Chapter 6:

Privacy Safeguard 6 —

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

Version 1.0, February 2020

OAIC

Contents

Key points

- Privacy Safeguard 6, together with consumer data rules (CDR Rules) 7.5 and 7.7, sets out the obligations and restrictions on accredited data recipients in the use and disclosure of Consumer Data Right (CDR) data.
- Generally, accredited data recipients 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 of their CDR data.
- CDR Rule 7.5(1) outlines the permitted uses or disclosures of CDR data.
- CDR Rule 7.5(2) prohibits certain uses or disclosures of CDR data.

What does Privacy Safeguard 6 say?

Accredited data recipients

6.1 An accredited data recipient must not use or disclose CDR data unless the:[1]

- 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 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.

[1] Note: The privacy safeguards apply only to CDR data for which there are one or more CDR consumers (s 56EB(1) of the Competition and Consumer Act). This means that Privacy Safeguard 6 does not prevent an accredited data recipient from using or disclosing CDR data for which there is no CDR consumer.

CDR data will be CDR data for which there is no consumer in circumstances including where the person is not identifiable or 'reasonably identifiable' from the CDR data or other information held by the entity, and where the CDR data does not 'relate to' the person (see Chapter B (Key Concepts)).

Who does Privacy Safeguard 6 apply to?

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

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.[2]

Note: *Currently, there are no designated gateways in the CDR regime responsible for facilitating the transfer of information between data holders and accredited persons (see Chapter B (Key concepts) for the meaning of designated gateway).*

How does Privacy Safeguard 6 interact with the Privacy Act and APP 6?

6.6 It is important to understand how Privacy Safeguard 6 interacts with the Privacy Act and the APPs.[3]

6.7 APP 6 relates to the use or disclosure of personal information. [4]

CDR entity	Privacy protections that apply in the CDR context
Accredited person / accredited data recipient	**Privacy Safeguard 6** Privacy Safeguard 6 applies instead of APP 6 to the use or disclosure of CDR data that has been disclosed to an accredited data recipient under the CDR Rules. APP 6 will continue to apply to the use or disclosure of personal information by an accredited person or accredited data recipient where the data is not CDR data.[5]
Designated gateway	**Privacy Safeguard 6** Privacy Safeguard 6 applies instead of APP 6 to the use and disclosure of CDR data.[6] APP 6 continues to apply to the use and disclosure of personal information that is not CDR data.
Data holder	**APP 6** Privacy Safeguard 6 does not apply to a data holder.

[2] 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.

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

[4] 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.

[5] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

[6] Section 56EC(4)(d) of the Competition and Consumer Act.

Why is it important?

6.8 Consumer consent for uses of their CDR data, including subsequent disclosure, 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.[7]

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.[8]

6.13 An accredited data recipient or designated gateway 'discloses' CDR data when it makes it accessible or visible to others outside the entity.[9] 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).

6.14 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
- publishes the CDR data on the internet, whether intentionally or not
- accidentally provides CDR data to an unintended recipient

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

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

[9] Information will be 'disclosed' under the CDR regime regardless of whether an entity retains effective control over the data. This is different to the situation under the Privacy Act, where in some limited circumstances the provision of information from an entity to a contractor to provide services on behalf of the entity may be a use, rather than a disclosure. See paragraph B.144 in Chapter B: Key concepts of the APP Guidelines.

- 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.

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

6.15 This section outlines when an accredited data recipient may use or disclose CDR data.[10]

6.16 This chapter does not consider when a designated gateway may use or disclose CDR data. This is because there are not currently any designated gateways for the banking sector.

6.17 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.

Permitted uses or disclosures 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 in order 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
- ✓ Using or disclosing CDR data where required or authorised by law

Prohibited uses or disclosures of CDR data

- ✗ Selling CDR data, unless the data has been de-identified in accordance with the CDR Rules
- ✗ Using CDR data to identify, compile insights or build a profile about a person who isn't the consumer, unless this is required to provide the consumer with the requested goods or services and the consumer has consented

[10] 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 6.19 onwards.

Use or disclosure required or authorised under the CDR Rules

6.18 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.[11]

6.19 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 consent from the consumer (other than a direct marketing consent)
- directly or indirectly deriving CDR data from the collected CDR data in accordance with the above use
- disclosing to the consumer any of their CDR data for the purpose of providing the existing goods or services[12]
- 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
- disclosing (by sale or otherwise) to any person, CDR data that has been de-identified in accordance with the CDR data de-identification process.

6.20 CDR Rule 7.5(2) prohibits the following uses or disclosures of CDR data:

- selling the CDR data (unless de-identified in accordance with the CDR data de-identification process), or
- using it 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.

6.21 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.[13]

6.22 The permitted uses and disclosures (in paragraph 6.20) are discussed further in this chapter.

---

[11] 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 Rule 7.7).

[12] 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.

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

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

6.23 An accredited data recipient is authorised to use CDR data in accordance with a current consent from the consumer to provide goods or services requested by the consumer.[14]

6.24 The relevant uses are those uses to which the consumer expressly consented when the consumer provided a valid request for the accredited person to collect their CDR data from a data holder. Valid requests are discussed further in Chapter 3 (Privacy Safeguard 3).

6.25 For information regarding how consents to collect and use CDR data 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, 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 consent, and this use would therefore not be a permitted use under CDR Rule 7.5(1)(a).[15]

Using CDR data in compliance with the data minimisation principle

6.26 An accredited data recipient must comply with the data minimisation principle when using the CDR data to provide goods or services requested by the consumer.[16]

6.27 An accredited data recipient complies with the data minimisation principle if, when providing the requested goods or services, 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.[17]

6.28 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).

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

[15] 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).

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

[17] CDR Rule 1.8(b).

Risk point: An accredited person should pay careful attention to its processes and systems to ensure it complies with the data minimisation principle in all of its 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.

Deriving or indirectly deriving CDR data

6.29 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.[18]

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

6.31 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.[19]

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

Disclosing CDR data to the consumer

6.33 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.[20]

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

6.35 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

6.36 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

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

[19] CDR Rule 4.12(4).

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

- 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.[21]

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).

6.37 The consumer's CDR data includes data collected from the data holder 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.

6.38 Disclosure of a consumer's CDR data by an accredited data recipient to an outsourced service provider for the purpose outlined in paragraph 6.35 is a permitted disclosure under CDR Rule 7.5(1) that does not require the consent of the consumer.[22]

6.39 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,[23] and
- include certain information about outsourced service providers in its CDR policy.[24]

6.40 An outsourced service provider is a person to whom an accredited data recipient discloses[25] CDR data under a CDR outsourcing arrangement.[26]

---

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

[22] However, the accredited data recipient must ensure it has complied with the requirements set out in paragraph 6.40.

[23] CDR Rule 4.11(3)(f). See Chapter 3 (Privacy Safeguard 3).

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

[25] Any provision of CDR data by an accredited data recipient to an outsourced service provider will be a disclosure. Whether an accredited data recipient retains effective control over the data does not affect whether data is 'disclosed'. This is different to the situation under the Privacy Act, where in some limited circumstances the provision of information from an entity to a contractor to provide services on behalf of the entity may be a use, rather than a disclosure. See paragraph B.144 in Chapter B: Key concepts of the APP Guidelines.

[26] CDR Rule 1.10. 'CDR outsourcing arrangement' is discussed in Chapter B (Key Concepts).

6.41 An accredited data recipient who discloses CDR data to a person under a CDR outsourcing arrangement must ensure that the person complies with its requirements under the arrangement.[27]

6.42 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.

6.43 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.

6.44 Where an accredited person has disclosed CDR data to a person under a CDR outsourcing arrangement, any use or disclosure of that data by the person (or their subcontractor) will be taken to have been by the accredited person. This occurs regardless of whether the use or disclosure is in accordance with the arrangement.[28]

6.45 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.[29] See Chapter 8 (Privacy Safeguard 8) for more information.

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

Disclosing de-identified CDR data

6.47 An accredited data recipient is permitted to disclose to any person, by sale or otherwise, CDR data that has been de-identified in accordance with the CDR data de-identification process,[30] which is set out in CDR Rule 1.17.[31]

6.48 However, before de-identifying in accordance with 1.17, the accredited data recipient must have first:

- received consent from the consumer to de-identify some or all of the collected CDR data for the purpose of disclosing (including by selling) the de-identified data,[32] and
- provided the consumer with additional information relating to the de-identification of CDR data.[33]

[27] CDR Rule 1.16.

[28] CDR Rule 7.6(2). This is the case whether the CDR data was disclosed directly to the person by the accredited person, or indirectly through one or more further CDR outsourcing arrangements (CDR Rule 7.6(3)).

[29] 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.

[30] CDR Rule 7.5(1)(e).

[31] The CDR data de-identification process is set out in CDR Rule 1.17. If the CDR data cannot be de-identified to the 'required extent', the accredited data recipient must not disclose the CDR data to any person for this purpose, whether by sale or otherwise. For information regarding the CDR data de-identification process, see Chapter 12 (Privacy Safeguard 12). Chapter 12 (Privacy Safeguard 12) also provides guidance on the requirement for an accredited data recipient to destroy or de-identify redundant CDR data.

[32] CDR Rule 4.11(3)(e).

[33] CDR Rule 4.15.

6.49 An accredited data recipient must ensure it complies with the CDR data de-identification process when de-identifying CDR data.[34] De-identification is discussed further in Chapter 12 (Privacy Safeguard 12).

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

6.50 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.[35]

6.51 For the purposes of Privacy Safeguard 6, an Australian law does not include the APPs under the Privacy Act.[36]

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

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

6.54 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

6.55 The restrictions on using or disclosing CDR data in Privacy Safeguard 6 are additional to Privacy Safeguard 7 (see Chapter 7 (Privacy Safeguard 7)) and Privacy Safeguard 8 (see Chapter 8 (Privacy Safeguard 8)).

6.56 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.

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

6.58 Privacy Safeguard 7 operates to the exclusion of Privacy Safeguard 6[37] (which means that direct marketing uses or disclosures cannot be authorised under Privacy Safeguard 6), while Privacy Safeguard 8 operates as a restriction in addition to Privacy Safeguard 6.[38]

---

[34] CDR Rule 1.17.

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

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

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

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