



Australian Government  
Department of Employment  
and Workplace Relations

# Aggregated Data Confidentiality Policy

March 2024



With the exception of the Commonwealth Coat of Arms, the Department's logo, any material protected by a trade mark and where otherwise noted all material presented in this document is provided under a [Creative Commons Attribution 4.0 International](https://creativecommons.org/licenses/by/4.0/) (<https://creativecommons.org/licenses/by/4.0/>) licence.

The details of the relevant licence conditions are available on the Creative Commons website (accessible using the links provided) as is the full legal code for the [CC BY 4.0 International](https://creativecommons.org/licenses/by/4.0/legalcode) (<https://creativecommons.org/licenses/by/4.0/legalcode>)

The document must be attributed as the Aggregated Data Confidentiality Policy.

## Contents

<b>Introduction.....</b>	<b>4</b>
<b>Policy.....</b>	<b>4</b>
Purpose.....	4
Scope .....	5
Policy statement.....	5
Release of data on deceased persons .....	5
<b>Responsibilities .....</b>	<b>6</b>
Related documents .....	6
<b>Procedure .....</b>	<b>6</b>
<b>Compliance with this policy .....</b>	<b>7</b>
<b>More information.....</b>	<b>7</b>

## Introduction

The Department of Employment and Workplace Relations (the Department) collects and produces data from its interactions with the Australian public (including individuals, businesses, staff and contractors), including personal information.

The Department has a legal obligation to keep personal information protected. The risks of unauthorised disclosure of personal information can be minimised by confidentialising aggregated data prior to external release.

## Policy

### Purpose

The purpose of this policy is to articulate the requirements for confidentialising aggregated (and de-identified) data derived from data held by the Department, relating to individuals, prior to external release, including to other government agencies, Minister's offices, and Senate Estimates.

#### **Notes:**

*Confidentiality* relates to protecting the secrecy and privacy of information collected from individuals and organisations and ensuring that no data is released in a manner likely to enable their identification.<sup>1</sup>

*External release* includes publication of data on a public website, provision of aggregated data to an external entity, the provision of data to the Minister's office(s) and data included in Senate Estimates briefs.

*Aggregate data* refers to high-level data which is acquired by combining transactional / unit record data.

Prior to the external release of data relating to individuals, the Privacy Principles require two steps for de-identification:

1. the removal of direct identifiers and
2. the removal or alteration of other information that could potentially be used to re-identify (or spontaneously recognise) an individual.

Currently, this policy ONLY relates to data involving individuals. The policy will be updated to include business data in the future.

The internal sharing of data is out of scope for the Aggregated Data Confidentiality Policy.

---

<sup>1</sup> [Glossary | Australian Bureau of Statistics \(abs.gov.au\)](#)

The sharing of highly disaggregated / transactional / unit record data is out of scope for the Aggregated Data Confidentiality Policy – see the Data Sharing Policies. This includes the sharing of highly disaggregated / transactional / unit record data with other government agencies.

## Scope

This policy covers the external release of aggregated data derived from data held by the Department and ties directly into the Department's Data Strategy, specifically the theme of data sharing and release.

The release of aggregated statistics on deceased persons is covered by this policy, see [Release of data on deceased persons](#) for more information.

## Policy statement

The Department uses a Frequency Rule of 5 (also known as a Threshold Rule) to confidentialise aggregated data, protecting the privacy of individuals. The Frequency Rule of 5 means that when the number of contributors to a cell is less than 5 (or 1, 2, 3 or 4), the cell is considered a disclosure risk and needs to be treated for confidentiality. This rule also applies to information that is derivable from externally released data which has not necessarily been published / included in the externally released table.

For example, if publishing data by age group, the data may have three age group categories: 18–20-year-olds, 21–25-year-olds and 26–30-year-olds. If the published table includes the actual total of the 18–30-year-olds but excludes the 18–20-year-old age group – this field is derivable and may break the frequency rule of 5. Please see Data Confidentiality Procedures for further information.

Some data may be more sensitive and require a higher threshold regarding the minimum contributors, minimising the risk of spontaneous recognition.

There are five endorsed confidentiality techniques:

1. Category aggregation
2. Cell suppression
3. Convention rounding
4. 50/50 rounding
5. Perturbation

See the Data Confidentiality Procedures for more detail on how to implement these confidentiality techniques.

## Release of data on deceased persons

Data about deceased persons is not subject to the Privacy Act, including the Australian Privacy Principles. However, data about deceased persons may still be subject to legislative secrecy provisions. For example, data related to deceased persons may still be protected information for the purposes of the social security law if it can be connected to those persons, even if de-identified.

In some circumstances, there are legislative requirements for the department to publish statistics on fatalities or deceased persons, such as statistics published by the Federal Safety Commissioner. In these situations, this policy does NOT apply.

## Responsibilities

Role	Description
All staff	<p>Have a legal obligation to keep personal information protected, minimising spontaneous recognition, by applying this policy and the related procedures. Personal information is any information related to an identifiable individual and includes (but is not limited to) names, address, dates of birth, indigenous status etc.</p> <p>Have a responsibility to escalate possible or actual breaches of this policy to their Assistant Secretary/Data Steward.</p>
Data Governance Committee	<p>The Data Governance Committee will consider adherence to this policy and associated guidelines, including any recommendations on modifications to this policy and the associated procedures from Committee members/Data Stewards.</p>
Data Steward	<p>Responsible for the business management and use of data including:</p> <ul style="list-style-type: none"><li>• the consideration and application of this policy, and associated procedures and</li><li>• authorising the aggregated data release.</li></ul>

## Related documents

- [Data Strategy](#)
- [Data Glossary](#)
- [Data Governance Framework](#)
- [Data Sharing and Release Policy](#)
- OAIC & CSIRO: [De-identification Decision Making Framework](#)
- OAIC: [De-identification and the Privacy Act](#)

## Procedures

- [Aggregated Data Confidentiality Procedures](#)
- [Data Publication Procedures](#)
- [Excel publication template](#)

- [Data Request Template](#)
- [Data Sharing Procedures](#)
- [Data Sharing Agreement Template](#)
- [Letter of Exchange Template](#)

## Compliance with this policy

Data Stewards will report to the Chief Data Officer on adherence to this policy and associated procedures, including any recommendations on modifications to this policy and the associated procedures.

If an exception to this policy is required for a specific purpose, this exemption will require approval from the DEWR Chief Data Officer.

The Chief Data Officer will report to the Data Governance Committee on adherence and exemptions, on an annual basis or as required.

## More information

For more information, please contact the Data Governance and Policy Section, Chief Data Officer Branch by email at [data@dewr.gov.au](mailto:data@dewr.gov.au).

## Document details

Policy Owner	<i>Chief Data Officer</i>
Document Status	<i>Approved</i>
Point of Contact	<i>Karen McGuigan</i> <i>Chief Data Officer Branch, Digital Services</i> <i>Division</i>
Approver	<i>Jenny Humphrys</i>
Approval Authority	<i>Chief Data Officer</i>
Date of Approval	<i>04/03/2024</i>

## Document Review and Change

Version	Date	Author/s	Summary of Changes	Date of next Scheduled review
<i>1.0</i>	<i>04/03/2024</i>	<i>Data Governance Section</i>	<i>New policy</i>	<i>04/03/2026</i>
<i>1.1</i>	<i>20/02/2025</i>	<i>Data Governance Section</i>	<i>Added section on deceased persons</i>	<i>04/03/2026</i>