Australian Government

Office of the Australian Information Commissioner

# Guide to developing a CDR Policy

September 2021

OAIC

| Version | Currency dates | Changes and other comments |
|---|---|---|
| 1.0 | 12-Jun-2020 to 22-Sep-2021 | |
| 2.0 | 23-Sep-2021 to… | Updated guidance to reflect amendments to Part IVD of the *Competition and Consumer Act 2010* introduced by the *Treasury Laws Amendment (2020 Measures No. 6) Act 2020*, including changes to reflect that Privacy Safeguard 1 (including the requirement to have a CDR policy) applies to accredited persons who are or who may become an accredited data recipient.<br><br>Updated guidance on what information must be included in an entity's CDR policy to reflect amendments to the CDR Rules introduced by the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, including that information about undertaking general research must be included in a CDR policy.<br><br>Updated guidance on the information a CDR policy must provide about who CDR data may be disclosed to, to reflect amendments to the CDR Rules introduced by the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2020*, that allows an outsourced service provider to collect CDR data.<br><br>New guidance on the interaction between the CDR policy and existing privacy and data protection policies.<br><br>New guidance on having a CDR policy where an entity performs more than one role in the CDR system (for example, where the entity is a data holder and an accredited person).<br><br>Updated privacy tip on ensure the CDR policy is easily read and understood.<br><br>Clarifications to guidance, including:<br>• that an accredited person's CDR policy must include information about the CDR data that another entity holds or may hold on the accredited person's behalf (for example, an outsourced service provider)<br>• information about the de-identification CDR data in a CDR policy. |

# Contents

This Guide aims to help data holders, designated gateways, accredited persons and those preparing for accreditation under the Consumer Data Right system (CDR) to prepare and maintain a CDR policy.

It sets out a suggested process for developing a CDR policy and outlines the minimum requirements for what must be included.

There is also a checklist to help you consider all your obligations under the *Competition and Consumer Act 2010* (Competition and Consumer Act)[1] and the *Competition and Consumer (Consumer Data Right) Rules 2020* (CDR Rules).

You should read this CDR policy guide together with the full text of Division 5 of Part IVD of the Competition and Consumer Act, the CDR Rules and the CDR Privacy Safeguard Guidelines.[2]

# Introduction

All CDR entities must have and maintain a clearly expressed and up-to-date CDR policy.[3] A CDR policy must be a separate document to the general privacy policy.[4]

A 'CDR entity' is:

- a data holder of CDR data
- a designated gateway for CDR data, or
- an accredited person who is or who may become an accredited data recipient of CDR data.[5]

This Guide uses 'accredited persons' to refer to accredited persons who are or who may become an accredited data recipient, unless otherwise indicated.

A CDR policy is a document that provides information to consumers about:

- how CDR data is managed,[6] and
- how they can make an inquiry or make a complaint.[7]

It is a key tool for ensuring that CDR participants manage CDR data in an open and transparent way.

[1] The privacy safeguards are set out in Division 5 of Part IVD of the Competition and Consumer Act.

[2] The CDR Privacy Safeguard Guidelines provide guidance on the privacy safeguards and related CDR Rules.

[3] Section 56ED of the Competition and Consumer Act.

[4] CDR Rule 7.2(2).

[5] An accredited person 'may become' an accredited data recipient when they are seeking to collect CDR data. This means that an accredited person must ensure that they have a CDR Policy before they seek to collect CDR data.

[6] Section 56ED(3)(a) of the Competition and Consumer Act.

[7] See sections 56ED(4)(b) (for data holders), 5(d) (for accredited persons) and 6(b) (for designated gateways) of the Competition and Consumer Act.

Privacy Safeguard 1 and CDR Rule 7.2 set out the requirements for what information must be included in a CDR policy, what form it should be in, and how it should be made available.

To help you meet these obligations, this Guide sets out a suggested process for developing a CDR policy and outlines the minimum requirements for what must be included.

There is also a checklist to help you work out if you have considered all your CDR policy obligations.

### How the CDR policy interacts with other existing privacy and data protection policies

It is important to understand how your CDR policy interacts with your obligations under the Australian Privacy Principles (APPs) contained in the *Privacy Act 1988* (Privacy Act), or other obligations (for example those under the European Union General Data Protection Regulation). the Privacy Act requires APP entities to have a clearly expressed and up-to-date APP Privacy Policy about how the entity manages personal information (APP 1.3 and 1.4).

Your CDR policy must be distinct from your APP Privacy Policy, or any other existing privacy policies.[8] This means your CDR policy must be a separate document and must expressly address each of the applicable matters listed in Privacy Safeguard 1 and CDR Rule 7.2. These matters are set out below in the section What information must be included in a CDR policy? For example, it would not be sufficient for a CDR entity to provide a link to its APP Policy to address how a consumer could make an inquiry or make a complaint (even where that APP policy includes identical or substantially similar complaint process information).

However, for CDR data that is also personal information, it may be appropriate for data holders to explain in a CDR policy when and how the APPs apply to that data. For example, a data holder should explain when and how the APP processes apply to access and correction of CDR data (see the Information on access to and correction of CDR data section below). In this situation, you may wish to link to other existing APP policies for further information on the APP process for handling CDR data.

**Note:** In addition to updating the CDR policy with information about the interaction between the CDR and APP requirements, it may be helpful to also update your APP policy so consumers are clear about what processes apply to CDR data and when.

## Steps in developing a CDR policy

This section provides an overview of a suggested six-step process for developing your entity's CDR policy.

These steps are intended to make it easier for you to meet your CDR policy obligations and to ensure that your CDR policy is genuinely informative and useful for consumers.

- Step 1: Understand your obligations and how you handle CDR data
- Step 2: Develop content, structure and presentation
- Step 3: Write your CDR policy

[8] CDR Rule 7.2(2).

- Step 4: Test your CDR policy
- Step 5: Make the policy available
- Step 6: Review and update your policy

### Step 1: Understand your obligations and how you handle or intend to handle CDR data

The first key step in developing a CDR policy is to ensure you have a clear understanding of how you handle (or intend to handle) CDR data, including relevant practices, procedures and systems. This will assist you to accurately and openly describe to your consumers how you will handle CDR data and enable you to deal with inquiries, requests and complaints under the CDR system.

You must include the mandatory requirements set out below under the section What information must be included in a CDR policy?

You must also understand your broader CDR privacy obligations regarding the collection, use and disclosure of CDR data. This will differ based on whether you are a data holder, an accredited person, or a designated gateway.

Where your entity performs more than one role in the CDR system (for example as both a data holder and an accredited person), you may either have a single CDR policy that outlines how you handle CDR data in both capacities, or have separate CDR policies for each capacity.

**Privacy tip**

Having a clear understanding of how you handle CDR data, including relevant practices, procedures and systems will assist you to accurately and openly describe to your consumers how you manage CDR data and deal with queries, requests and complaints under the CDR system.

### Step 2: Develop content, structure and presentation

Although the CDR policy must cover all the topics in Privacy Safeguard 1 and CDR Rule 7.2, the information does not have to be presented in that order. You should aim to make the policy as easy as possible for the consumer to find the information that is most important to them.

Below are some tips to make the content and structure useful and manageable for consumers.

- **Arrange the information in a way that makes sense** so that it is easy to follow and intuitive to the reader. The presentation of the information should make sense and reflect your entity's functions, activities and audience.
- **Focus on key topics** that consumers are likely to be most concerned about, unaware of, won't reasonably expect or may not understand easily.
- **Be as specific as possible** about how your entity manages CDR data, as this will provide clarity and build trust. Unqualified use of vague words (such as 'may') could lead to concern about uses and disclosures that are not intended.

- **Take a layered approach** to providing information about how your entity will handle CDR data, by providing a summary version that focuses on what the consumer should know with a link to the complete CDR policy. This will be particularly effective in the online environment.

**Privacy tip**

While the CDR policy must be a document, you may also wish to consider other innovative formats to best communicate your privacy messaging to consumers, such as the use of infographics, animation or video, or other forms of technology.[9]

### Step 3: Write your CDR policy

Once you have a clear idea of how your entity handles CDR data, what must be included in the CDR policy, and the proposed content and structure for your policy, you can begin drafting.

The CDR policy must be clearly expressed and up-to-date.[10] To ensure the CDR policy is easy to read and understand:

- Use an active voice and simple language — avoid legal jargon, acronyms and terms that may only be understood in-house
- Use short sentences, break up text into paragraphs and group relevant sections together
- Use headings to assist navigation
- Avoid unnecessary length — include only relevant information.

### Step 4: Test your policy

Test your CDR policy on the target audience or audiences, including likely readers. Where your resources are limited and systematic testing is not possible, you could consider providing it to colleagues from other internal business units to give you an idea of how easy it is to read.

**Privacy tip**

The CDR policy should be able to be easily read and understood. You can test this by using external standards, such as the Flesch-Kincaid grade level test. When setting a readability goal, you should consider who your consumers are to ensure your CDR policy suits their level of understanding. Generally, it is good to aim for a secondary school reading level. [11]

### Step 5: Make the policy available

Your CDR policy must be freely and publicly available for consumers. If you are an accredited data recipient or data holder, the policy must be available through the online service that you ordinarily

[9] CDR Rule 7.2(2).

[10] Section 56ED(3) of the Competition and Consumer Act.

[11] For example, a quick online test is available at read-able.com.

use to deal with consumers, such as your website or mobile applications.[12] Additionally, you must provide the CDR policy electronically or in hard copy if requested by the consumer (for example in a word document or pdf).[13]

Appropriate accessibility measures should also be put in place so that the policy may be accessed by all consumers (including consumers with a vision impairment, or those from a non-English speaking background). It is a good idea to provide information about how to request an accessible copy of the CDR policy, in the same locations where consumers can access the policy.

Once you become accredited, a hyperlink to your CDR policy will need to be included on the CDR Register.[14]

**Privacy tip**

The CDR policy should be prominently displayed, accessible and easy to download. For example, a prominent link or icon, displayed on the relevant pages of the website or mobile application, could provide a direct link to the CDR policy.

### Step 6: Review and update your policy

As there is a requirement to ensure the CDR policy is to up-to-date, the CDR policy should be reviewed regularly. This will help to ensure that the information in the policy accurately reflects your current CDR handling practices.[15]

This review should, at a minimum, be undertaken as part of annual planning processes. To assist readers, you could also:

- include the date the policy was last reviewed or updated
- invite comments on the policy to gain feedback and evaluate its effectiveness, and
- explain how any comments will be dealt with.

## What information must be included in a CDR policy?

Depending on whether you are an accredited person, data holder or designated gateway, there are different matters that need to be covered in your CDR policy.

Categories of information that must be included are:

- **Requirements for both data holders and accredited persons**:
  - Information about the consumer complaints process

[12] Section 56ED(7) of the Competition and Consumer Act and CDR Rule 7.2(8).

[13] Section 56ED(8) of the Competition and Consumer Act and CDR Rule 7.2(9).

[14] CDR Rules 5.24 (i)(ii) and 5.25(1)(b)(ii)(B).

[15] Section 56ED(3) of the Competition and Consumer Act.

  - Information about access to and correction of CDR data

- **Specific requirements for data holders:**
  - Acceptance of voluntary consumer or product data requests
- **Specific requirements for accredited persons:**
  - What CDR data is held, and how it is held
  - Purposes CDR data is used for
  - Information about undertaking general research
  - Additional information about who CDR data may be disclosed to
  - Overseas storage practices
  - When consumers will be notified about certain events
  - Consequences of withdrawing consent
  - Deletion of CDR data
  - De-identification of CDR data
- **Specific requirements for designated gateways**:
  - Facilitating disclosure or accuracy of CDR data, and
    - Information about the complaints process

The sections below cover each of these items in more detail. There is also a checklist at Attachment A below to help you work out whether you have considered all of the relevant requirements.

For further information, see Chapter 1 (Open and transparent management of CDR data) of the CDR Privacy Safeguard Guidelines.

## Information about the consumer complaints process — for data holders and accredited persons

Both accredited persons and data holders must have a process to deal with consumer complaints, in the event that a consumer thinks you have not met your CDR related obligations under the Consumer and Competition Act and/or CDR Rules.[16]

The CDR Rules specify that the CDR policy needs to cover:

- where, how and when a complaint can be lodged
- when a consumer should expect an acknowledgment of their complaint
- the information that the consumer needs to provide

[16] Sections 56ED(4)(b) and (5)(d) of the Competition and Consumer Act.

- the process for handling consumer complaints
- the time periods associated with the various stages of the complaints process
- options for redress, and
- options for review (both internally, if available) and externally.[17]

## Information on access to and correction of CDR data — for data holders and accredited persons

### How to access CDR data

Both accredited persons and data holders must include information for consumers about how they may access their CDR data.[18]

A data holder may receive a request from an accredited data recipient on the consumer's behalf, or a consumer may make a request directly to the data holder.[19]

Where the data holder is also an Australian Privacy Principle (APP) entity under the Privacy Act, the data holder should provide information in its CDR policy about how a consumer may access their personal information (that is also CDR data) under APP 12.[20]

For further information about the CDR access requirements, see the Guide to privacy for data holders.

### How to correct CDR data

Both accredited persons and data holders must include information for consumers about how they can correct their CDR data. The CDR policy should make clear that the consumer has a right to request correction of their CDR data.[21] For data holders, a consumer's right to request correction under Privacy Safeguard 13 applies once the data holder has previously been required or authorised to disclose the CDR data.[22] Where a data holder is also an APP entity under the Privacy Act, the data holder should provide additional information in its CDR policy about how a consumer who is an individual may seek correction of their personal information that is also CDR data under APP 13.[23]

---

[17] CDR Rule 7.2(6).

[18] Section 56ED(5)(c) of the Competition and Consumer Act.

[19] For the banking sector, a data holder's obligations under Part 3 of the CDR Rules (regarding consumer data requests made by consumers) do not commence until 1 November 2021: clause 6.6 of Schedule 3 to the CDR Rules.

[20] Note: APP entities only have APP 12 obligations in relation to consumers who are individuals (not businesses).

[21] Section 56ED(4)(a) and 56ED (5)(c) of the Competition and Consumer Act.

[22] Section 56EP(1)(c) of the Competition and Consumer Act.

[23] Where a data holder has not previously been required or authorised to disclose a consumer's CDR data, a consumer is unable to make a correction request under Privacy Safeguard 13. However, where the data holder is an APP entity, the consumer will be able to make a correction request under APP 13. This is because APP 13 will continue to apply to CDR data that is personal information in all other circumstances. For further information, see Chapter 13 (Correction of CDR data) of the CDR Privacy Safeguard Guidelines.

For information about the correction requirements, see Chapter 13 (Correction of CDR data) of the CDR Privacy Safeguard Guidelines and the Guide to privacy for data holders.

**Privacy tip**

Any preferred procedures for consumers to make access or correction requests should be outlined in the CDR policy. For example, the CDR policy could provide a link to a form, and/or provide the contact details for consumers to make correction requests. However, consumers cannot be required to follow that procedure and entities must respond to correction requests from consumers, regardless of the way in which the request is made.

### Specific requirements for data holders — acceptance of voluntary consumer or product data requests

In addition to the requirements set out above, a data holder's CDR policy must:

- make clear whether the entity accepts voluntary consumer or product data requests,[24] and
- state whether the data holder charges fees for such requests (and if so, how information about those fees can be obtained).[25]

### Specific requirements for accredited persons

In addition to the requirements set out above, an accredited person's CDR policy must include information about:

- what CDR data is held, and how it is held
- purposes CDR data is used for
- undertaking general research
- who CDR data may be disclosed to
- overseas storage practices
- when consumers will be notified about certain events
- consequences of withdrawing consent
- deletion of CDR data, and
- de-identification of CDR data.[26]

[24] CDR Rule 7.2(3)(a). Voluntary product data means CDR data for which there are no consumers that is not required product data (clause 1 of Schedule 3 to the CDR Rules). Voluntary Consumer data means CDR data for which there are consumers that is not required consumer data (clause 3.2 of Schedule 3 to the CDR Rules).

[25] CDR Rule 7.2(3)(b).

[26] See s 56ED (5) of the Competition and Consumer Act and CDR Rule 7.2(4)

More detail on these requirements is set out below.

### What CDR data is held, and how it is held

An accredited person's CDR policy must refer to the different classes of CDR data that it holds or may hold. This includes CDR data that another entity holds or may hold on the accredited person's behalf (for example, by an outsourced service provider).[27] The classes of CDR data for each sector will be set out in the relevant designation instrument. For example, for the banking sector the designation instrument sets out three classes of information: customer information, product use information and information about the product.[28]

The CDR policy must also set out how the CDR data is held. This means providing general information about how data is stored.[29]

### Purposes CDR data is used for

An accredited person must indicate the purposes for which they collect, hold, use or disclose CDR data with the consumer's consent.[30]

### Undertaking general research

If an accredited data recipient wishes to undertake general research[31] using de-identified CDR data, their CDR Policy must include:

- a description of the research to be conducted, and
- a description of any additional benefit to be provided to the consumer for consenting to the use.

### Who CDR data may be disclosed to

An accredited person must include further specific information about their disclosures of CDR data to outsourced service providers, non-accredited entities and entities located overseas, as set out below.[32]

---

[27] Section 56ED(5)(a) of the Competition and Consumer Act. An OSP may collect CDR data on an accredited person's behalf. For further information, see CDR Rule 1.10, and Chapter 3 (Seeking to collect CDR data from CDR participants) of the CDR Privacy Safeguard Guidelines.

[28] See sections 6-8 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.

[29] Section 4(1) of the Competition and Consumer Act provides that a person 'holds' information if they have possession or control of a record within the meaning of the Privacy Act. If a person has a right or power to deal with particular data, the person has effective control of the data and therefore 'holds' the data. See Chapter B (Key Concepts) of the CDR Privacy Safeguard Guidelines for further information about the meaning of 'holds'.

[30] Section 56ED(5)(b) of the Competition and Consumer Act.

[31] CDR Rule 7.2(4)(ca). General research relates to research an accredited data recipient wishes to undertake using de-identified CDR data, that does not relate to the provision of goods or services to any particular CDR consumer. CDR Rule 7.5(1)(aa) permits the use of CDR data for general research, where it has been de-identified in accordance with the CDR data de-identification processes.

[32]Note that at present, the CDR Rules only permit an accredited data recipient to disclose CDR data to an outsourced service provider and another accredited person with an AP disclosure consent.

**Disclosures to Outsourced Service Providers and non-accredited entities:**

- *Disclosures to outsourced service providers (OSPs):* An accredited data recipient must provide:
  - a list of all the outsourced service providers to whom information may be disclosed (whether based in Australia or overseas, and whether they are accredited or not) [33],
  - specific details about the nature of the services provided by these OSPs (for example, where an accredited OSP is collecting CDR data on the accredited data recipient's behalf),[34] and
  - the CDR data or classes of CDR data that may be disclosed to these OSPs.[35]
- *Disclosures to any non-accredited entities (including OSPs):* If an accredited person intends to disclose data to any non-accredited entity, they must include the circumstances in which the accredited person intends to disclose such data.[36]

**Disclosures to entities located overseas:**

- *Disclosures to any overseas accredited data recipients:* If an accredited person is likely to disclose data to any overseas accredited data recipients, the CDR policy must state this fact,[37] and must also include the countries where they are likely to be located, where practicable.[38] If there are numerous countries where CDR data may be disclosed, one option would be to list those countries in an appendix or linked document. If it is impractical to list countries, the CDR policy could instead provide general regions.
- *Disclosures to any overseas, non-accredited OSPs***:** If an accredited person is likely to disclose to any overseas-based, non-accredited OSPs, the CDR policy must include the countries where there are likely to be based in the CDR policy, where practicable.[39] If there are numerous countries where CDR data may be disclosed, one option would be to list those countries in an appendix or linked document. If it is impractical to list countries, the CDR policy could instead provide general regions.

## Overseas storage practices

Where an accredited data recipient proposes to store CDR data outside of Australia or an external territory, it must specify the countries where it proposes to store the data in the policy.[40]

---

[33] CDR Rule 7.2(4)(b).

[34] CDR Rule 7.2(4)(c)(i).

[35] CDR Rule 7.2(4)(c)(ii). The 'classes of CDR data' are set out in the designation instrument for the relevant sector. In the banking sector, the designation instrument sets out three classes of information: customer information, product use information and information about a product.

[36] Section 56ED(5)(g) of the Competition and Consumer Act. Note that at present, the CDR Rules only permit an accredited data recipient to disclose data to non-accredited entities in the cases of outsourced service providers. However, Privacy Safeguard 1 contemplates disclosures to other non-accredited persons.

[37] Section 56ED(5)(e) of the Competition and Consumer Act.

[38] See section 56ED(5)(e)-(f) of the Competition and Consumer Act.

[39] CDR Rule 7.2(4)(d).

[40] CDR Rule 7.2(7).

### When consumers will be notified about certain events

An accredited person's CDR policy must specify the events it will notify the consumer about, in relation to their CDR data.[41]

The events that an accredited person is required to notify the consumer about include:

- when a consumer gives consent to the person collecting, using and/or disclosing their CDR data[42]
- when a consumer amends[43] or withdraws consent[44]
- collection of a consumer's CDR data[45]
- disclosure of a consumer's CDR data to an accredited person[46]
- ongoing notification requirements about a consumer's consent[47]
- notification requirements in relation to the expiry or amending of a consumer's consent[48]
- responses to a consumer's correction request,[49] and
- any eligible data breaches affecting a consumer under the Notifiable Data Breach Scheme.[50]

### Consequences of withdrawing consent

An accredited data recipient must provide a statement in the CDR policy indicating the consequences for the consumer of withdrawing their consent to collect and use CDR data.[51] This may include the details of any early cancellation fees.

### Deletion of CDR data

An accredited data recipient has obligations to destroy or delete or de-identify any redundant CDR data that they hold under Privacy Safeguard 12 and the CDR Rules.

---

[41] Section 56ED (5)(h) of the Competition and Consumer Act.

[42] CDR Rule 4.18 (1)(a). See paragraph C.65-66 of Chapter C (Consent) of the CDR Privacy Safeguard Guidelines.

[43] CDR Rule 4.18 (1)(aa). (See para C.37-43 of Chapter C (Consent of the CDR Privacy Safeguard Guidelines)).

[44] CDR Rule 4.18 (1)(b). See paragraph C.65-66 of Chapter C (Consent) of the CDR Privacy Safeguard Guidelines.

[45] CDR Rule 7.4. See paragraphs 5.29-533 of Chapter 5 (Notifying of collection of CDR data) of the CDR Privacy Safeguard Guidelines.

[46] CDR Rule 7.9(2) (see Chapter 10 (Privacy Safeguard 10).

[47] CDR Rule 4.20. See paragraphs C.65-66 of Chapter C (Consent) of the CDR Privacy Safeguard Guidelines.

[48] CDR Rules 4.18A, 4.18B and 4.18C.

[49] CDR Rule 7.15. See paragraphs 13.25-31 of Chapter 13 (Correction of CDR data) of the CDR Privacy Safeguard Guidelines.

[50] See Chapter 12 (Security of CDR data and destruction and de-identification of redundant CDR data) of the CDR Privacy Safeguard Guidelines, section 56ES of the Competition and Consumer Act, and Part IIIC, Division 3 of the Privacy Act. Further information is available on the OAIC's Notifiable Data Breaches scheme webpage.

[51] CDR Rule 7.2(4)(a).

Consequently, an accredited data recipient must include the following information about the deletion of redundant CDR data in their CDR policy:

- **When redundant data is deleted**.[52] An accredited data recipient may be required to delete redundant data, including where:
  - the consumer has elected for their redundant data to be deleted[53]
  - the general policy is to delete redundant data,[54] or
  - it is not possible to de-identify CDR data to the required extent. [55]
- **Elections to delete redundant data**. An accredited data recipient must include information about:
  - how a consumer may elect for their redundant data to be deleted[56]
  - how the election operates
  - the effect of an election, and
  - how a consumer may exercise their election.[57]
- **How redundant data is deleted**.[58]
  - An accredited data recipient should include a general description of how redundant data is deleted in a way that is helpful and meaningful to the consumer.

### De-identification of CDR data

An accredited data recipient must include the following information about the de-identification of CDR data in their policy:

[52] CDR Rule 7.2(4)(f)(i). See also s 56ED(5)(i) of the Competition and Consumer Act.

[53] A consumer who gave a consent for an accredited person to collect and use CDR data may elect that the CDR data, and any data derived from it, be deleted when it becomes redundant data: CDR Rule 4.16. See Chapter C (Consent) and Chapter 12 (Security of CDR data and destruction of de-identification of redundant CDR data) of the CDR Privacy Safeguard Guidelines for further information.

[54] Where an accredited data recipient advised the consumer of a general policy of deletion, the accredited data recipient must delete the redundant data, even if their general policy has since changed. See Chapter 12 (Security of CDR data and destruction of de-identification of redundant CDR data) of the CDR Privacy Safeguard Guidelines for further information.

[55] CDR Rule 1.17(4). See Chapter 12 (Security of CDR data and destruction of de-identification of redundant CDR data) of the CDR Privacy Safeguard Guidelines for further information about de-identification of CDR data and the 'required extent'.

[56] CDR Rule 7.2(4)(f)(ii).

[57] CDR Rule 7.2(4)(h). A consumer's right to elect for their redundant CDR data to be deleted is contained in CDR Rule 4.16. See Chapter C (Consent) and Chapter 12 (Security of CDR data and destruction of de-identification of redundant CDR data) of the CDR Privacy Safeguard Guidelines for further information about this right.

[58] CDR Rule 7.4(f)(iii).

- **The circumstances in which CDR data is de-identified in accordance with a consumer's request.**[59]
- **For an accredited data recipient, the following information must be included about de-identification of CDR data that is *not* redundant,:**[60]
  - how de-identified CDR data is used to provide goods or services to consumers[61]
  - the process for de-identification including, a description of techniques that are used to de-identify CDR data,[62] and
  - if de-identified CDR data is ordinarily disclosed to one or more persons:
    - the fact of this disclosure
    - the classes of persons to whom such data is ordinarily disclosed,[63] and
    - the purposes for which de-identified CDR data is disclosed.[64]
- **For an accredited data recipient, the following information about de-identification of *redundant* CDR data must be included,:**[65]
  - how the entity ordinarily uses any de-identified redundant data, including examples
  - the process for de-identification, including a description of techniques that are used to de-identify CDR data,[66] and
  - if de-identified redundant data is ordinarily disclosed (by sale or otherwise) to one or more persons:

[59] Section 56ED(5)(i) of the Competition and Consumer Act. A consumer may provide consent for an accredited data recipient to de-identify their CDR data for the purpose of disclosure (including selling) and/or for use in general research (see CDR Rule 1.10A(1)(e) and 7.5(1)(aa). Where the accredited data recipient seeks or intends to seek a de-identification consent, it must provide certain information about de-identification in its CDR policy as outlined in CDR Rule 7.2(4)(e).

[60] These requirements are contained in CDR Rules 7.2(4)(e) and 7.2(5). Examples where this would be applicable include where the accredited data recipient intends to use de-identified CDR data for general research, and/or disclose (including by selling) the de-identified data in accordance with a de-identification consent. See CDR Rules 1.10A(1)(e) and 7.5(1)(aa).

[61] CDR Rule 7.2(4)(e)(i).

[62] CDR Rule 7.2(5)(a). The aim of this requirement is to give consumers greater transparency. This should therefore include a general description of how redundant data is de-identified, with the aim being to assist consumers to understand how the entity gives effect to this de-identification obligation, in a way that is helpful and meaningful to them.

[63] In the context of the CDR policy, 'classes of persons' means the types of entities or persons an accredited data recipient usually discloses de-identified data to ('classes of persons' is not defined in the CDR regime. Accordingly, it has its ordinary meaning). Entities or persons do not need to be listed individually in the CDR policy, but should be described with enough specificity so that the consumer can understand the nature of those parties who will hold or have access to de-identified data.

[64] CDR Rule 7.2(5)(b)(i)-(iii).

[65] These requirements are contained in CDR Rules 7.2(4)(g) and 7.2(5).

[66] CDR Rule 7.2(5)(a). The aim of this requirement is to give consumers greater transparency. Therefore this should include a general description of how redundant data is de-identified, with the aim being to assist consumers to understand how the entity gives effect to this de-identification obligation, in a way that is helpful and meaningful to them.

- the fact of this disclosure
- the classes of person to whom such data is ordinarily disclosed,[67] and
- the purposes for which the de-identified data is disclosed. [68]

## Specific requirements for designated gateways

A designated gateway's CDR policy must provide details about how a consumer can make a complaint in the event that they think the designated gateway has not met its CDR related obligations under the Consumer and Competition Act and/or CDR Rules. The CDR policy must also set out how the designated gateway will deal with these complaints.[69]

Designated gateways must also include information about how they will facilitate the disclosure or ensure the accuracy of CDR data, and any other matters set out under the CDR Rules.[70]

Note: *There are no designated gateways in the banking sector.*

[67] In the context of the CDR policy, 'classes of persons' means the types of entities or persons an accredited data recipient usually discloses de-identified data to ('classes of persons' is not defined in the CDR regime. Accordingly, it has its ordinary meaning). Entities or persons do not need to be listed individually in the CDR policy, but should be described with enough specificity so that the consumer can understand the nature of those parties who will hold or have access to de-identified data.

[68] CDR Rule 7.2(5)(b).

[69] Section 56ED (6)(b) of the Competition and Consumer Act.

[70] Section 56ED (6)(a) of the Competition and Consumer Act.

# Attachment A — Checklist for your CDR policy

### General — for all participants

| Issue | Questions to consider |
|---|---|
| A clearly expressed and up to date policy | • Is your policy clearly expressed, in plain English?<br>• Does the policy reflect your current practices?<br>• Have you planned to undertake a review of your policy? |
| Form and availability of policy | • Is your policy in a different document to your privacy policy?<br>• Is your policy available free of charge? |

### Data holders

| Issue | Questions to consider |
|---|---|
| Availability | • Is your policy readily available on all of the online platforms where you ordinarily deal with consumers?<br>• Does your policy let consumers know that, when requested, you will provide them with a copy of your policy electronically or in hard copy? |
| Complaints process | • Does the policy state where, how and when a complaint can be lodged?<br>• Does the policy state when a consumer should expect an acknowledgment of their complaint?<br>• Does the policy state the information that the consumer needs to provide when making a complaint?<br>• Does the policy outline the process for handling consumer complaints?<br>• Does the policy outline the time periods associated with various stages throughout the complaints process?<br>• Does the policy state the options for redress?<br>• Does the policy state the options for review (both internally, if available) and externally? |
| Access to data | • Does the policy provide information about how a consumer may access their CDR data?<br>• If you are an APP entity under the Privacy Act, does it state how consumers may seek access to their personal information under APP 12? |

| Issue | Questions to consider |
|---|---|
| Correction requests | • Does the policy provide specific details about how a consumer may correct their CDR data?<br>• If you are an APP entity under the Privacy Act, does it state how consumers may seek correction of their personal information under APP 13? |
| Voluntary Consumer Data | • Does the policy state whether you accept requests for voluntary consumer or product data?<br>• If so, are details about how fees can be obtained also provided? |

### Accredited persons

| Issue | Questions to consider |
|---|---|
| Availability | • Is your policy readily available on all the online platforms where you ordinarily deal with consumers?<br>• Does your policy let consumers know that, when requested, you will give them a copy of your policy electronically or in hard copy? |
| Complaints process | • Does the policy state where, how and when a complaint can be lodged?<br>• Does the policy state when a consumer should expect an acknowledgment of their complaint?<br>• Does the policy state the information that the consumer needs to provide when making a complaint?<br>• Does the policy outline the process for handling consumer complaints?<br>• Does the policy outline the time periods associated with various stages throughout the complaints process?<br>• Does the policy state the options for redress?<br>• Does the policy state the options for review (both internally, if available) and externally? |
| Classes of data held | • Does the policy state the classes of CDR data you hold or may hold?<br>• Does the policy state the classes of CDR data that other entities hold or may hold on your behalf?<br>• Does the policy state how CDR data is held? |
| Purpose of data handling | • Are the purposes for which you collect, hold, use or disclose the CDR with the consent of the consumer made clear? |

| Issue | Questions to consider |
|---|---|
| General research | • Does the policy clarify whether any CDR data will be used for general research purposes? If so, does it provide a description of the research to be conducted and detail the additional benefits for a consumer consenting to this use? |
| Access to data | • Does the policy provide information about how a consumer may access their CDR data? |
| Correction requests | • Does the policy provide specific details about how consumers may correct their CDR data? |
| Disclosure | **Outsourced service providers (OSPs)**<br>• If you use or intend to use OSPs, does your CDR policy include a list of all the OSPs to which information may be disclosed?<br>• Does your CDR policy include specific details about the nature of the services provided by these OSPs and the CDR data or classes of CDR data that may be disclosed to them?<br>**Any non-accredited entities**<br>• If you intend to disclose CDR data to any non-accredited entities (including OSPs), does your CDR policy include the circumstances in which you intend to disclose CDR data?<br>**Overseas Accredited Data Recipients**<br>• If you are likely to disclose CDR data to any accredited data recipients located overseas, does your CDR policy state this fact and include the countries where they are likely to be located?<br>**Overseas non-accredited OSPs**<br>• If you are likely to disclose CDR data to any non-accredited OSPs located overseas, does your CDR policy include the countries where they are likely to be located? |
| Withdrawal of consent | • Does your policy include a statement explaining the consequences to the consumer if they withdraw their consent to collect or use CDR data? |
| Storage | • Does your policy provide a list of countries where you intend to store CDR data other than in Australia or an external territory? |
| Notification | • Does your policy contain information about when and in which circumstances you will provide a notification to the consumer? |

| Issue | Questions to consider |
|---|---|
| Deletion of CDR data | • Does your policy include information about the circumstances in which you delete redundant data?<br>• Does your policy include information about how a consumer may elect for their redundant data to be deleted, including how the election operates and the effect of an election?<br>• Do your policy include information about how you delete redundant data? |
| De-identification of CDR data | • Does your policy include information about the circumstances in which you must de-identify CDR data at a consumer's request?<br>• If applicable, does your CDR policy include information about the specified matters, including how de-identified redundant data is ordinarily used?<br>• If applicable, does your CDR policy include information about the specified matters, including how you use de-identified CDR data that is not redundant? |

### Designated gateways

| Issue | Questions to consider |
|---|---|
| Facilitating data flows | • Does the policy include an explanation about how you will act between entities to facilitate the disclosure or accuracy of CDR data, and any other matters outlined under the CDR rules?<br>• Does the policy provide details about how a consumer can make a complaint about a breach of the CDR rules or privacy safeguards? |