Chapter 6:

Privacy Safeguard 6 —

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

Version 3.0, June 2021

OAIC

Contents

Key points

- Privacy Safeguard 6, together with consumer data rules (CDR Rules) 7.5, 7.5A, 7.6 and 7.7, 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.
- 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.
- CDR Rule 7.5(1) outlines the permitted uses and disclosures of CDR data.
- In addition, CDR Rules 7.5(2), 7.5A and 7.6(1) 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 CDR Rule 7.5.

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
- 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.

Who does Privacy Safeguard 6 apply to?

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

6.5 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 Australian privacy Principles (APPs), including APP 6, when using or disclosing personal information.[1]

Note: *There are no designated gateways in the banking sector. See Chapter B (Key concepts) for the meaning of designated gateway.*

How Privacy Safeguard 6 interacts with the Privacy Act

6.6 It is important to understand how Privacy Safeguard 6 interacts with the Privacy Act and the APPs.[2]

6.7 APP 6 relates to the use or disclosure of personal information.[3]

CDR entity	Privacy protections that apply in the CDR context
Accredited data recipient	**Privacy Safeguard 6** For accredited data recipients of a consumer's CDR data, Privacy Safeguard 6 applies to the use or disclosure of that data.[4] APP 6 does not apply in relation to that CDR data.[5]
Designated gateway	**Privacy Safeguard 6** For designated gateways for CDR data, Privacy Safeguard 6 applies to the use and disclosure of the CDR data.[6]

[1] 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.

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

[3] 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 Chapter 6: APP 6 — Use or disclosure of personal information of the APP Guidelines.

[4] 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 s 56EK of the Competition and Consumer Act.

[5] The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data - s 56EC(4)(a) of the Competition and Consumer Act. However, s 56EC(4) does not affect how the APPs apply to accredited 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 s 6E(1D) of the Privacy Act.) Section 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 s 56EC(5)(aa) of the Competition and Consumer Act.

[6] Section 56EI(2) of the Competition and Consumer Act.

	APP 6 does not apply in relation to that CDR data. [7]
Data holder	**APP 6** Privacy Safeguard 6 does not apply to a data holder.

Why is it important?

6.8 Consumer consent for the use and disclosure of their CDR data is at the heart of the CDR regime.

6.9 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 regime.

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

'Use'

6.10 The term 'use' is not defined within the Consumer and Competition Act.[8]

6.11 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.

'Disclose'

6.12 The term 'disclose' is not defined within the Consumer and Competition Act.[9]

6.13 An accredited data recipient or designated gateway 'discloses' CDR data when it makes it accessible or visible to others outside the entity.[10] 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).

[7] The APPs do not apply to designated gateways for CDR data in relation to that CDR data - s 56EC(4)(d) of the Competition and Consumer Act. However, s 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 s 56EC(5)(b) of the Competition and Consumer Act.

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

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

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

6.14 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 6.15 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.

6.15 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 paragraphs B.123 and B.172-173 of 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?

6.16 This section outlines when an accredited data recipient may use or disclose CDR data.[11]

6.17 This chapter does not consider when a designated gateway may use or disclose CDR data. This is because there are no designated gateways for the banking sector.

6.18 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.

6.19 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 6.25-6.27 below.

[11] 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 (s 56EI(1)(a) of the Competition and Consumer Act). 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 [6.20] onwards.

Permitted uses or disclosure of CDR data

- 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 an outsourced service provider 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
- From 1 July 2021 (or a relevant data standard being made), disclosing CDR data to an accredited person, in accordance with a consumer's 'AP 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
- Using or disclosing CDR data where required or authorised by law

Prohibited uses or disclosure of CDR data

- 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)
- Prior to 1 July 2021 (or a relevant data standard being made) disclosing the CDR data to an accredited person in accordance with an 'AP disclosure consent'

Use or disclosure required or authorised under the CDR Rules

6.20 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.[12]

6.21 CDR Rule 7.5(1) authorises the following permitted uses or disclosures of CDR data:

- 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 Rules 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 [13]
- 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[14]
- disclosing the consumer's CDR data to an outsourced service provider:
  - for the purpose of doing the things referred to above, and
  - to the extent reasonably needed to do those things
- from 1 July 2021 or the making of a relevant data standard, disclosing CDR data to an accredited person in accordance with a current 'AP disclosure consent'[15]
- disclosing (by sale or otherwise) to any person, CDR data that has been de-identified in accordance with the CDR data de-identification process[16]

---

[12] Section 56EI(1)(b) of the Competition and Consumer Act. The use or disclosure of CDR data is not currently required under the CDR Rules. The use or disclosure of CDR data 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 7.6(1) and 7.7).

[13] 'General research' is defined in CDR Rule 1.7 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 CDR Rule 7.5(1)(aa) 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 CDR Rule 7.5(1)(aa).

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

[15] Disclosure of CDR data to an accredited person under an 'AP disclosure consent' is not a permitted use or disclosure until the earlier of 1 July 2021 or the day a consumer experience data standard is made for the disclosure of CDR data to accredited persons: CDR Rule 7.5A.

Note that while CDR Rule 7.5(1)(ca) refers to a current 'disclosure consent', an AP disclosure consent is a form of 'disclosure consent' and is the relevant category of consent that must be obtained for the purposes of CDR Rule 7.5(1)(ca).

[16] CDR Rule 7.5(1)(e). This permitted disclosure authorises the disclosure of CDR data that has been de-identified in accordance with the CDR data de-identification process, whether in accordance with a de-identification consent from the consumer or because the data was redundant data that needed to be de-identified for the purposes of Privacy Safeguard 12.

- where the accredited data recipient collected CDR data on behalf of a principal under a CDR outsourcing arrangement—disclosing service data to the principal under the arrangement, and
- disclosing CDR data to an accredited person if the CDR consumer has provided the accredited person and accredited data recipient the appropriate consents.[17]

6.22 CDR Rules 7.5(2) and 7.5A prohibit the following uses or disclosures of CDR data:

- any uses or disclosures that an accredited data recipient is not permitted to seek consent for[18]
- prior to 1 July 2021 or a relevant data standard being made, disclosing CDR data to an accredited person under an AP disclosure consent[19]
- 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.

6.23 CDR Rule 4.12(3) prohibits an accredited data recipient from asking a consumer to give consent to the use or disclosure of their CDR data for the above prohibited uses or disclosures.[20]

6.24 The permitted uses and disclosures (in paragraph 6.21) are discussed further in this chapter.

Using CDR data in compliance with the data minimisation principle

6.25 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.[21]

6.26 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.[22]

---

[17] CDR Rule 7.5(1)(g) 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).

[18] 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 CDR Rule 1.10A(2). For further information on consent, see Chapter C (Consent).

[19] Disclosure of CDR data to an accredited person under an AP disclosure consent is not a permitted use or disclosure until the earlier of 1 July 2021 or the day a consumer experience data standard is made for the disclosure of CDR data to accredited persons: CDR Rule 7.5A.

[20] For further information regarding restrictions on seeking consent, see Chapter C (Consent).

[21] CDR Rule 7.5(1)(a).

[22] CDR Rule 1.8(b).

The accredited data recipient must also not seek to collect the CDR data to use for a longer time period than is reasonably needed.[23]

6.27 The data minimisation principle and meaning of 'reasonably needed' is discussed in more detail in Chapter B (Key concepts) and, as it relates 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.

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

6.28 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.[24]

6.29 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 CDR Rule 4.3(1).[25] Valid requests are discussed further in Chapter 3 (Privacy Safeguard 3).

6.30 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.

cont

[23] CDR Rule 1.8 (a)(ii).

[24] CDR Rule 7.5(1)(a). The requested goods or services are the goods or services requested under CDR Rule 4.3(1) as part of the consumer's valid request.

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

When providing his valid request to SpendLess,[26] 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 CDR Rule 7.5(1)(a).[27]

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

6.31 An accredited data recipient is permitted to de-identify CDR data in accordance with a current de-identification consent[28] from the consumer to:

- use the de-identified data for general research, and/or
- disclose (including by selling) the de-identified data.[29]

6.32 The CDR data must be de-identified in accordance with the CDR data de-identification process outlined in CDR Rule 1.17.[30]

6.33 'General research' means research undertaken using de-identified CDR data, and that does not relate to the provision of goods or services to any particular consumer[31] (for example, research for product or business development).[32]

6.34 Before de-identifying CDR data in accordance with CDR Rule 1.17, the accredited data recipient must have first:

- received a de-identification consent from the consumer,[33] and
- provided the consumer with additional information relating to the de-identification of CDR data.[34]

[26] 'Valid requests' are defined in CDR Rule 4.3. 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).

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

[28] Note that while CDR Rule 7.5(1)(aa) 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 CDR Rule 7.5(1)(aa).

[29] CDR Rule 7.5(1)(aa).

[30] For further information regarding the CDR data de-identification process, see Chapter 12 – Security of CDR data and destruction or deidentification of redundant data. CDR Rule 7.5(1)(aa).

[31] CDR Rule 1.7(1).

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

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

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

Deriving or indirectly deriving CDR data

6.35 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.[35]

6.36 This is a permitted use under CDR Rule 7.5(1) and does not require the consent of the consumer.

6.37 However, where an accredited person:

- wishes to derive, from the consumer's CDR data, CDR data about the interactions between the consumer and an identifiable person who is not the consumer, and
- will use that derived data to provide the goods or services requested by the consumer

the accredited data recipient must seek consent from the consumer before doing so.[36]

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

Disclosing CDR data to the consumer

6.39 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.[37]

6.40 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.

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

Disclosing CDR data to an outsourced service provider

6.42 An accredited data recipient is permitted to disclose the consumer's CDR data to an outsourced service provider 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, and
- disclosing, to the consumer, any of their CDR data for the purpose of providing the existing goods or services,

to the extent reasonably needed to do those things.[38]

[35] CDR Rule 7.5(1)(b).

[36] CDR Rule 4.12(4).

[37] CDR Rule 7.5(1)(c).

[38] CDR Rule 7.5(1)(d).

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 engages KnowYourMoney Pty Ltd to analyse consumers' data and report on consumers' spending trends per category, so that SpendLess can provide tailored budgeting advice to consumers.

SpendLess discloses Oliver's account and transaction data to KnowYourMoney. However, Spendless did not first consider whether KnowYourMoney needs both transaction and account data for this purpose.

If KnowYourMoney does not need to analyse Oliver's account data in order to report on his spending trends, SpendLess may have disclosed Oliver's CDR data to an outsourced service provider beyond the extent reasonably needed to provide the service requested by Oliver. The disclosure by SpendLess may therefore not be a permitted disclosure under CDR Rule 7.5(1)(d).

6.43 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.

6.44 Disclosure of a consumer's CDR data by an accredited data recipient to an outsourced service provider for the purpose outlined in paragraph 6.39 is a permitted disclosure under CDR Rule 7.5(1) that does not require the consent of the consumer.[39]

6.45 Where an accredited person intends to disclose the CDR data of a consumer to an outsourced service provider, the accredited person must:

- provide certain information to the consumer at the time of seeking the consumer's consent to collect and use the consumer's CDR data,[40] and
- include certain information about outsourced service providers in its CDR policy.[41]

6.46 An accredited data recipient who discloses CDR data to an outsourced service provider under a CDR outsourcing arrangement must ensure that the provider complies with its requirements under the arrangement.[42]

6.47 For the purposes of this permitted disclosure, an outsourced service provider is a person to whom an accredited data recipient discloses CDR data under a CDR outsourcing arrangement.[43]

6.48 In addition, the accredited data recipient should ensure that the relevant CDR outsourcing arrangement requires the outsourced service provider to adhere to the accredited data recipient's Privacy Safeguard obligations.

---

[39] However, the accredited data recipient must ensure it has complied with the requirements set out in paragraph 6.39.

[40] CDR Rule 4.11(3)(f). See Chapter C (Consent).

[41] CDR Rule 7.2(4). See Chapter 1 (Privacy Safeguard 1).

[42] CDR Rule 1.16.

[43] CDR Rule 1.10. A CDR outsourcing arrangement is a written contract between the accredited data recipient and outsourced service provider which meets the requirements set out in CDR Rule 1.10(2), and under which the provider will provide goods or services to the accredited data recipient. For further information, see Chapter B (Key Concepts).

6.49 The contract should also provide the accredited data recipient with the appropriate level of transparency to allow them to monitor and audit the CDR outsourcing arrangement.

6.50 The CDR data disclosed by an accredited data recipient to a provider under the CDR outsourcing arrangement, including any data directly or indirectly derived from such CDR data, is known as 'service data' in relation to that arrangement.

6.51 Any use or disclosure of such service data by the outsourced service provider (or their subcontractor) will be taken to have been by the accredited data recipient. This occurs regardless of whether the use or disclosure is in accordance with the arrangement.[44]

6.52 When disclosing CDR data to an outsourced service provider 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.[45] See Chapter 8 (Privacy Safeguard 8) for more information.

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

Disclosing CDR data to an accredited person

6.54 From the earlier of 1 July 2021 or the making of a relevant data standard,[46] an accredited data recipient is permitted to disclose a consumer's CDR data to an accredited person in accordance with an 'AP disclosure consent'.[47] Prior to this, disclosing CDR data to an accredited person under an AP disclosure consent is prohibited.[48]

6.55 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.[49]

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

Disclosing service data to a principal in an CDR outsourcing arrangement

6.57 Where an accredited data recipient has collected CDR data on behalf of a principal (i.e. as an outsourced service provider) under a CDR outsourcing arrangement, the accredited data recipient is permitted to disclose that CDR data (known as 'service data') to the principal.[50]

---

[44] CDR Rule 7.6(2). This is the case whether the CDR data was used or disclosed by the outsourced service provider, or indirectly used or disclosed through one or more further CDR outsourcing arrangements (CDR Rule 7.6(2)(b)(ii)). See also s 56AU of the Competition and Consumer Act, regarding the application to acts done by or in relation to agents of CDR entities.

[45] An accredited person must also include certain information in its CDR policy about outsourced service providers located overseas (CDR Rule 7.2(4)(d)). See Chapter 1 (Privacy Safeguard 1) for further information.

[46] That is, a consumer experience data standard for the disclosure of CDR data to accredited persons: CDR Rules 7.5A and 8.11(1)(c)(iii).

[47] CDR Rules 7.5(1)(ca) and 7.5(1)(g). Note that while CDR Rule 7.5(1)(ca) refers to a current 'disclosure consent', an AP disclosure consent is a form of 'disclosure consent' and is the relevant category of consent that must be obtained for the purposes of CDR Rule 7.5(1)(ca).

[48] CDR Rule 7.5A.

[49] CDR Rule 1.10A(1)(c)(i). For further information, see Chapter C (Consent).

[50] CDR Rule 7.5(1)(f).

6.58 'Service data' consists of any CDR data that was collected from a CDR participant in accordance with the CDR outsourcing arrangement, or has been directly or indirectly derived from such CDR data.[51]

6.59 The 'principal' refers to the accredited person that engaged the accredited data recipient as an outsourced service provider under a CDR outsourcing arrangement.

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

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

6.61 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.[52]

6.62 For the purposes of Privacy Safeguard 6, an Australian law does not include the APPs under the Privacy Act.[53]

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

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

6.65 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

6.66 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)).

6.67 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.

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

---

[51] CDR Rule 1.10(4).

[52] Section 56EI(1)(c) of the Competition and Consumer Act.

[53] Sections 56EI(1) (Note 3) and 56EC(4)(a) of the Competition and Consumer Act.

6.69 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.

6.70 Privacy Safeguard 7 operates to the exclusion of Privacy Safeguard 6[54] (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.[55]

[54] Section 56E(3) of the Competition and Consumer Act.

[55] See Note 2 of s 56EK and Note 2 of s 56EL of the Competition and Consumer Act.