Australian Government

Consumer Data Right

De-identification of CDR data under the Consumer Data Right guidance

January 2024

Version Control		
October 2022	Version 1	First version of guidance
May 2023	Version 2	Removal of references to the Telecommunications sector
January 2024	Version 3	Updates to reflect amendments made in version 5 of the CDR Rules.

Table of Contents

1. Purpose of this document

This document outlines the obligations of accredited data recipients (ADRs) in relation to the treatment of de-identified and redundant data under the *Competition and Consumer (Consumer Data Right) Rules 2020* (the rules) and the *Competition and Consumer Act 2010* (the Act). Participants should read this guidance in conjunction with the rules and Act.

> **NOTE:** This document provides general guidance only. It does not constitute legal or other professional advice and should not be relied on as a statement of the law. As this is only a guide, it may contain generalisations. We encourage participants to obtain independent advice to ensure they understand their obligations under the CDR framework.

2. OAIC guidance

The Office of the Australian Information Commissioner (OAIC) has a role in providing guidance in relation to the privacy safeguards and protection of CDR data (s 56EQ(1)(a)). Chapters B, C, 6 and 12 of the OAIC's CDR Privacy Safeguard Guidelines deal with the de-identification of CDR data and references to the OAIC's guidance are included throughout this document.

3. CDR data and de-identified CDR Data

CDR data is information that is specified in a designation instrument or any data wholly or partly derived from that information.

CDR data may be considered de-identified if no person would be identifiable or reasonably identifiable from the data and any other information that would be held by any person following the de-identification process. If a person can be identified from data, for example, the identity of a person or organisation can be determined even though directly identifying information has been removed, the data would not be considered de-identified for the purposes of the CDR. This may be the case where a person is identified from data using other publicly or privately held information about the person.

4. When can a CDR consumer's CDR data be de-identified?

An ADR may de-identify a CDR consumer's CDR data if:

- the CDR consumer gives a 'de-identification consent', which allows the ADR to de-identify some or all of the CDR data for general research and/or to disclose to others (including by sale)
- the CDR consumer does not elect that their redundant data must be deleted, and at the time of seeking consent the ADR informed the CDR consumer of its general policy of:
    - de-identifying redundant data, or
    - deciding whether to delete or de-identify redundant data, and the ADR considers it appropriate in the circumstances to de-identify rather than delete the redundant data.

These circumstances are discussed further below.

5. CDR data de-identification process

The CDR data de-identification process is set out in rule 1.17. The ADR must consider whether it would be possible to de-identify the relevant data to the extent (the **required extent**) that no person would be identifiable, or reasonably identifiable, from the data and any other information that would be held by any person following the de-identification process.[1] In considering this the ADR must have regard to:

- the De-Identification Decision Making Framework
- the techniques that are available to de-identify data
- the extent to which it would be technically possible for any person to be identifiable or reasonably identifiable, after de-identification
- the likelihood of any person becoming identifiable, or reasonably identifiable from the data after de-identification.

If it is possible to de-identify the relevant data to the required extent, the ADR must:

- determine and apply the appropriate technique to de-identify the data
- delete (in accordance with the CDR data deletion process)[2] any CDR data that must be deleted to ensure that no person is identifiable or reasonably identifiable from the de-identified data and any other information that would be held by any person following the de-identification process
- as soon as practicable, make a record to evidence:
    - its assessment that it is possible to de-identify the relevant data to the required extent
    - that the data was de-identified to that extent
    - how the data was de-identified, including records of the technique used
    - who the de-identified data is disclosed to.

The requirement to keep records of who the de-identified data is disclosed to is not a time-limited obligation – a record must be made every time the de-identified data is disclosed.[3]

If it is not possible to de-identify data to the required extent, then the ADR must apply the CDR data deletion process.[4]

Further information on the de-identification process can be found in the OAIC's CDR Privacy Safeguard Guidelines:

- Chapter 6: Privacy Safeguard 6 — Use or disclosure in accordance with de-identification consent
- Chapter 12: Privacy Safeguard 12 — Deciding how to deal with redundant data; Step 5: de-identifying redundant data
- Chapter 12: Privacy Safeguard 12 — 'Steps to de-identify redundant data'

[1] For example, the ADR must consider whether data that has been de-identified could be re-identified using data or information that may be held by another party.

[2] CDR Rules, rule 1.18.

[3] Explanatory statement to principal rules: Competition and Consumer (Consumer Data Right) Rules 2020, paragraph 58.

[4] CDR Rules, rule 1.17(4) and rule 1.18.

6. Using or disclosing de-identified data in accordance with a de-identification consent

A CDR consumer may consent to an ADR de-identifying CDR data that it has collected and using the de-identified data for general research and/or disclosing (including by selling) the de-identified data. This is called a de-identification consent.[5]

If an ADR seeks a de-identification consent from a CDR consumer, the ADR must (in addition to the ordinary requirements for seeking consent) give the consumer information about:[6]

- the CDR de-identification process
- whether the ADR will disclose the de-identified data, who it would disclose it to and why
- if the ADR will use the de-identified data for general research, that fact and a link to a description in the ADR's CDR policy[7] of the research and any additional benefits to the consumer of consenting[8]
- the CDR consumer's inability to elect to have de-identified data deleted in accordance with rule 4.16 once it becomes redundant data.

Further information on de-identification consents can be found in the following chapters of the OAIC's CDR Privacy Safeguard Guidelines:

- Chapter B: Key concept: de-identification consent
- Chapter C: Consent — De-identification consents
- Chapter 6 - 'Using or disclosing de-identified CDR data in accordance with a de-identification consent'.

7. De-identification or deletion of redundant data

Section 56EO(2) (Privacy Safeguard 12) of the *Competition and Consumer Act 2010* defines 'redundant data' as data the CDR entity no longer needs for a purpose permitted under the rules or Part IVD Division 5 of the Act (which outlines the Privacy Safeguards).

When an accredited person asks a CDR consumer to give a consent, it must provide a statement regarding its intended treatment of redundant data, including whether it has a general policy of deleting or de-identifying redundant data.[9]

If the accredited person states it has a general policy of deleting redundant data, it must delete the CDR consumer's CDR data once it becomes redundant.

[5] CDR Rules, rule 1.10A(1)(e).

[6] CDR Rules, rule 4.11(3)(e) and rule 4.15.

[7] The OAIC has published a Guide to developing a CDR policy to help ADRs prepare and maintain a CDR policy.

[8] The ACCC's September 2020 consultation paper in relation to the version 3 rules states: "The benefit to the consumer could be, for example, the ADR paying a fee to the CDR consumer or providing a discount on services provided to the CDR consumer".

[9] CDR Rules, rule 4.17(1).

If the accredited person has a general policy that it will or may de-identify redundant data, it must state the following when seeking consent:

- it will apply the CDR data de-identification process (and what this means)
- it would be able to use or disclose the de-identified redundant data without seeking further consent
- if applicable, examples of how it could use the de-identified redundant data.[10]

The accredited person must also outline the CDR consumer's right to elect that their redundant data be deleted, and instructions for how the election can be made.[11] This is because under rule 4.16 a CDR consumer may choose to have their collected data and any data derived from it deleted when it becomes redundant data, notwithstanding any general policy the accredited person may have to de-identify redundant data.

If the CDR consumer does not elect that their redundant data be deleted, the ADR may de-identify the data in accordance with the CDR data de-identification process.[12] In these circumstances, the ADR must also direct any of its direct outsourced service providers (OSP) or CDR representatives that possess a copy of the redundant data to delete it, as well as any data directly or indirectly derived from it and notify the ADR of the deletion.[13] If the direct OSP or CDR representative has provided the redundant data to its own direct OSP (the further recipient), the ADR must also direct its direct OSP or CDR representative to direct the further recipient to both delete the redundant data (as well as any data directly or indirectly derived from it) and notify the ADR of the deletion .[14]

If the CDR consumer elects that their redundant data should be deleted, the redundant data must be deleted in accordance with the CDR data deletion process contained in rule 1.18. This involves:

- deleting the redundant data and any copies
- making a record of the deletion
- where another person, such as an OSP or a CDR representative, holds the redundant data on behalf of the ADR and will perform the above steps, the ADR must direct that person to notify it when the person has carried out those steps.[15]

If the redundant data cannot be de-identified in accordance with the CDR data de-identification process, it must be deleted in accordance with the CDR data deletion process.[16]

Treatment of derived CDR data

An ADR is not required to delete derived CDR data that was de-identified before the collected data from which it was derived became redundant. For example, an ADR may combine data from various data holders to create a spending summary for budgeting purposes. This spending summary would be derived CDR data and with the consumer's consent, it could be de-identified in accordance with the rules before the data sets from which it was derived become redundant. An election under rule 4.16 would not require

[10] CDR Rules, rule 4.17(2).

[11] CDR Rules, rule 4.11(3)(h).

[12] CDR Rules, rule 7.12.

[13] CDR Rules, rule 7.12(2)(b)(i).

[14] CDR Rules, rule 7.12(2)(b)(ii).

[15] CDR Rules, rule 1.18(a)-(b) and 7.13.

[16] CDR Rules, rule 1.17(4) and 7.13.

the deletion of the de-identified spending summary. However, copies of the spending summary or the initial data sets may need to be deleted in accordance with the rules.

More information on the treatment of redundant data can be found in the OAIC's CDR Privacy Safeguard Guidelines, particularly Chapter B - Key concepts - Redundant data, Chapter C - Consent - The basis for collecting, using and disclosing CDR data - Treatment of redundant data and Chapter 12: Privacy Safeguard 12.

8. Retention of redundant data

Rule 1.17A states that an ADR is required to retain CDR data it has identified as redundant if:

- it is required to do so under an Australian law or a court/tribunal order; or
- the redundant data relates to legal proceedings or dispute resolution proceedings that the ADR or CDR consumer is a party to.

In these circumstances the ADR must retain the CDR data while the legal requirement continues to apply. Further information can be found in chapter 12 of the OAIC's CDR Privacy Safeguard Guidelines.