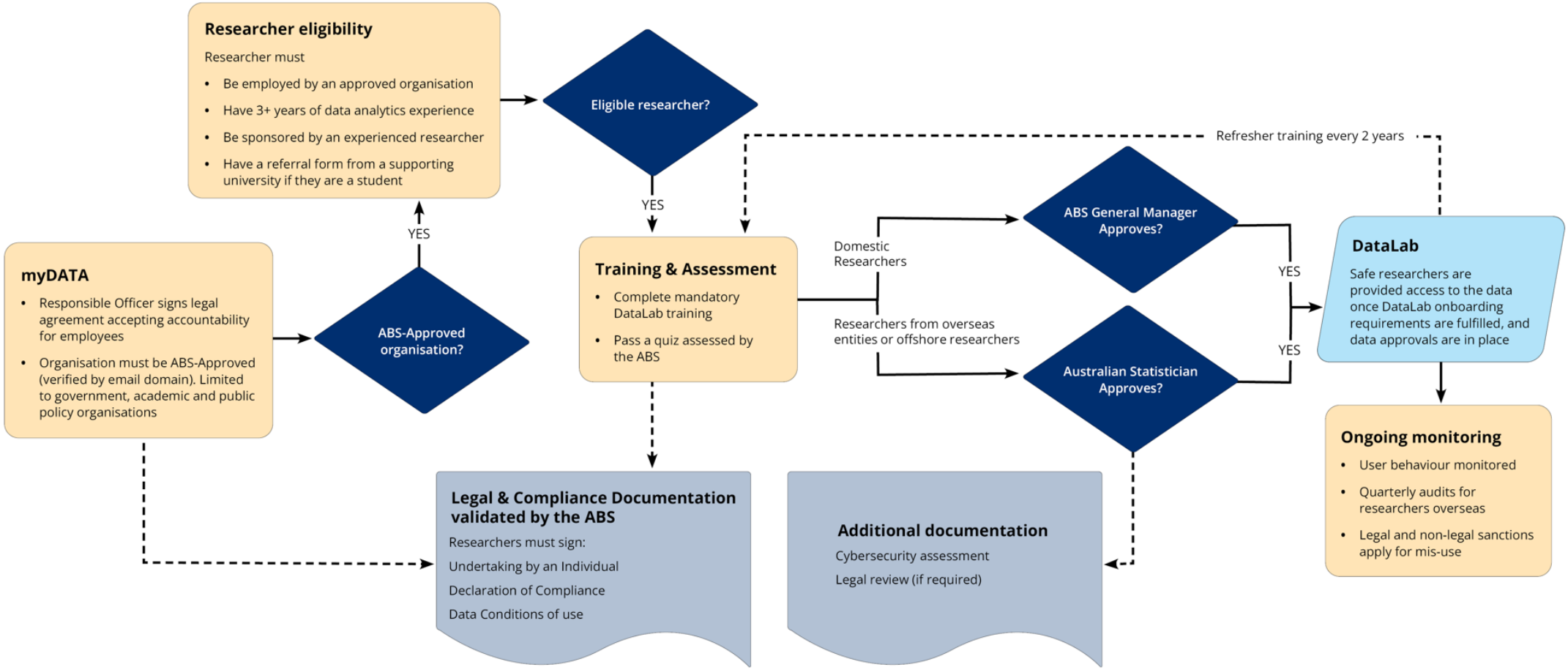
The DataLab User Guide outlines the requirements users must meet before access is granted. Authorised users requesting access to the linked data must:

- 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 researcher onboarding process.

Researcher onboarding process (as part of the ABS Data Integration process flow)

Individual researchers and their organisations sign legally binding undertakings and complete DataLab training



Offshore or overseas researcher access

The 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 LoE, the data custodian must indicate if international access to their data is allowable under their legislation. More information can be found here: Access outside of Australia.

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.

Data custodians will always be given the opportunity to approve or deny projects from overseas entities, or those partnering with an overseas entity, and can request that no overseas entity has access to their data.

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).

Sensitive data or topics

If a project requests access to sensitive data, such as health information or information about Aboriginal and Torres Strait Islander people then the project must go through additional steps.

The Five Safes form the safeguard for data at the project and researcher level. Data custodians support Safe Project controls. At this level, access to any data that is deemed sensitive can be denied by custodians.

If a project with approved access to sensitive data or topics wanted to add an overseas researcher, or a domestic researcher wanted to travel overseas, and the data was restricted to domestic research only, the access would either be approved with the restricted data removed or not approved.

Project approval process

Standard approval process

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 detailed steps, refer to ‘Access approvalssection above. Additional criteria are outlined in Who can access the DataLab. Further guidance is available in: What is DataLab, Using DataLab responsibly.

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, the 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, custodians are notified of each approval. This approach can reduce the data custodian's assessment workload by up to 90%, depending on how the threshold model is implemented.

Adopting the threshold model for assessment is agreed upon between the ABS and data custodians and documented in the LoE instrument.

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 review takes place ahead of data custodian approval activities, so that any additional considerations or protections can be incorporated into the final proposal.

The cultural review process involves referring the project proposal to the 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 Indigenous communities
- 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 Human Research Ethics Committee (HREC) should also be discussed.

The ABS is actively engaged with the Framework for Governance of Indigenous Data (GID), 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 their priorities and aspirations are reflected.

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

Human Research Ethics Committee approvals

Ethics approval requirements are currently part of PLIDA processes, with Data Custodians being able to stipulate ethical approval requirements and ABS tracking whether an approved project has the necessary ethics approval.

The PLIDA Board has endorsed principles as part of the PLIDA Strategy to guide its strategic advice on the operation of the PLIDA operating model. This includes the principle of **'Responsible use of data'** which states:

Build and maintain trust of the Australian community in government data use by:

- Being transparent about the data in PLIDA, its use and handling
- Ensuring security and safety of data
- Promoting ethical use of data about people in Australia, especially vulnerable groups
- Adhering to legislation, regulations and standards.

To support this principle, ethics approval plays a key role in ensuring that data integration projects involving personal information are conducted with appropriate ethical oversight.

Ethics approval is an important part of the PLIDA governance process. Data custodians may require that a project obtain approval from a Human Research Ethics Committee (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
- 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 LoE. 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.

Government-led projects

The ABS does not currently mandate HREC approval for all government-led projects, including those led by state and territory agencies. However, these projects are still subject to the full suite of PLIDA governance requirements, including:

- Assessment under the Five Safes framework (safe people, projects, settings, data, and outputs)
- Alignment with the PLIDA Board's principles, including responsible use of data and transparency
- Compliance with relevant legislation, data sharing agreements, and custodian-specific conditions.

In addition, Australian Government staff are guided by the APS Values, as set out in Section 10 of the *Public Service Act 1999* and the Australian Public Service Commissioner's Directions 2022, which include expectations around ethical conduct, integrity, and stewardship.

Together, these measures ensure that government-led projects are held to high standards of ethical and responsible data use, even where HREC approval is not explicitly required.

PLIDA Ethics Framework for sensitive data

The ABS is progressing work to strengthen and formalise its data ethics approach, including specific enhancements for PLIDA. This work responds to recommendations from external PIAs and aligns with the APS Data Ethics Principles to ensure projects serve the public interest, minimise harm, and maintain transparency and accountability.

The PLIDA Board and ABS have agreed to implement a PLIDA Ethics Framework to strengthen ethical oversight of projects involving health data.

The Framework will build on existing PLIDA governance arrangements and provide a consistent process for identifying when further ethics review is required, and when existing safeguards may be sufficient.

This work aims to ensure consistent, transparent, and proportionate ethics practices across PLIDA projects. The Framework will be made available on the ABS website once finalised.

For PLIDA projects, the ABS can introduce an ethics threshold assessment during project initiation to identify potential ethical risks and determine whether further review (such as a HREC approval) is required. This assessment can be provided to Data Custodians at the project approval stage to support their evaluation and ensure ethical risks are adequately addressed.

Ethical oversight can be embedded through:

- Risk-based ethics assessments for all PLIDA projects
- Referral to HRECs where required by custodians or identified through assessment
- Transparent documentation of ethical considerations shared with custodians.

In addition, the ABS applies a privacy-by-design approach to PLIDA, supported by strong governance and a layered assessment framework. This includes multiple major independent PIAs over time to address evolving risks, as well as project-specific PIAs for new linkages. Independent reviews, detailed PIAs for medium–high risk projects, and PTAs for all new linkages ensure privacy risks are identified and managed proactively.

PLIDA is governed by the Census and Statistics Act, which imposes strict secrecy provisions (Section 19) and controlled release conditions (Section 13). These provisions allow data use only for approved statistical and research purposes in the public interest. There is no authority for commercial exploitation. All ethics assessments will include a compliance check to ensure projects do not involve commercial intent. PLIDA access conditions and ABS governance process will reinforce this restriction.

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 view the projects they have approved by logging into their **myDATA** account.

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 LoE, 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. The ABS manages statistical disclosure for data outputs to minimise re-identification risk. This is an activity conducted by ABS staff under the Census and Statistics Act.

Output refers to all information a DataLab researcher requests to be egressed out of the secure settings and into their non-DataLab space. This covers statistics, other analytical output, code and notes. Enabled by the *Census and Statistics (Information Release and Access) Determination 2018* the ABS manages outputs from the DataLab in a manner that is not likely to enable the identification of a particular person or organisation.

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 ((comprising SES and EL2 experts from across technical, security, policy and statistical areas), led by the ABS Chief Methodologist, making assessments against the Five Safes framework, considering the risk of re-identification and recommending steps to minimise disclosure risk.

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.

If the ABS have cleared outputs from the DataLab it means they have passed statistical disclosure checks and are cleared to be released. These outputs are not reviewed by custodians prior to release.

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.

For more information, see: DataLab Clearance | Australian Bureau of Statistics.

Research output publication review process

Any publication, report and presentation that references integrated data needs to be provided to the ABS a minimum of two weeks prior to wider release. This process does not seek approval from data custodians, rather, it is in place to give custodians visibility of project outputs, provide comments and brief Ministers as required. Analysts will receive any comments or feedback provided by custodians on their publications.

The two-week clearance notification applies once analysis is ready for publication.

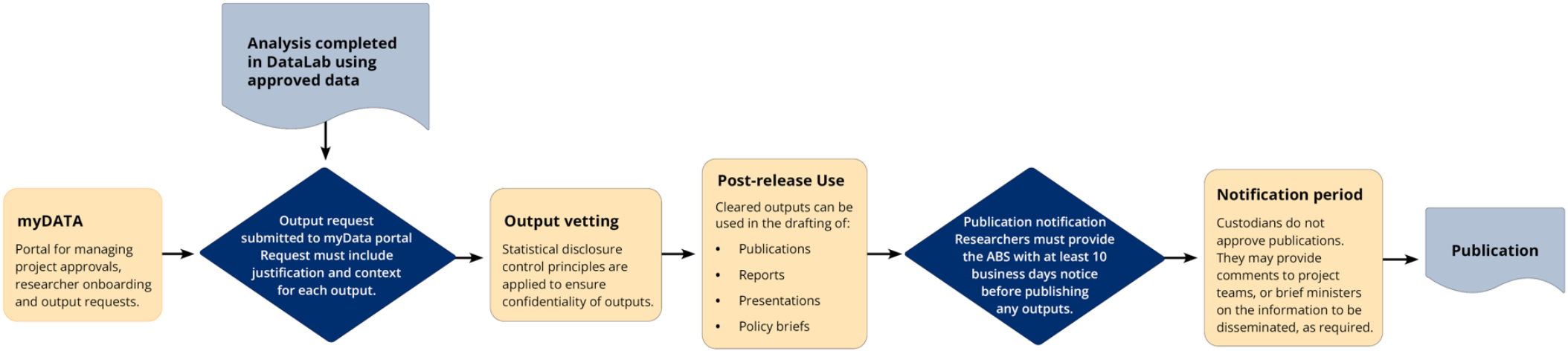
As part of the Project Proposal in myDATA, the following condition must be read and acknowledged by every Project Lead before a new project is accepted:

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

Project Leads must write their full name to acknowledge understanding of 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 arising from this project, including presentations at academic conferences.

Output vetting and publication process for ABS 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)* (Archives Act) 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 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.

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. This legislation provides a strong legal framework for confidentiality and responsible data use. Under the Act:

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

The ABS collects data for PLIDA from a range of different data custodians. Legislative authority for sharing may come from the data custodians:

- Establishing legislation
- Legislation relating to the original collection of the data
- Specific data sharing legislation
- Other legislation.

Accredited Data Service Provider documentation

Data Integration - ABS Integrating Authority information | Australian Bureau of Statistics

The ABS has been an Accredited Integrating Authority since April 2012. The ABS serves as the Integrating Authority for PLIDA and is responsible for the day-to-day operational activities and investments associated with PLIDA. 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 become 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.

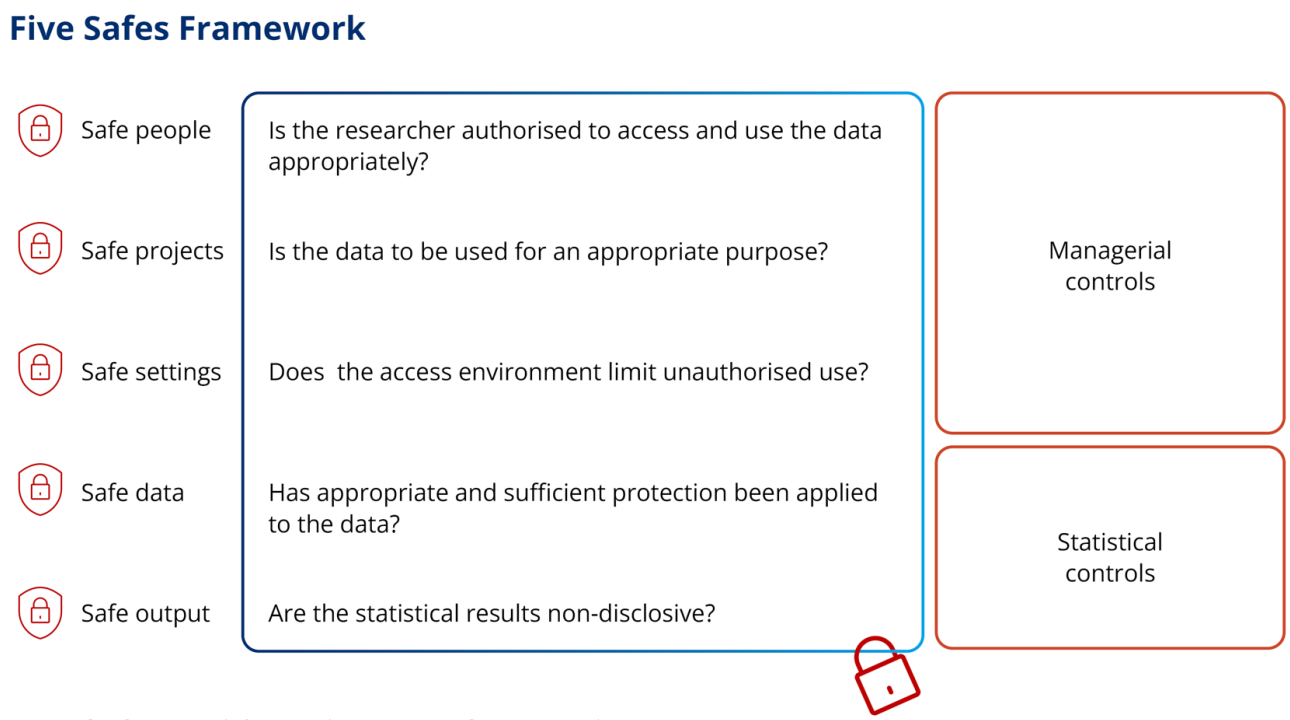
How data in PLIDA is kept safe

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. 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, see Keeping integrated data safe and Privacy at the ABS.

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

- **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 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.



Five Safes framework | Australian Bureau of Statistics (abs.gov.au)

Safe data handling practices - the ABS has adopted the Five Safes framework to enable secure access to data for authorised users only, and to manage disclosure risks. These include:

1. **Safe people** – researchers must undergo training and be approved by all data custodians. This safe has particular emphasis on creating strong controls to enable a shared accountability model for access. The successful and safe access to data relies upon researchers understanding their responsibilities and obligations when accessing the ABS DataLab
2. **Safe projects** – to ensure the use of data is appropriate, 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.

Re-identification risks are considered minimal under the Five Safes framework. The framework takes a multi-dimensional approach to managing disclosure risk. Each safe refers to an independent but related aspect of disclosure risk.

The framework poses specific questions to help assess and describe each risk aspect (or safe) in a qualitative way. This allows data custodians to place appropriate controls, not just on the data itself, but on the manner in which data is accessed. The framework is designed to facilitate safe data release and prevent over-regulation.

Examples of the controls ABS has for each of the safes:

Safe people

- Organisations must have their Responsible Officer sign a legal document that accepts and makes them legally accountable for its employees
- Researchers must undertake mandatory training, including refresher training, covering confidentiality and the conditions of safe system and data use
    - Part of this training reinforces:
        - the need to treat all data in the DataLab as potentially disclosive
        - to only discuss unvetted data with approved project team members in a controlled environment (i.e. where the discussion cannot be overheard and without copying any information seen onto paper or into a messaging system or email)
        - to be transparent with the ABS around any mistakes made with following conditions of use and participating fully in any investigation. Even where the mistake has been made by the ABS (e.g. vetted outputs sent to the researcher include data that should not have been cleared for release), if the researchers ignore this or fail to follow any directions of the ABS to manage any further disclosure risks (e.g. destroying emails with outputs sent incorrectly) then they may be found to be in breach of DataLab rules and procedures
- Completion of a post training assessment that meets an acceptable standard as assessed by the ABS before access is granted
- Demonstration of three years' worth of experience in data analytics, or referral/sponsorship by an experienced researcher
- Provision of signed legal undertakings to comply with DataLab terms and conditions. Researchers are legally bound to sanctions that can be applied if the researcher is found to have acted contrary to the terms and conditions. Sanctions include those that can be legally imposed under the Census and Statistics Act 1905 (e.g. jail time and/or fines) and non-legal sanctions (e.g. DataLab bans for both the researcher and/or their organisation)
- Sanctions (legal and non-legal) apply if a user misuses the DataLab.

Safe projects:

- Review the proposal to ensure the project is statistical in nature, and not for a compliance or regulatory purpose
- Engage with subject areas and project team to ensure requested data is suitable for the research purpose
- Determine whether the project proposal requires additional rigor (e.g. Ethics committee approval or a privacy impact assessment)
- Conduct a technical assessment on all projects
- Seek approval from relevant data custodians.

Safe settings

- DataLab is a secure and closed system utilising Microsoft Windows Virtual Desktop that has no internet access
- Multi-Factor Authentication for access, rated to handle ‘Protected’ data, subject to Privacy and IRAP assessments, and strict security posture

- Approved researchers' accounts are only provisioned post training, relevant undertakings signed and only to approved datasets
- No direct researcher data sharing between projects, users select one active project at a time
- Screen sharing and taking screen shots strictly governed
- The system is regularly reviewed to align with current security protocols
- System based auditing is conducted on a regular basis
- Additional user monitoring and auditing via DTEX platform including session recording and file access logging. All sessions within the ABS DataLab are recorded for auditing purposes and can be checked to ensure researcher compliance with the requirements around appropriate use are being met at any time. All researchers are aware of this system control
- Data Ingress/Egress by ABS Administrators (& Output team) only.

Safe data

- Direct identifiers are removed to comply with general release requirements under the Census & Statistics Determination (s15) which requires that data are not likely to enable the identification of an individual if released via the DataLab.
- Assessed for outliers/remarkable records and sensitive data items
- Supplied at higher level of details if it relates to highly sensitive topics that the respondent has been assured will be afforded greater levels of anonymity (e.g. domestic violence or abuse)
- Treated by the Safe Data Assessment team
- The Disclosure Review Committee (DRC) receives advice on data being released into the DataLab which is assessed against the 5 safes and additionally reviewed if the data has medium-to-high privacy/confidentiality risks after treatment
- Approved by an ABS delegate for loading into the DataLab after receiving DRC endorsement and agreement from data custodians.

Safe outputs

- All DataLab output produced by researchers is reviewed by the ABS DataLab Clearance team
- Unit record information is not permitted
- Project proposals are reviewed to ensure output is with the intention, objectives or method stated therein
- DataLab clearance procedure pinpoints identification/re-identification risks associated with each type of output
- Researchers must follow output rules and apply treatments to ensure outputs are non-disclosive. See DataLab Clearance | Australian Bureau of Statistics
- Extraordinary measures are applied depending on the data, data custodian, and project-level requirements.

Audits

The ABS undertakes a range of regular internal audits to ensure the security and integrity of PLIDA access and systems.

For systems used to prepare PLIDA, the current security audits range from regular user access reviews, to complex assessments such as the Independent Risk Assessor Program (IRAP) and system penetration tests ("pen tests"). These tests examine compliance with the Information Security Manual (ISM) which forms part of the Australian Government's Protective Security Policy Framework (PSPF).

Internal audits by ABS administration teams to verify appropriate user access are conducted approximately quarterly on PLIDA systems. IRAP assessments and pen tests typically occur biennially. An IRAP will always be conducted by an independent assessor, and pen tests are usually completed by an external security expert.

Information revealed in the audits are subject to strict security restrictions. Redacted versions of reports can be made available on request. In addition, the ABS Chief Information Officer will continue to be available to brief data custodians on audit outcomes. Any medium or high severity data incident as defined in the ABS Data Breach and Incident Response Plan would typically trigger an immediate, non-scheduled access audit.

Where States and Territories request a user access audit, it is likely to be accepted whenever reasonably justified and budgeted. Jurisdictions requesting a non-scheduled or irregular IRAP or pen test are expected to fund this activity.

For data linkage, librarian and assembly work, the ABS conducts internal biannual Role Access Management (RAM) audits and access role audits. These audits ensure internal staff access permissions align with actual data access requirements. Regular changes to access are conducted by approved means as part of daily operations; these audits provide an extra layer of assurance to capture any administrative processes that may not have been correctly applied in the preceding six months.

Our data infrastructure, including the ANDII ICT Solution and DataLab, is also audited regularly. All systems and processes meet Australian Government standards for information, personnel and physical security, and comply with the Information Technology security arrangements set out in the ISM and PSPF requirements.

ABS Data Storage Environments

During the term of the LoE, the linkage data (Linkage Data) and analytical data (Family File) will be transferred separately to the ABS using secure file transfer protocols. All 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 undergone multiple security assessments. Each of these environments provide the ABS with additional layers of control and assurance, reducing residual risks and safeguarding the privacy and confidentiality of all data supplied to the ABS.

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 manages these risks through 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, 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 align with ABS processes
- Review any relevant DSAs, MoUs or LoEs for notification obligations
- Be prepared to engage in joint incident response and public communication if required.

ABS System and Security Measures

The ABS's data integration systems and processes are designed to meet the highest security standards. They:

- 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 (ASD)
- Comply with the Australian Government Protective Security Policy Framework (PSPF).

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

- All IT systems will conform with the technical security requirements defined by the ISM
- Strict physical security controls will cover access to ABS premises, consistent with 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 Census and Statistics Act
    - Obtaining a baseline security clearance prior to access being granted to the ABS's secure data integration processing environments.
- Maintaining a secured internet gateway, reviewed annually by the Australian Signals Directorate
- Conducting regular protective security risk reviews to ensure security arrangements remain effective
- Ongoing security audit and review programs covering both IT systems and physical environments.

www.abs.gov.au