Australian Government

Office of the Australian Information Commissioner

Guide to developing a CDR policy

December 2022

OAIC

Version	Currency dates	Changes and other comments
1.0	12-Jun-2020 to 22-Sep-2021	
2.0	23-Sep-2021 to 22-Dec-22	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. 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. 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. New guidance on the interaction between the CDR policy and existing privacy and data protection policies. 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). Updated privacy tip on ensure the CDR policy is easily read and understood. Clarifications to guidance, including: • 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) • information about the de-identification CDR data in a CDR policy.

3.0	22-Dec-22 to …	Updated guidance to reflect amendments to the Competition and Consumer (Consumer Data Right) Rules 2020 made by the Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2021, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021 and Competition and Consumer Amendment (Consumer Data Right) Regulations 2021 including: • new CDR policy content requirements for accredited persons in relation to sponsorship and CDR representative arrangements • a requirement for accredited persons to make their CDR policy readily available through online services of their CDR representatives • additional guidance and context related to the expansion of CDR into the energy sector, including a requirement for energy retailer data holders to explain how a CDR consumer can access and correct their AEMO data • additional detailed guidance about CDR policy requirements.

Contents

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

This Guide does not apply to the Australian Energy Market Operator Limited (AEMO) in its capacity as a data holder, as AEMO is not subject to Privacy Safeguard 1 in this capacity.[1] Accordingly, unless otherwise indicated, references in this Guide to data holders and CDR entities exclude AEMO.

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 consider all your obligations under the *Competition and Consumer Act 2010* (Competition and Consumer Act)[2], the Competition and Consumer (Consumer Data Right) Rules 2020 (CDR Rules) and the *Competition and Consumer Regulations 2010* (Competition and Consumer Regulations).

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, Part 2BA of the Competition and Consumer Regulations and the CDR Privacy Safeguard Guidelines[3] to ensure compliance with your legislative obligations.

Introduction

All CDR entities must have and maintain a clearly expressed and up-to-date CDR policy.[4] A CDR policy must be a separate document to the general privacy policy.[5]

For this Guide, a 'CDR entity' is:

- a data holder of CDR data (other than AEMO)
- a designated gateway for CDR data, or
- an accredited person who is or who may become an accredited data recipient of CDR data.[6]

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:

[1] Competition and Consumer Regulations, paragraph 28RA(1)(a)(i).

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

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

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

[5] CDR Rules, subrule 7.2(2).

[6] An accredited person 'may become' an accredited data recipient when it is seeking to collect CDR data. This means that an accredited person must ensure that it has a CDR policy before it seeks to collect CDR data.

- how CDR data is managed,[7] and
- how they can make an inquiry or make a complaint.[8]

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

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.[9] 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 Privacy Policy to address how a consumer could make an inquiry or make a complaint (even where that APP Privacy 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 Privacy 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 Privacy Policy so consumers are clear about what processes apply to CDR data and when.

[7] Paragraph 56ED(3)(a) of the Competition and Consumer Act.

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

[9] CDR Rules, subrule 7.2(2).

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
- Step 4: Test your CDR policy
- Step 5: Make your CDR policy available
- Step 6: Review and update your CDR 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. This includes understanding relevant practices, procedures and systems, and the other parties you may have arrangements with, such as outsourced service providers or CDR representatives. 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, and other parties you may have arrangements with (such as outsourced service providers or CDR representatives) 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 CDR 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 be clear 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,[10] 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.

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.[11] 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.

[10] CDR Rules, subrule 7.2(2).

[11] Subsection 56ED(3) of the Competition and Consumer Act.

Step 4: Test your CDR 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 easy to read and understand. 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.[12]

Step 5: Make the CDR policy available

Your CDR policy must be freely and publicly available for consumers. If you are an accredited person or data holder, the CDR policy must be available through each online service that you ordinarily use to deal with consumers, such as your website or mobile applications.[13] Additionally, you must provide the CDR policy electronically (for example in a word document or pdf) or in hard copy if requested by the consumer.[14] If you are an accredited person with one or more CDR representatives, your CDR policy must also be available through each online service that your CDR representatives ordinarily use to deal with consumers.[15]

Appropriate accessibility measures should also be put in place so that the CDR 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.[16]

> 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.

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

[13] Subsection 56ED(7) of the Competition and Consumer Act and CDR Rules, subrule 7.2(8).

[14] Subsection 56ED(8) of the Competition and Consumer Act and CDR Rules, subrule 7.2(9).

[15] CDR Rules, subrule 7.2(8). Note that a CDR representative is required to adopt and comply with its CDR principal's CDR policy (CDR Rules, paragraph 1.10AA(2)(e)).

[16] CDR Rules, paragraphs 5.24(i)(ii) and 5.25(1)(b)(ii)(B).

Step 6: Review and update your CDR 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 CDR policy accurately reflects your current CDR data handling practices.[17]

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

- include the date the CDR policy was last reviewed or updated
- invite comments on the CDR 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
  - 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

[17] Subsection 56ED(3) of the Competition and Consumer Act.

- Information about sponsorship arrangements
- Information about CDR representative arrangements
- Information about CDR outsourcing arrangements

- **Specific requirements for designated gateways**:
  - Facilitating disclosure or accuracy of CDR data
  - 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 Competition and Consumer Act and/or CDR Rules.[18]

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
- the process for handling consumer complaints[19]
- the time periods associated with the various stages of the complaints process
- options for redress,[20] and
- options for review both internally (if available) and externally.[21]

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

[19] Internal dispute resolution requirements are set out in the CDR Rules (Part 5 of Schedule 3 for the banking sector and Part 5 of Schedule 4 for the energy sector).

[20] 'Redress' in this context means options for remedy, rather than options for review. This could include resolution options such as correction, apology, etc.

[21] CDR Rules, subrule 7.2(6). This would include the relevant recognised external dispute resolution scheme and the Office of the Australian Information Commissioner.

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.[22]

A data holder may receive a request from an accredited person on the consumer's behalf, or a consumer may make a request directly to the data holder.[23]

A data holder that is a retailer in the energy sector must also ensure that its CDR policy explains how a consumer can access their AEMO data.[24]

Where the data holder is also an 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.[25]

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.[26] 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.[27] 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.[28]

A data holder that is a retailer in the energy sector must also ensure that its CDR policy explains how a CDR consumer can correct their AEMO data.[29]

---

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

[23] For the banking sector, a data holder's obligations under Part 3 of the CDR Rules (regarding consumer data requests made by consumers) have not yet commenced: clause 6.6 of Schedule 3 to the CDR Rules. Part 3 does not apply in relation to energy sector data: clause 8.5 of Schedule 4 to the CDR Rules.

[24] Competition and Consumer Regulations, paragraph 28RA(3)(a).

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

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

[27] Paragraph 56EP(1)(c) of the Competition and Consumer Act.

[28] 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.

[29] Competition and Consumer Regulations, paragraph 28RA(3)(a).

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,[30] and
- state whether the data holder charges fees for such requests (and if so, how consumers can obtain information about those fees).[31]

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 for which CDR data is collected, held, used and disclosed
- undertaking general research
- who CDR data may be disclosed to
- overseas data storage practices
- when consumers will be notified about certain events
- consequences of withdrawing consent
- deletion of CDR data
- de-identification of CDR data[32]

[30] CDR Rules, paragraph 7.2(3)(a). Voluntary product data means CDR data for which there are no consumers that is not required product data (clause 3.1 of Schedule 3, and clause 3.1 of Schedule 4, 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, and clause 3.2 of Schedule 4 to the CDR Rules).

[31] CDR Rules, paragraph 7.2(3)(b).

[32] See subsection 56ED(5) of the Competition and Consumer Act and CDR Rules, subrule 7.2(4).

- Information about sponsorship arrangements
- Information about CDR representative arrangements, and
- Information about CDR outsourcing arrangements.

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).[33] 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 3 classes of information: customer information, product use information and information about the product.[34] For the energy sector, the designation instrument sets out 4 classes of information: information about a customer or associate, information about the sale or supply of electricity, information about retail arrangements, and information about retail arrangements (natural gas).[35]

The CDR policy must also set out how the CDR data is held. This means providing general information about how data is stored.[36]

Purposes for which CDR data is collected, held, used and disclosed

An accredited person must indicate the purposes for which it does each of the following (with the consumer's consent): collects, holds, uses or discloses CDR data.[37]

Undertaking general research

If an accredited person wishes to undertake general research[38] using de-identified CDR data, its CDR policy must include:

- a description of the research to be conducted, and

---

[33] Paragraph 56ED(5)(a) of the Competition and Consumer Act. An outsourced service provider may collect CDR data on an accredited person's behalf. For further information, see CDR Rules, rule 1.10, and Chapter 3 (Seeking to collect CDR data from CDR participants) of the CDR Privacy Safeguard Guidelines.

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

[35] See sections 7-10 of the Consumer Data Right (Energy Sector) Designation 2020.

[36] Subsection 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'.

[37] Paragraph 56ED(5)(b) of the Competition and Consumer Act.

[38] CDR Rules, paragraph 7.2(4)(h). 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 consumer. CDR Rules, paragraph 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.

- 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 its disclosures of CDR data to outsourced service providers, non-accredited entities and entities located overseas, as set out below.[39]

Disclosures to outsourced service providers and non-accredited entities:

- *Disclosures to outsourced service providers:* Where an accredited person may disclose CDR data to an outsourced service provider, it must include the CDR data or classes of CDR data that may be disclosed to these outsourced service providers.[40,41]
- *Disclosures to any non-accredited entities (including non-accredited outsourced service providers):* If an accredited person intends to disclose CDR data to any non-accredited entity, it must include the circumstances in which the accredited person intends to disclose such data.[42] Disclosures to non-accredited entities include disclosures:
  - to unaccredited outsourced service providers
  - to CDR representatives with whom the accredited person has a CDR representative arrangement[43]
  - to trusted advisers with a TA disclosure consent,[44] and
  - of CDR insights to specified persons with an insight disclosure consent.[45]

Disclosures to entities located overseas:

- *Disclosures to any overseas accredited persons:* If an accredited person is likely to disclose CDR data to any overseas accredited persons, the CDR policy must state this fact,[46] and must also

[39]Note that the CDR Rules only permit an accredited data recipient to disclose CDR data in limited circumstances: to an outsourced service provider, to another accredited person with an AP disclosure consent, to a trusted adviser with a TA disclosure consent, or to its CDR representative in accordance with a CDR representative arrangement. An accredited data recipient is also permitted to disclose a CDR insight to a specified person with an insight disclosure consent.

[40] CDR Rules, paragraph 7.2(4)(g)(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. In the energy sector, the designation instrument sets out four classes of information: customer or associate information, information about the sale or supply of electricity, information about retail arrangements, and information about retail arrangements (natural gas).

[41] Additional CDR policy requirements in relation to outsourced services providers are outlined below under the heading 'Information about outsourced service providers'.

[42] Paragraph 56ED(5)(g) of the Competition and Consumer Act.

[43] Note that an accredited person who is a CDR principal also needs to include in its CDR policy details of CDR representative arrangements – see CDR Rules, paragraphs 7.2(4)(d) – (e).

[44] See CDR Rules, subparagraph 1.10A(1)(c)(iii) for information about TA disclosure consents.

[45] See CDR Rules, subparagraph 1.10A(1)(c)(iv) and subrule 1.10A(3) for information about insight disclosure consent.

[46] Paragraph 56ED(5)(e) of the Competition and Consumer Act.

include the countries where they are likely to be located, where practicable.[47] 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 outsourced service providers*: If an accredited person is likely to disclose CDR data to any overseas-based, non-accredited outsourced service providers, the CDR policy must include the countries where they are likely to be based, where practicable.[48] 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 data storage practices

If an accredited person 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 CDR policy.[49]

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.[50]

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[51]
- when a consumer amends[52] or withdraws consent[53]
- collection of a consumer's CDR data[54]
- disclosure of a consumer's CDR data to an accredited person[55]
- ongoing notification requirements about a consumer's consent[56]
- notification requirements in relation to the expiry of a consumer's consent[57]

---

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

[48] CDR Rules, paragraph 7.2(4)(i).

[49] CDR Rules, subrule 7.2(7).

[50] Paragraph 56ED (5)(h) of the Competition and Consumer Act.

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

[52] CDR Rules, paragraph 4.18 (1)(aa). See paragraphs C.37-43 of Chapter C (Consent of the CDR Privacy Safeguard Guidelines.

[53] CDR Rules, paragraph 4.18 (1)(b). See paragraphs C.65-66 of Chapter C (Consent) of the CDR Privacy Safeguard Guidelines.

[54] CDR Rules, rule 7.4. See paragraphs 5.29-533 of Chapter 5 (Notifying of collection of CDR data) of the CDR Privacy Safeguard Guidelines.

[55] CDR Rules, subrule 7.9(2) (see Chapter 10 (Notifying of the disclosure of CDR data) of the CDR Privacy Safeguard Guidelines).

[56] CDR Rules, rule 4.20. See paragraphs C.65-66 of Chapter C (Consent) of the CDR Privacy Safeguard Guidelines.

[57] CDR Rules, rule 4.18A.

- responses to a consumer's correction request,[58] and
- any eligible data breaches affecting a consumer under the Notifiable Data Breach Scheme.[59]

Consequences of withdrawing consent

An accredited person must provide a statement in the CDR policy indicating the consequences for the consumer of withdrawing their consent to collect and use CDR data.[60] This may include the details of any early cancellation fees or loss of access to goods or services based on CDR data.

Deletion of CDR data

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

An accredited person must include the following information about the deletion of redundant CDR data in its CDR policy:

- **When redundant CDR data is deleted**.[61] An accredited data recipient may be required to delete redundant CDR data, including where:
  - the consumer has elected for their redundant CDR data to be deleted[62]
  - the general policy is to delete redundant CDR data,[63] or
  - it is not possible to de-identify CDR data to the required extent. [64]
- **Elections to delete CDR redundant data**. An accredited person must include information about:
  - how a consumer may elect for their redundant CDR data to be deleted[65]
  - how the election operates

---

[58] CDR Rules, rule 7.15. See paragraphs 13.25-31 of Chapter 13 (Correction of CDR data) of the CDR Privacy Safeguard Guidelines.

[59] See Chapter 12 (Security of CDR data and destruction and de-identification of redundant CDR data) of the CDR Privacy Safeguard Guidelines, s 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.

[60] CDR Rules, paragraph 7.2(4)(a).

[61] CDR Rules, paragraph 7.2(4)(k)(i). See also para 56ED(5)(i) of the Competition and Consumer Act.

[62] 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 CDR data: CDR Rules, 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.

[63] Where an accredited data recipient advised the consumer of a general policy of deletion, the accredited data recipient must delete the redundant CDR data, even if its 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.

[64] CDR Rules, subrule 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'.

[65] CDR Rules, paragraph 7.2(4)(k)(ii).

- the effect of an election, and
- how a consumer may exercise their election.[66]

- **How redundant CDR data is deleted**.[67]
- An accredited person should include a general description of how redundant CDR data is deleted in a way that is helpful and meaningful to the consumer.[68]

De-identification of CDR data

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

- **The circumstances in which CDR data is de-identified in accordance with a consumer's request.**[69]
- **The following information about de-identification of CDR data that is *not* redundant:**[70]
- how de-identified CDR data is used to provide goods or services to consumers[71]
- the process for de-identification including, a description of techniques that are used to de-identify CDR data,[72] and
- if de-identified CDR data is ordinarily disclosed to one or more persons:
    - the fact of this disclosure

[66] CDR Rules, paragraph 7.2(4)(m). A consumer's right to elect for their redundant CDR data to be deleted is contained in CDR Rules, 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.

[67] CDR Rules, paragraph 7.4(k)(iii).

[68] This could include whether redundant CDR data is irretrievably destroyed, reference to any applicable standards, how the accredited person manages hard copy information, how it confirms third party deletion and whether back-ups are secured. Part B of the OAIC's Guide to securing personal information outlines questions entities should consider when destroying personal information. Also see Chapter 12 of the CDR Privacy Safeguard Guidelines for information on the CDR deletion process.

[69] Paragraph 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 Rules, paragraphs 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 Rules, paragraph 7.2(4)(j).

[70] These requirements are contained in CDR Rules, paragraph 7.2(4)(j) and subrule 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, paragraphs 1.10A(1)(e) and 7.5(1)(aa).

[71] CDR Rules, paragraph 7.2(4)(j)(i).

[72] CDR Rules, paragraph 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 CDR 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 classes of persons to whom such data is ordinarily disclosed,[73] and
- the purposes for which de-identified CDR data is disclosed.[74]

- **The following information about de-identification of *redundant* CDR data:**[75]

- how the entity ordinarily uses any de-identified redundant CDR data, including examples
- the process for de-identification, including a description of techniques that are used to de-identify CDR data,[76] and
- if de-identified redundant CDR data is ordinarily disclosed (by sale or otherwise) to one or more persons:
  - the fact of this disclosure
  - the classes of person to whom such data is ordinarily disclosed,[77] and
  - the purposes for which the de-identified data is disclosed. [78]

Information about sponsorship arrangements

An accredited person must ensure that its CDR policy sets out:

- if the accredited person is a sponsor, a list of affiliates with whom the sponsor has a sponsorship arrangement, and the nature of the services one party provides to the other under each arrangement, and
- if the accredited person is an affiliate, a list of sponsors with whom the affiliate has a sponsorship arrangement, and the nature of the services one party provides to the other party under each arrangement.[79]

[73] 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 system. 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.

[74] CDR Rules, paragraph 7.2(5)(b)(i)-(iii).

[75] These requirements are contained in CDR Rules, paragraph 7.2(4)(l) and subrule 7.2(5).

[76] CDR Rules, paragraph 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 CDR 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.

[77] 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 system. 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.

[78] CDR Rules, paragraph 7.2(5)(b).

[79] CDR Rules, paragraphs 7.2(4)(aa) - (c).

Information about CDR representative arrangements

Where an accredited person is a CDR principal under a CDR representative arrangement, its CDR policy must include:

- a list of its CDR representatives
- for each CDR representative, the nature of the goods and services that the CDR representative provides to customers using CDR data.[80]

Information about CDR outsourcing arrangements

Where an accredited person has one or more CDR outsourcing arrangements with outsourced service providers, its CDR policy must include:

- a list of its outsourced service providers (whether based in Australia or overseas, and whether they are accredited or not)[81]
- specific details about the nature of the services provided by these outsourced service providers (for example, where an outsourced service provider is collecting CDR data on the accredited person's behalf)[82]
- the CDR data or classes of CDR data that may be disclosed to, or collected by, these outsourced service providers.[83]

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 Part IVD of the Competition and Consumer Act and/or CDR Rules. The CDR policy must also set out how the designated gateway will deal with these complaints.[84]

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.[85]

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

---

[80] CDR Rules, paragraphs 7.2(4)(d) and (e).

[81] CDR Rules, paragraph 7.2(4)(f).

[82] CDR Rules, paragraph 7.2(4)(g)(i).

[83] CDR Rules, paragraph 7.2(4)(g)(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. In the energy sector, the designation instrument sets out four classes of information: customer or associate information, information about the sale or supply of electricity, information about retail arrangements, and information about retail arrangements (natural gas).

[84] Paragraph 56ED (6)(b) of the Competition and Consumer Act.

[85] Paragraph 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 CDR policy	• Is your CDR policy clearly expressed, in plain English? • Does your CDR policy reflect your current practices? • Have you planned to undertake a review of your CDR policy?
Form and availability of CDR policy	• Is your CDR policy in a different document to your privacy policy? • Is your CDR policy available free of charge?

Data holders

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

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

Accredited persons

Issue	Questions to consider
Availability	• Is your CDR policy readily available on all online platforms where you ordinarily deal with consumers? • If you have a CDR representative, is your CDR policy available on all the online platforms through which it ordinarily deals with consumers? • Does your CDR 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 CDR policy state where, how and when a complaint can be lodged? • Does the CDR policy state when a consumer should expect an acknowledgment of their complaint? • Does the CDR policy state the information that the consumer needs to provide when making a complaint? • Does the CDR policy outline the process for handling consumer complaints? • Does the CDR policy outline the time periods associated with various stages throughout the complaints process? • Does the CDR policy state the options for redress? • Does the CDR policy state the options for review (both internally, if available) and externally?

Issue	Questions to consider
Classes of CDR data held	• Does the CDR policy state the classes of CDR data you hold or may hold? • Does the CDR policy state the classes of CDR data that other entities hold or may hold on your behalf? • Does the CDR policy state how CDR data is held?
Purpose of CDR data handling	• Are the purposes for which you collect, hold, use or disclose the CDR with the consent of the consumer made clear?
General research	• Does the CDR 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 CDR data	• Does the CDR policy provide information about how a consumer may access their CDR data?
Correction requests	• Does the CDR policy provide specific details about how consumers may correct their CDR data?
Disclosure	**Outsourced service providers** • If you use or intend to disclose CDR data to outsourced service providers, does your CDR policy include the CDR data or classes of CDR data that may be disclosed to them? **Any non-accredited entities** • If you intend to disclose CDR data to any non-accredited entities (including outsourced service providers), does your CDR policy include the circumstances in which you intend to disclose CDR data? **Overseas accredited persons** • If you are likely to disclose CDR data to any accredited persons located overseas, does your CDR policy state this fact and include the countries where they are likely to be located? **Overseas non-accredited outsourced service providers** • If you are likely to disclose CDR data to any non-accredited outsourced service providers located overseas, does your CDR policy include the countries where they are likely to be located?
Withdrawal of consent	• Does your CDR policy include a statement explaining the consequences to the consumer if they withdraw their consent to collect or use CDR data?
Storage	• Does your CDR policy provide a list of countries where you intend to store CDR data other than in Australia or an external territory?

Issue	Questions to consider
Notification	• Does your CDR policy contain information about when and in what circumstances you will provide a notification to the consumer?
Deletion of CDR data	• Does your CDR policy include information about the circumstances in which you delete redundant CDR data? • Does your CDR policy include information about how a consumer may elect for their redundant CDR data to be deleted, including how the election operates and the effect of an election? • Does your CDR policy include information about how you delete redundant data?
De-identification of CDR data	• Does your CDR policy include information about the circumstances in which you must de-identify CDR data at a consumer's request? • If applicable, does your CDR policy include information about the specified matters, including how de-identified redundant data is ordinarily used? • If applicable, does your CDR policy include information about the specified matters, including how you use de-identified CDR data that is not redundant?
CDR outsourcing arrangements	• If you use outsourced service providers, does your CDR policy set out a list of your outsourced service providers, the nature of the services each outsourced service provider provides, and the CDR data or classes of CDR data that may be disclosed to, or collected by, each provider?
Sponsorship arrangements	• If you are a sponsor, does your CDR policy set out a list of affiliates with whom you have a sponsorship arrangement, and the nature of the services one party provides to the other under each arrangement? • If you are an affiliate, does your CDR policy set out a list of sponsors with whom you have a sponsorship arrangement, and the nature of the services one party provides to the other under each arrangement?
CDR representative arrangements	• If you are a CDR principal, does your CDR policy set out a list of the representatives with whom you have a CDR representative arrangement, and the nature of the goods and services that the representatives provide to consumers using CDR data?

Designated gateways

Issue	Questions to consider
Facilitating data flows	• Does your CDR 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? • Does the CDR policy provide details about how a consumer can make a complaint about a breach of the CDR Rules or privacy safeguards?