Chapter 6:

# Privacy Safeguard 6 —

## Use or disclosure of CDR data by accredited data recipients or designated gateways

Version 5.0, November 2023



OAIC

# Contents

# Key points

- Privacy Safeguard 6,[1] together with rules 7.5, 7.5A, 7.6 and 7.7 of the consumer data rules (CDR Rules), applies to accredited data recipients of a consumer's CDR data, placing restrictions and obligations on them in relation to the use and disclosure of that data.[2]
- Generally, accredited data recipients of CDR data and designated gateways can use or disclose CDR data only where required or authorised under the CDR Rules. The consumer must consent to these uses and disclosures of their CDR data.
- Subrule 7.5(1) of the CDR Rules outlines the permitted uses and disclosures of CDR data.
- In addition, subrule 7.5(2), rule 7.5A and subrule 7.6(1) of the CDR Rules prohibit certain uses or disclosures of CDR data.
- Accredited data recipients of CDR data must comply with the data minimisation principle when using that data to provide the goods or services requested by the consumer, or to fulfil any other purpose consented to by the consumer.

# What does Privacy Safeguard 6 say?

## Accredited data recipients

6.1 An accredited data recipient of a consumer's CDR data must not use or disclose that data unless the:

- disclosure is required under the CDR Rules in response to a valid request from a consumer for the CDR data
- use or disclosure is otherwise required or authorised under the CDR Rules, or
- use or disclosure is required or authorised by or under another Australian law or a court/tribunal order, and the accredited data recipient makes a written note of the use or disclosure.

6.2 To be compliant with Privacy Safeguard 6, an accredited data recipient of CDR data must satisfy the requirements under subrules 7.5(1) and (2), and rules 7.5A and 7.6 of the CDR Rules.

## Designated gateways

6.3 A designated gateway for CDR data must not use or disclose CDR data unless the:

- disclosure is required under the CDR Rules
- use or disclosure is authorised under the CDR Rules, or

[1] Competition and Consumer Act, section 56EI.

[2] Privacy Safeguard 6 also applies to designated gateways. However, there are currently no designated gateways in the banking or energy sector, and no CDR Rules for the use or disclosure of CDR data by designated gateways. See paragraphs 6.3 to 6.4 for further information about the current application of Privacy Safeguard 6 to designated gateways.

- use or disclosure is required or authorised by or under an Australian law, or a court/tribunal order, and the designated gateway makes a written note of the use or disclosure.

6.4 While Privacy Safeguard 6 applies to designated gateways, there are currently no designated gateways in the banking or energy sector.[3] There are also currently no CDR Rules for the use or disclosure of CDR data by designated gateways.[4]

# Who does Privacy Safeguard 6 apply to?

6.5 Privacy Safeguard 6 applies to accredited data recipients of CDR data and designated gateways for CDR data.

6.6 It does not apply to data holders. However, data holders should ensure that they adhere to their obligations under the *Privacy Act 1988* (the Privacy Act) and the APPs, including APP 6, when using or disclosing personal information.[5]

6.7 Data holders should also ensure that if they are a primary data holder, they comply with rule 1.24 of the CDR Rules in relation to SR data they receive from a secondary data holder in response to an SR data request.[6] Rule 1.24 states that primary data holders must not use or disclose such SR data for a purpose other than responding to the SR data request. Once the primary data holder has responded to the SR data request, it must follow the CDR data deletion process in rule 1.18 of the CDR Rules.

6.8 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 6. However, under the terms of the CDR representative arrangement with their CDR representative principal,[7] a CDR representative is required to comply with Privacy Safeguard 6 as if it were the CDR representative principal.[8] It also must not use or disclose the service data unless doing so would be in accordance with the CDR representative arrangement,[9] and a permitted use or disclosure under certain provisions in CDR Rules, rule 7.5.[10] Further, any use or disclosure of service data by the CDR representative is taken to

[3] For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: Consumer Data Right (Energy Sector) Designation 2020, subsection 6(4). However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in paragraph 56AL(2)(c) of the Competition and Consumer Act.

There are also no designated gateways in the telecommunications sector or non-bank lending sectors, although unlike banking and energy at the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications or non-bank lending data under the CDR system: Consumer Data Right (Telecommunications Sector) Designation 2022; Consumer Data Right (Non-Bank Lenders) Designation 2022.

[4] CDR Rules, rule 7.7, which relates to Privacy Safeguard 6, only applies to accredited data recipients.

[5] For the purposes of APP 6.2(b), the Competition and Consumer Act is an Australian law that may require or authorise a data holder to disclose personal information.

[6] See Chapter B (Key concepts) for more information on SR data and primary and secondary data holders.

[7] A CDR representative arrangement is a written contract between a CDR representative and their CDR representative principal. The requirements for this arrangement are outlined in CDR Rules, rule 1.10AA.

[8] CDR rules, paragraph 1.10AA(4)(a)(iia).

[9] CDR Rules, paragraph 1.10AA(4)(c).

[10] CDR Rules, paragraph 1.10AA(4)(d).

have been a use or disclosure by their CDR representative principal (regardless of whether the CDR representative's actions accord with the CDR representative arrangement).[11]

6.9 Where they are a non-accredited entity, an outsourced service provider (OSP) is not directly bound by Privacy Safeguard 6. However, under the terms of the CDR outsourcing arrangement with their OSP principal,[12] an OSP is required to comply with Privacy Safeguard 6 in its handling of service data as if it were the OSP principal.[13] It also must not use or disclose the service data unless doing so would be in accordance with the CDR outsourcing arrangement.[14] Further, any use or disclosure of service data by the OSP is taken to have been a use or disclosure by their OSP principal (regardless of whether the OSP's actions accord with the CDR outsourcing arrangement).[15]

# How Privacy Safeguard 6 interacts with the Privacy Act

6.10 It is important to understand how Privacy Safeguard 6 interacts with the Privacy Act and the APPs.[16]

6.11 APP 6 relates to the use or disclosure of personal information. [17]

| CDR entity | Privacy protections that apply in the CDR context |
|---|---|
| **Accredited data recipient** | **Privacy Safeguard 6**<br>For accredited data recipients of a consumer's CDR data, Privacy Safeguard 6 applies to the use or disclosure of that data. [18]<br>APP 6 does not apply in relation to that CDR data.[19] |

[11] CDR Rules, subrule 7.6(4). See also rule 1.16A in relation to a CDR representative principal's obligations and liability.

[12] A CDR outsourcing arrangement is a written contract between an OSP principal and their provider that meets the minimum requirements listed in CDR Rules, subrule 1.10(3).

[13] CDR Rules, paragraph 1.10(3)(b)(i)(C),

[14] CDR Rules, paragraph 1.10(3)(b)(iv).

[15] CDR Rules, subrule 7.6(5). See also rule 1.16 in relation to an OSP principal's obligations and liability.

[16] The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

[17] APP 6 provides that if an APP entity holds personal information about an individual that was collected for a particular purpose, the entity must not use or disclose the information for another purpose unless an exception applies. See APP Guidelines, Chapter 6 (APP 6).

[18] Privacy Safeguard 6 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the consumer data rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See Competition and Consumer Act, section 56EK.

[19] The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 56EC(4) does not affect how the APPs apply to accredited

| | |
|---|---|
| **Designated gateway** | **Privacy Safeguard 6**<br>For designated gateways for CDR data, Privacy Safeguard 6 applies to the use and disclosure of the CDR data.[20]<br>APP 6 does not apply in relation to that CDR data. [21] |
| **Data holder**[22] | **APP 6**<br>Privacy Safeguard 6 does not apply to a data holder. |

# Why is it important?

6.12 Consumer consent for the use and disclosure of their CDR data is at the heart of the CDR system.

6.13 By adhering to Privacy Safeguard 6 an accredited data recipient or designated gateway will ensure consumers have control over what their CDR data is being used for and who it is disclosed to. This is an essential part of the CDR system.

# What is meant by 'use' and 'disclose'?

## 'Use'

6.14 The term 'use' is not defined within the *Competition and Consumer Act 2010* (Competition and Consumer Act).[23]

6.15 An accredited data recipient or designated gateway 'uses' CDR data where it handles or undertakes an activity with the CDR data within its effective control. For further discussion of use, see Chapter B (Key concepts). For example, 'use' includes:

- the entity accessing and reading the CDR data
- the entity making a decision based on the CDR data
- the entity de-identifying the CDR data, and
- the entity passing the CDR data from one part of the entity to another.

persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See Privacy Act, subsection 6E(1D).) Subsection 56EC(4) also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See Competition and Consumer Act, paragraph 56EC(5)(aa).

[20] Competition and Consumer Act, subsection 56EI(2). See paragraphs 6.3 to 6.4 for further information about the current application of Privacy Safeguard 6 to designated gateways.

[21] The APPs do not apply to designated gateways for CDR data in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(d). However, subsection 56EC(4) does not affect how the APPs apply to designated gateways who are APP entities, in relation to the handling of personal information outside the CDR system. See Competition and Consumer Act, paragraph 56EC(5)(b).

[22] In this chapter, references to data holders include AEMO. See Chapter B for further information about how the privacy safeguards apply to AEMO.

[23] The term 'use' is also not defined in the Privacy Act.

## 'Disclose'

6.16 The term 'disclose' is not defined within the Competition and Consumer Act.[24]

6.17 An accredited data recipient or designated gateway 'discloses' CDR data when it makes it accessible or visible to others outside the entity.[25] This focuses on the act done by the disclosing party, and not on the actions or knowledge of the recipient. There will be a disclosure in these circumstances even where the information is already known to the recipient. For further discussion of disclosure, see Chapter B (Key concepts).

6.18 Examples of disclosure include where an accredited data recipient or designated gateway:

- shares the CDR data with another entity or individual, including a related party of the entity (subject to some exceptions, as outlined in paragraph 6.19 below)
- publishes the CDR data on the internet, whether intentionally or not
- accidentally provides CDR data to an unintended recipient
- reveals the CDR data in the course of a conversation with a person outside the entity, and
- displays data on a computer screen so that the CDR data can be read by another entity or individual.

6.19 Where an accredited data recipient engages a third party to perform services on its behalf, the provision of CDR data to that third party will in most circumstances be a disclosure. However, in limited circumstances, providing CDR data to a third party to perform services on behalf of the entity may be a use, rather than a disclosure. See 'use' and 'disclosure' in Chapter B (Key concepts) for guidance on how to determine whether providing CDR data to a third party is a use or disclosure.

# When can an accredited data recipient use or disclose CDR data?

6.20 This section outlines when an accredited data recipient may use or disclose CDR data.[26]

6.21 This chapter does not consider when a designated gateway may use or disclose CDR data. This is because there are currently no designated gateways in the banking sector or energy sector.[27]

---

[24] The term 'disclose' is also not defined in the Privacy Act.

[25] Information will be 'disclosed' under the CDR system regardless of whether an entity retains effective control over the data.

[26] Privacy Safeguard 6 allows for the use or disclosure of CDR data in certain circumstances. One of these circumstances is where the disclosure is required under the CDR Rules in response to a valid request from a consumer for the CDR data: Competition and Consumer Act, paragraph 56EI(1)(a). The CDR Rules do not currently require an accredited data recipient to disclose CDR data in response to a valid request – they only *authorise* the accredited data recipient to do so.

As such, an accredited data recipient is currently only able to use or disclose CDR data where required or authorised under the CDR Rules or under an Australian law or a court/tribunal order. These circumstances are outlined in this chapter from paragraph 6.24 onwards.

[27] For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: Consumer Data Right (Energy

6.22 The following diagram outlines at a high-level the permitted and prohibited uses or disclosures of CDR data for an accredited data recipient. These uses and disclosures are discussed further below in this section.

6.23 An accredited data recipient must comply with the data minimisation principle when using CDR data. For further information on the data minimisation principle, see paragraphs 6.29-6.31 below.

Sector) Designation 2020, subsection 6(4). However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in paragraph 56AL(2)(c) of the Competition and Consumer Act.

## Permitted uses or disclosures of CDR data by accredited data recipients[1]

- Providing goods or services requested by the consumer
- Deriving CDR data to provide goods or services requested by the consumer
- Disclosing CDR data to the consumer to provide the requested goods or services
- Disclosing CDR data to a direct or indirect OSP in order to provide goods or services requested by the consumer
- Disclosing CDR data that has been de-identified in accordance with the CDR rules
- De-identifying CDR data for use in general research and/or for disclosure, with the consumer's consent and in accordance with the CDR data de-identification process
- Disclosing CDR data to an accredited person, in accordance with a consumer's 'AP disclosure consent'
- Disclosing CDR data to a trusted adviser in accordance with a consumer's 'TA disclosure consent'
- Disclosing CDR insights to a specified person in accordance with a consumer's 'insight disclosure consent'
- Disclosing a CDR business consumer's CDR data in accordance with a business consumer disclosure consent
- Disclosing CDR data to an accredited person if the CDR consumer has provided the accredited person and accredited data recipient with the appropriate consents
- Disclosing service data to the principal under a CDR outsourcing arrangement
- Disclosing CDR data to the other party in a sponsorship arrangement for the purpose of providing goods or services requested by the consumer
- For a CDR representative principal, disclosing CDR data to a CDR representative for certain permitted purposes
- Using or disclosing CDR data where required or authorised by law

## Prohibited uses or disclosures of CDR data by accredited data recipients

- Using the CDR data to identify, compile insights or build a profile about a person who isn't the consumer, unless an exception applies
- Any uses or disclosures that an accredited data recipient is not permitted to seek consent for (permitted consents are listed in Rule 1.10A)
- Disclosing a CDR insight that includes or reveals sensitive information as defined in the *Privacy Act 1988*

[1] A disclosure is only a permitted use or disclosure if it is done in accordance with the data standards

## Use or disclosure required or authorised under the CDR Rules

6.24 Privacy Safeguard 6 provides that an accredited data recipient of CDR data must not use or disclose CDR data unless the use or disclosure is required or authorised under the CDR Rules.[28]

6.25 Subrule 7.5(1) of the CDR Rules authorises the following permitted uses or disclosures of CDR data by accredited data recipients:

- using CDR data to provide goods or services requested by the consumer in compliance with the data minimisation principle and in accordance with a current use consent from the consumer (other than a direct marketing consent)
- de-identifying CDR data in accordance with the CDR de-identification process[29] to use for general research and/or for disclosing (including by selling) the de-identified data, in accordance with a current de-identification consent from the consumer[30]
- directly or indirectly deriving CDR data from the collected CDR data in accordance with the above uses
- disclosing to the consumer any of their CDR data for the purpose of providing the existing goods or services[31]
- disclosing the consumer's CDR data in accordance with a current disclosure consent. This includes:[32]
    - disclosing CDR data to an accredited person in accordance with a current 'AP disclosure consent'
    - disclosing CDR data to a trusted adviser in accordance with a current 'TA disclosure consent'
    - disclosing a CDR insight to a specified person for a permitted purpose in accordance with a current 'insight disclosure consent'

[28] Competition and Consumer Act, paragraph 56EI(1)(b). The use or disclosure of CDR data by accredited data recipients is not currently required under the CDR Rules. The use or disclosure of CDR data by accredited data recipients is authorised under the CDR Rules if it is a 'permitted use or disclosure' under CDR Rule 7.5 that does not relate to direct marketing: CDR Rules, subrule 7.6(1) and rule 7.7. See paragraphs 6.3 to 6.4 for further information about the current application of Privacy Safeguard 6 to designated gateways.

[29] See CDR Rules, rule 1.17.

[30] 'General research' is defined in rule 1.7 of the CDR Rules to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular CDR consumer. Note that while paragraph 7.5(1)(b) of the CDR Rules refers to a current 'use consent', a de-identification consent is a form of 'use consent' and is the relevant category of consent that must be obtained for the purposes of paragraph 7.5(1)(b) of the CDR Rules.

[31] The phrase, 'existing goods or services' is defined in paragraph 7.5(1)(a) of the CDR Rules to mean the goods or services requested by the consumer.

[32] Note that a 'TA disclosure consent', an 'insight disclosure consent', an 'AP disclosure consent' and a 'business consumer disclosure consent' are all forms of 'disclosure consents' referred to in paragraph 7.5(1)(e) of the CDR Rules and are the relevant categories of consent that must be obtained for the purposes of this rule.

- disclosing a CDR business consumer's CDR data to a specified person in accordance with a current 'business consumer disclosure consent.[33]

- disclosing the consumer's CDR data to a direct or indirect OSP under a CDR outsourcing arrangement, or to the other party in a sponsorship arrangement:
  - for specific purposes, and
  - to the extent reasonably needed to do those things[34]
- disclosing (by sale or otherwise) to any person, CDR data that has been de-identified in accordance with the CDR data de-identification process on becoming redundant data[35]
- where the accredited data recipient collected CDR data on behalf of an OSP principal under a CDR outsourcing arrangement— using or disclosing service data to in accordance with the relevant CDR outsourcing arrangement [36]
- disclosing CDR data to an accredited person if the CDR consumer has provided the accredited person and accredited data recipient the appropriate consents,[37] and
- where the accredited data recipient is a CDR representative principal under a CDR representative arrangement – disclosing CDR data to a CDR representative for the purposes of a use or disclosure by the CDR representative that would be a permitted use or disclosure under certain provisions in rule 7.5(1) if the CDR representative were an accredited data recipient that had collected the CDR data under the consumer data request.[38]

6.26 The disclosures outlined in paragraph 6.25 are only permitted disclosures if they are done in accordance with the data standards.[39]

6.27 Subrule 7.5(2) and rule 7.5A of the CDR Rules prohibit the following uses or disclosures of CDR data by accredited data recipients:

- any uses or disclosures that an accredited data recipient is not permitted to seek consent for[40]

---

[33] This will become a permitted use or disclosure on the earlier of 1 November 2023 or the day the Data Standards Chair makes standards about the process for obtaining and managing business consumer statements and business consumer disclosures – see CDR Rules, subrule 7.5A(5).

[34] CDR Rules, paragraph 7.5(1)(f).

[35] CDR Rules, paragraph 7.5(1)(g).

[36] CDR Rules, paragraph 7.5(1)(h).

[37] CDR Rules, paragraph 7.5(1)(i) permits the disclosure of CDR data to an accredited person if the consumer has given the accredited person a collection and use consent to collect CDR data from the accredited data recipient. The consumer must also have given the accredited data recipient an AP disclosure consent. For further information on the types of consents, see Chapter C (Consent).

[38] CDR Rules, paragraph 7.5(1)(j). A permitted use or disclosure includes those uses and disclosures outlined in paragraphs (a) to (g) or (i) of subrule 7.5(1) of the CDR Rules.

[39] CDR Rules, subrule 7.5(2)(a).

[40] CDR Rules, paragraphs 7.5(2)(b) and 4.12(3)(a) (and paragraph 4.20F(3)(a) in relation to CDR representatives). An accredited data recipient may only ask a consumer to consent to the use or disclosure of their CDR data where use or disclosure falls within a category of consents. The categories of consents are outlined subrule 1.10A(2) of the CDR Rules. For further information on consent, see Chapter C (Consent).

- disclosures of a CDR insight under an insight disclosure consent if the insight includes or reveals sensitive information as defined under section 6 of the Privacy Act.[41] For the definition of sensitive information, see Chapter B (Key concepts).
- using CDR data for the purpose of identifying, compiling insights in relation to, or building a profile in relation to, any identifiable person who is not a consumer who made the consumer data request (including through aggregating the CDR data), unless the accredited data recipient is, in accordance with the consumer's consent:
    - deriving, from that CDR data, CDR data about that person's interactions with the consumer, and
    - using that derived CDR data in order to provide the requested goods or services.[42]

6.28 The permitted uses and disclosures (in paragraph 6.25) are discussed further in this chapter.

## Using CDR data in compliance with the data minimisation principle

6.29 An accredited data recipient must comply with the data minimisation principle when using CDR data to provide goods or services requested by the consumer, or to fulfil any other purpose consented to by the consumer.[43]

6.30 An accredited data recipient complies with the data minimisation principle if, when providing the requested goods or services or using collected CDR data for any other purpose consented to by the CDR consumer, it does not use the collected CDR data, or CDR data derived from it, beyond what is reasonably needed to provide the goods or services requested by the consumer or fulfill the other purpose as consented to by the consumer. [44] The accredited data recipient must also not seek to collect more CDR data than is reasonably needed or CDR data that relates to a longer time period than is reasonably needed..[45]

6.31 The data minimisation principle and meaning of 'reasonably needed' are discussed in more detail in Chapter B (Key concepts) and, as they relate to consent for collection, in Chapter 3 (Privacy Safeguard 3).

**Risk point:** An accredited person should pay careful attention to its processes and systems to ensure it complies with the data minimisation principle for all uses of CDR data. This includes consideration of the minimum CDR data needed to provide each good or service to a consumer.

**Privacy tip:** An accredited person should set up its systems and processes so that it can identify the minimum CDR data needed for a particular good or service. This will reduce the risk of over collection of CDR data and ensure that the person does not exceed the limitations imposed by the data minimisation principle.

---

[41] CDR Rules, subrule 7.5A(4).

[42] CDR Rules, paragraphs 7.5(2)(b) and 4.12(3)(b) (and paragraph 4.20F(3)(b) in relation to CDR representatives). Subrule 4.12(3) prohibits an accredited data recipient from asking a consumer to give consent to use or disclosure for these purposes. For further information regarding restrictions on seeking consent, see Chapter C (Consent).

[43] CDR Rules, paragraph 7.5(1)(a) and subrule 1.8(2).

[44] CDR Rules, subrule 1.8(2).

[45] CDR Rules, subrule 1.8 (1).

## Using CDR data in accordance with a current consent to provide goods or services requested by the consumer

6.32 An accredited data recipient is authorised to use CDR data in accordance with a current use consent from the consumer to provide goods or services requested by the consumer.[46]

6.33 The relevant uses are those uses to which the consumer expressly consented, when providing a valid request for the accredited person to collect their CDR data from a CDR participant under subrule 4.3(1) of the CDR Rules.[47] Valid requests are discussed further in Chapter 3 (Privacy Safeguard 3).

6.34 For information regarding use consents and how they must be managed, see Chapter C (Consent).

**Example**

SpendLess Pty Ltd is an accredited data recipient for Oliver's CDR data, and provides Oliver with budgeting tips through its mobile budgeting application.

SpendLess runs Oliver's transaction data through an algorithm to ascertain what other SpendLess products Oliver might be interested in.

When providing his valid request to SpendLess,[48] Oliver consented to the analysis of his transaction data so that SpendLess can identify how much money he has been spending in particular categories. He did not consent to his transaction data being used to allow SpendLess to develop and communicate offers about other products.

SpendLess has used Oliver's CDR data in a way that is not in accordance with his use consent, and this use would therefore not be a permitted use under paragraph 7.5(1)(a) of the CDR Rules.[49]

## Using or disclosing de-identified CDR data in accordance with a de-identification consent

6.35 An accredited data recipient is permitted to de-identify CDR data in accordance with a current de-identification consent from the consumer to:

- use the de-identified data for general research, and/or
- disclose (including by selling) the de-identified data.[50]

---

[46] CDR Rules, paragraph 7.5(1)(a). The requested goods or services are the goods or services requested under subrule 4.3(1) of the CDR Rules as part of the consumer's valid request.

[47] Note: paragraph 7.5(1)(a) of the CDR Rules permits the general 'use' of CDR data to provide the goods and services requested by the consumer. Paragraph 7.5(1)(a) of the CDR Rules does not authorise the specific types of uses defined under 'de-identification consent' or 'direct marketing consent' as per rule 1.10A. (These uses are instead authorised by CDR Rules, paragraph 7.5(1)(b) and subrule 7.5(3), respectively.)

[48] 'Valid requests' are defined in rule 4.3 of the CDR Rules. A key component of a 'valid request' is the consumer's collection consent and use consent. For further information, see Chapter 3 (Privacy Safeguard 3).

[49] SpendLess has used Oliver's CDR data in a manner that may constitute direct marketing under the CDR system. For information regarding direct marketing, see Chapter 7 (Privacy Safeguard 7).

[50] CDR Rules, paragraph 7.5(1)(b).

6.36 The CDR data must be de-identified in accordance with the CDR data de-identification process outlined in rule 1.17 of the CDR Rules.[51]

6.37 'General research' means research undertaken using de-identified CDR data that does not relate to the provision of goods or services to any particular consumer[52] (for example, research for product or business development).[53]

6.38 Before de-identifying CDR data under a de-identification consent in accordance with rule 1.17 of the CDR Rules, the accredited data recipient must have first:

- received a de-identification consent from the consumer,[54] and
- provided the consumer with additional information relating to the de-identification of CDR data.[55]

## Deriving or indirectly deriving CDR data

6.39 An accredited data recipient is permitted to directly or indirectly derive CDR data from the collected CDR data in order to use the data to provide the goods or services requested by the consumer.[56]

6.40 Derived CDR data is discussed in more detail in Chapter B (Key concepts).

## Disclosing CDR data to the consumer

6.41 An accredited data recipient is permitted to disclose to a consumer any of their CDR data for the purpose of providing the existing goods or services.[57]

6.42 This includes CDR data collected from a data holder or accredited data recipient in response to the consumer's valid request, as well as data that has been directly and/or indirectly derived from such CDR data.

6.43 This is a permitted disclosure under subrule 7.5(1) of the CDR Rules and does not require the consent of the consumer.

## Disclosing CDR data to an accredited person

6.44 An accredited data recipient is permitted to disclose a consumer's CDR data to an accredited person in accordance with an 'AP disclosure consent'.[58]

---

[51] For further information regarding the CDR data de-identification process, see Chapter 12 (Privacy Safeguard 12). CDR Rules, paragraph 7.5(1)(b).

[52] CDR Rules, subrule 1.7(1).

[53] Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [21].

[54] A 'de-identification consent' is defined in paragraph 1.10A(1)(e) of the CDR Rules. It must be sought in accordance with the requirements in Division 4.3 of the CDR Rules. For further information, see Chapter C (Consent).

[55] CDR Rules, paragraph 4.11(3)(e) and rule 4.15. For further information, see Chapter C (Consent).

[56] CDR Rules, paragraph 7.5(1)(c).

[57] CDR Rules, paragraph 7.5(1)(d).

[58] CDR Rules, paragraphs 7.5(1)(e) and 7.5(1)(i). Note that while paragraph 7.5(1)(e) of the CDR Rules refers to a current 'disclosure consent', an AP disclosure consent is a form of 'disclosure consent' and is a relevant category of consent for the purposes of paragraph 7.5(1)(e).

6.45 An 'AP disclosure consent' is a consent given by the consumer for an accredited data recipient to disclose their CDR data to an accredited person in response to a consumer data request.[59]

6.46 For further information on 'AP disclosure consents' and consumer data requests, see Chapter C Consent).

## Disclosing CDR data to a trusted adviser

6.47 An accredited data recipient is permitted to disclose a consumer's CDR data to a 'trusted adviser' in accordance with a 'TA disclosure consent'.[60]

6.48 A 'TA disclosure consent' is a consent given by the consumer for an accredited data recipient to disclose their CDR data to a trusted adviser to enable the consumer to receive advice or a service from that adviser.[61]

6.49 Trusted advisers must belong to one of the following specified classes:[62]

- qualified accountants within the meaning of the *Corporations Act 2001*[63]
- people admitted to the legal profession that hold a current practising certificate
- registered tax agents, BAS agents and tax (financial) advisers within the meaning of the *Tax Agent Services Act 2009*
- financial counselling agencies within the meaning of the ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792
- financial advisers that are relevant providers under the *Corporations Act 2001*, other than provisional and limited-service time-share advisers, and
- mortgage brokers within the meaning of the *National Consumer Credit Protection Act 2009*.

6.50 A person is taken to be a member of a class of trusted adviser if the accredited data recipient has taken 'reasonable steps' to confirm that the person is, and remains, a member of that class.[64] For more information on reasonable steps, see Chapter B (Key concepts).

6.51 Where an accredited data recipient discloses CDR data to someone who is not a member of a trusted adviser class the disclosure would contravene subrule 7.6(1) of the CDR Rules, unless the person took reasonable steps to confirm the person belonged to the class.

6.52 Trusted advisers are not CDR participants and are therefore not subject to the privacy safeguards or other obligations that apply under the CDR system. This means that the CDR data will no longer be subject to the protections of the CDR system. An accredited data recipient must explain this to the consumer at the time of disclosure in accordance with the

---

[59] CDR Rules, paragraph 1.10A(1)(c)(i). For further information, see Chapter C (Consent).

[60] CDR Rules, paragraph 7.5(1)(e). Note that while paragraph 7.5(1)(e) refers to a current 'disclosure consent', a TA disclosure consent is a form of 'disclosure consent' and is a relevant category of consent for the purposes of paragraph 7.5(1)(e).

[61] CDR Rules, paragraph 1.10A(1)(c)(iii).

[62] CDR Rules, subrule 1.10C(2).

[63] Section 88B of the *Corporations Act 2001* states that ASIC may declare in writing persons who are qualified accountants for the purposes of that Act. ASIC's qualified accountant declaration instrument can be accessed here: https://asic.gov.au/regulatory-resources/financial-services/financial-product-disclosure/certificates-issued-by-a-qualified-accountant/.

[64] CDR Rules, subrule 1.10C(3)).

relevant data standard.[65] The classes of trusted advisers are professions subject to existing regulatory frameworks, including consumer protection mechanisms.

6.53 For further information on 'TA disclosure consents' and consumer data requests, see Chapter C (Consent).

## Disclosing a CDR insight to a specified person

6.54 An accredited data recipient is permitted to disclose a CDR insight in accordance with an 'insight disclosure consent'.[66]

6.55 'CDR insights' are insights based on a consumer's CDR data. CDR insights remain CDR data. These insights are intended to allow accredited data recipients to disclose CDR data outside the CDR system to either confirm, deny, or provide simple information to a person selected by the consumer, where this is for a limited, permitted purpose.

6.56 An 'insight disclosure consent' is a consent given by the consumer for an accredited data recipient to disclose CDR insights outside the CDR system for these limited purposes:[67]

- to verify the consumer's identity
- to verify the consumer's account balance, or
- to verify the details of credits to, and debits from, the consumer's accounts.[68]

6.57 CDR insights can be disclosed to any person, provided the consumer has given valid consent.

6.58 This means that, unless the insight is disclosed to an accredited person, the CDR data will no longer be subject to the protections and safeguards of the CDR system. An accredited data recipient must explain this to the consumer at the time of disclosure in accordance with the relevant data standard.[69]

6.59 For further information on 'insight disclosure consents' and consumer data requests, see Chapter C (Consent).

## Disclosing CDR data under a business consumer disclosure consent

6.60 An accredited data recipient is permitted to disclose a CDR business consumer's CDR data to a specified person in accordance with a 'business consumer disclosure consent' if the consumer has also given a business consumer statement.[70]

---

[65] CDR Rules, paragraph 8.11(1)(c)(iv). See section on 'Disclosure Consent: Non-Accredited Person Disclosure Notification' in the Consumer Data Standards, available at: https://consumerdatastandards.gov.au/consumer-data-standards/current-reference.

[66] CDR Rules, paragraph 7.5(1)(e)). Note that while paragraph 7.5(1)(e) refers to a current 'disclosure consent', an insight disclosure consent is a form of 'disclosure consent' and is a relevant category of consent for the purposes of paragraph 7.5(1)(e).

[67] CDR Rules, subrule 1.10A(3).

[68] CDR Rules, paragraph 1.10A(3)(a)(i)-(iii).

[69] CDR Rules, paragraph 8.11(1A)(b). See section on 'Disclosure Consent: Non-Accredited Person Disclosure Notification' in the Consumer Data Standards, available at: https://consumerdatastandards.gov.au/consumer-data-standards/current-reference.

[70] CDR Rules, paragraph 1.10A(1)(c)(v), subrule 1.10A(10) and paragraph 7.5(1)(e). Note that while paragraph 7.5(1)(e) of the CDR Rules refers to a current 'disclosure consent', a business consumer disclosure consent is a form of 'disclosure consent' and is a relevant category of consent for the purposes of paragraph 7.5(1)(e).

6.61 For further information on 'business consumer disclosure consents' and consumer data requests, see Chapter C (Consent).

## Disclosing CDR data to an OSP

6.62 An accredited data recipient is permitted to disclose the consumer's CDR data to their direct or indirect OSP for the purpose of:

- using the consumer's CDR data to provide goods or services requested by the consumer, including by directly or indirectly deriving CDR data from the CDR data
- disclosing, to the consumer, any of their CDR data for the purpose of providing the existing goods or services, or
- disclosing CDR data in accordance with a current disclosure consent,

to the extent reasonably needed to do those things.[71]

**Example**

BrightSpark Pty Ltd is an accredited data recipient for Zachary's CDR data and provides Zachary with electricity savings tips through its mobile electricity usage application.

BrightSpark provided the information required by paragraph 4.11(3)(f) of the CDR Rules to Zachary when it asked him to give the relevant consent. BrightSpark includes information about OSPs in its CDR policy (per subrule 7.2(4) of the CDR Rules).

BrightSpark engages SaveEnergy Pty Ltd to analyse consumers' data and report on consumers' electricity usage trends, so that BrightSpark can provide tailored electricity savings advice to consumers.

BrightSpark discloses Zachary's account and electricity usage data to SaveEnergy. However, BrightSpark did not first consider whether SaveEnergy needs both electricity usage and account data for this purpose.

If SaveEnergy does not need to analyse Zachary's account data in order to report on his electricity usage trends, BrightSpark may have disclosed Zachary's CDR data to an OSP beyond the extent reasonably needed to provide the service requested by Zachary. The disclosure by BrightSpark may therefore not be a permitted disclosure under paragraph 7.5(1)(f) of the CDR Rules.

6.63 The consumer's CDR data includes data collected from a data holder or accredited data recipient in response to the consumer's request. The consumer's CDR data also includes data that has been directly and/or indirectly derived from their CDR data.

6.64 Disclosure of a consumer's CDR data by an accredited data recipient to an OSP for the purpose outlined in paragraph 6.62 is a permitted disclosure under subrule 7.5(1) of the CDR Rules that does not require the consent of the consumer.[72]

6.65 Any use or disclosure by a direct or indirect OSP of an accredited data recipient (or of a CDR representative of an accredited data recipient) of CDR data disclosed under a CDR

[71] CDR Rules, paragraph 7.5(1)(f).

[72] However, the accredited data recipient must ensure it has complied with the requirements set out in paragraph 6.62.

outsourcing arrangement will be taken to have been a use or disclosure by the accredited data recipient. This occurs regardless of whether the use or disclosure is in accordance with the arrangement.[73]

6.66 When disclosing CDR data to an OSP located outside of Australia, an accredited data recipient must also have regard to the requirements for disclosure of CDR data to an overseas recipient under Privacy Safeguard 8.[74] See Chapter 8 (Privacy Safeguard 8) for more information.

6.67 For further information, see Chapter B (Key Concepts), 'Outsourced service providers'.

## Disclosing CDR data to the other party in a sponsorship arrangement

6.68 A party to a sponsorship arrangement is permitted to disclose the consumer's CDR data to the other party to the arrangement for the purpose of:

- using the consumer's CDR data to provide goods or services requested by the consumer, including by directly or indirectly deriving CDR data from the CDR data
- de-identifying CDR data to use for general research and/or to disclose (including by selling) the de-identified data, in accordance with a current de-identification consent
- disclosing, to the consumer, any of their CDR data for the purpose of providing the existing goods or services
- disclosing CDR data in accordance with a current disclosure consent

to the extent reasonably needed to do those things.[75]

## Disclosures of CDR data by an accredited OSP

6.69 Where an accredited data recipient has collected CDR data on behalf of another accredited person in its capacity as a direct or indirect OSP of the person under a CDR outsourcing arrangement, the accredited data recipient is permitted to use or disclose that CDR data in accordance with the arrangement.[76]

6.70 Disclosure of CDR data in relation to a CDR outsourcing arrangement by an accredited data recipient to the relevant principal is a permitted disclosure under subrule 7.5(1) of the CDR Rules that does not require the consent of the consumer.

[73] CDR Rules, subrule 7.6(2). See also section 56AU of the Competition and Consumer Act, regarding the application to acts done by or in relation to agents of CDR entities.

[74] An accredited person must also include certain information in its CDR policy about OSPs located overseas: CDR Rules, paragraph 7.2(4)(d). See Chapter 1 (Privacy Safeguard 1) for further information.

[75] CDR Rules, paragraph 7.5(1)(f).

[76] CDR Rules, paragraph 7.5(1)(h)—this rule only applies to OSPs who are accredited. More broadly, all OSPs must only use and disclose data in accordance with their CDR outsourcing arrangement with their OSP principal.

## Disclosing service data to a CDR representative in a CDR representative arrangement

6.71 A CDR representative principal may disclose CDR data it collected on behalf of its CDR representative to that CDR representative for purposes of the CDR representative:

- using the CDR data to provide goods or services (in accordance with a use consent, and the data minimisation principal)
- in accordance with a de-identification consent, de-identifying the data to use for general research or to disclose (including by sale)
- directly or indirectly deriving CDR data from the collected CDR data in order to use the data for the 2 purposes outlined above
- disclosing to the CDR consumer any of their own CDR data, to provide the consumer with the requested good or services
- disclosing the consumer's CDR data in accordance with a current disclosure consent
- disclosing a CDR consumer's CDR data to a direct or indirect OSP for the purpose of:
    - using the consumer's CDR data to provide goods or services requested by the consumer, including by directly or indirectly deriving CDR data from the CDR data, or
    - disclosing, to the consumer, any of their CDR data for the purpose of providing the existing goods or services,
    - disclosing CDR data in accordance with a current disclosure consent,

  to the extent reasonably needed to do those things
- disclosing (by sale or otherwise) to any person, CDR data that has been de-identified in accordance with the CDR data de-identification process on the data becoming redundant data, and
- disclosing CDR data to an accredited person if the CDR consumer has provided the accredited person and accredited data recipient the appropriate consents.[77]

6.72 Any use or disclosure of service data by a CDR representative is taken to have been by the CDR representative principal, whether or not the use or disclosure is in accordance with the CDR representative arrangement.[78]

# Use or disclosure under Australian law or a court/tribunal order

6.73 An accredited data recipient may use or disclose CDR data if that use or disclosure is required or authorised by or under an Australian law or a court/tribunal order, and the entity makes a written note of the use or disclosure.[79]

[77] CDR Rules, paragraph 7.5(1)(j).

[78] CDR Rules, subrule 7.6(4).

[79] Competition and Consumer Act, paragraph 56EI(1)(c).

6.74 For the purposes of Privacy Safeguard 6, an Australian law does not include the APPs under the Privacy Act.[80]

6.75 'Australian law' and 'court/tribunal order' are discussed in Chapter B (Key concepts).

6.76 The accredited data recipient must keep a written note of any uses or disclosures made on this ground.

6.77 A written note should include the following details:

- the date of the use or disclosure
- details of the CDR data that was used or disclosed
- the relevant Australian law or court/tribunal order that required or authorised the use or disclosure
- if the accredited data recipient used the CDR data, how the CDR data was used by the accredited data recipient, and
- if the accredited data recipient disclosed the CDR data, to whom the CDR data was disclosed.

# Interaction with other Privacy Safeguards

6.78 The restrictions on using or disclosing CDR data in Privacy Safeguard 6 are additional to those in Privacy Safeguards 7 (see Chapter 7 (Privacy Safeguard 7)), 8 (see Chapter 8 (Privacy Safeguard 8)) and 9 (see Chapter 9 (Privacy Safeguard 9)).

6.79 Privacy Safeguard 7 prohibits accredited data recipients and designated gateways from using or disclosing CDR data for direct marketing unless the use or disclosure is required or authorised under the CDR Rules and in accordance with a valid consent.

6.80 Privacy Safeguard 8 prohibits an accredited data recipient from disclosing CDR data to an overseas recipient unless an exception applies.

6.81 Privacy Safeguard 9 prohibits an accredited data recipient of CDR data that contains a government related identifier from adopting, using or disclosing that identifier, unless an exception applies.

6.82 Privacy Safeguard 7 operates to the exclusion of Privacy Safeguard 6[81] (which means that direct marketing uses or disclosures cannot be authorised under Privacy Safeguard 6), while Privacy Safeguards 8 and 9 operate as restrictions in addition to Privacy Safeguard 6.[82]

[80] Competition and Consumer Act, subsection 56EI(1) (Note 3) and paragraph 56EC(4)(a).

[81] Competition and Consumer Act, subsection 56E(3).

[82] See Competition and Consumer Act, Note 2 of section 56EK and Note 2 of section 56EL.