Chapter 6:

Privacy Safeguard 6 —

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

Consultation draft, October 2019

OAIC

Contents

Key points

- Privacy Safeguard 6, together with 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 only use or disclose CDR data where required or authorised under the Consumer Data Rules. In most cases, the consumer is required to expressly consent to these uses of their CDR data.
- Consumer Data Rule 7.5 outlines the permitted uses or disclosures of CDR data.
- Consumer Data Rule 4.12(3) also 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:

- disclosure is required under the Consumer Data Rules in response to a valid request from a CDR consumer for the CDR data, or
- use or disclosure is otherwise required or authorised under the Consumer Data 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 Consumer Data Rules 7.5 and 4.12(3).

Designated gateways

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

- disclosure is required under the Consumer Data Rules, or
- use or disclosure is authorised under the Consumer Data 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 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.

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 1988 (the Privacy Act) and Australian Privacy Principles (APPs).[1]

6.7 Like Privacy Safeguard 6, APP 6 relates to the use or disclosure of personal information.[2]

Summary of application of Privacy Safeguard 6 by CDR entity

CDR entity	Privacy principle that applies to CDR data
Accredited person	**Australian Privacy Principle 6** Privacy Safeguard 6 does not apply to an accredited person who is not an accredited data recipient of the relevant CDR data.
Accredited data recipient	**Privacy Safeguard 6** Privacy Safeguard 6 applies instead of APP 6,[3] meaning APP 6 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime. APP 6 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data.[4]
Designated gateway	**Privacy Safeguard 6** Privacy Safeguard 6 applies instead of APP 6, meaning APP 6 will not apply to CDR data that has been received by a designated gateway through the CDR regime. APP 6 will continue to apply to the designated gateway where they are handling personal information in their capacity as an APP entity.
Data holder	**Australian Privacy Principle 6** Privacy Safeguard 6 does not apply to a data holder.

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

[2] 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.

[3] 56EC(4)(a). Section 56EC(4) provides that the APPs do not apply to an accredited data recipient of CDR data in relation to the CDR data. An accredited person who holds CDR data that was disclosed to the person under the Consumer Data Rules falls within the definition of 'accredited data recipient' for that data (unless they are a data holder or designated gateway for the data) (see s 56AK).

[4] All accredited data recipients are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. This means that non-CDR personal information handling by accredited data recipients is covered by the Privacy Act and the APPs, while the handling of CDR data is covered by the CDR regime and the Privacy Safeguards. See s 6E(1D) of the Privacy 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 going to be given 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.[5]

6.11 An accredited data recipient or designated gateway 'uses' CDR data where it handles or undertakes an activity with the CDR data, within the entity's 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
- 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.[6]

6.13 An accredited data recipient or designated gateway 'discloses' CDR data where it makes it accessible to others outside the entity and releases the subsequent handling of the information from its effective control. This focuses on the act done by the disclosing party. The state of mind or intentions of the recipient does not affect the act of disclosure.

6.14 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).

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

- shares the CDR data with another entity or individual
- discloses CDR data to themselves, but in their capacity as a different entity
- 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
- displays a computer screen so that the CDR data can be read by another entity or individual.

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

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

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.[7]

6.17 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.

Use or disclosure required or authorised under the Consumer Data 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 Consumer Data Rules.[8]

6.19 Consumer Data Rule 7.5 authorises the following permitted uses or disclosures of CDR data[9]:

- 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 CDR consumer
- directly or indirectly deriving CDR data from the collected CDR data for the above purpose
- disclosing to the CDR consumer any of their CDR data
- disclosing the CDR consumer's CDR data to an outsourced service provider:
  - for the purpose of doing the things referred to the above three dot points, 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 However, an accredited data recipient must not ask a CDR consumer to give consent to use or disclose their CDR data for the following prohibited uses or disclosures:

- 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 CDR consumer who made the

[7] 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 Consumer Data Rules in response to a valid request from a CDR consumer for the CDR data (56EI(1)(a)). The Consumer Data 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 Consumer Data Rules or under an Australian law or a court/tribunal order. These circumstances are outlined in this chapter from paragraph 6.18 onwards.

[8] Section 56EI(1)(b). The use or disclosure of CDR data is not currently required under the Consumer Data Rules. The use or disclosure of CDR data is authorised under the Consumer Data Rules if it is a 'permitted use or disclosure' under Consumer Data Rule 7.5 that does not relate to direct marketing (Consumer Data Rule 7.7).

consumer data request (including through aggregating the CDR data), unless the accredited data recipient is seeking consent to:

- derive, from that CDR data, CDR data about that person's interactions with the CDR consumer, and
- use that derived CDR data in order to provide the requested goods or services.[10]

Example

MinYin is a money transfer app allowing friends to split bills and request payments without the need to log-in to banking apps. Elizabeth wishes to try out MinYin's service via a CDR transfer.

When seeking Elizabeth's consent to the CDR transfer, MinYin also asks for consent to analyse Elizabeth's frequent payees to identify those who use the app. MinYin tells Elizabeth that it needs this information to be able to send and receive payment requests from those friends.

MinYin has followed the requirements in rule 4.12(3), as MinYin used Elizabeth's CDR data to identify persons who are not Elizabeth for a permitted purpose. The permitted purpose here is to derive data about Elizabeth's interactions with that person in order to deliver the service to Elizabeth.

MinYin changes its CDR consent process to also ask for consent to attempt to identify demographic information about those payees. MinYin intends to analyse data on Elizabeth's payees to build a profile of her social circle. It will then sell this information.

MinYin has now sought consent for a prohibited use of CDR data, breaching the requirement in rule 4.12(3). This is because MinYin used Elizabeth's CDR data to identify persons who are not Elizabeth for a prohibited purpose. The prohibited purpose here is to build a 'silent profile' on Elizabeth's social circle for a purpose other than providing Elizabeth's service to her.

6.21 The above permitted uses and disclosures (in paragraph 6.19) are discussed further below.

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

6.22 An accredited data recipient is authorised to use CDR data in accordance with a current consent from the CDR consumer to provide goods or services requested by the CDR consumer.[11]

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

6.24 For information regarding how consents to collect and use CDR data must be managed, see Chapter C (Consent).

[10] Consumer Data Rule 4.12(3).

[11] Consumer Data Rule 7.5(1)(a).

Example

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

SpendLess notices that Oliver has similar spending habits to several of its other consumers who are of a similar demographic background. SpendLess runs Oliver's transaction data through an algorithm with the other consumers' transaction data to analyse trends and provide predictive and bigger picture budgeting recommendations to Oliver.

When providing his valid request to SpendLess, Oliver consented to the analysis of his transaction data for the purpose of providing him with tailored budgeting tips. He did not consent to his transaction data being used to allow SpendLess to compile broader insights in conjunction with other datasets.

SpendLess has not used Oliver's CDR data in accordance with his consent and is therefore in breach of Consumer Data Rule 7.5(1)(a). Assuming the other consumers provided valid requests on the same terms as Oliver, SpendLess is also in breach of Consumer Data Rule 7.5(1)(a) in relation to the other consumers whose transaction data was combined with Oliver's.

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 the CDR data to provide goods or services requested by the CDR consumer.[12]

6.26 The data minimisation principle provides that the accredited data recipient must 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 CDR consumer.[13]

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 data recipient should pay careful consideration to its processes and systems to ensure it is compliant with the data minimisation principle in all of its uses of CDR data. This includes a separate consideration of the minimum CDR data required to provide each good or service (including each upgraded good or service) to a CDR consumer.

Privacy tip: An accredited data recipient should set up its systems and processes so that it can identify minimum required CDR data for a particular good or service. This reduces variance and ensures prompt and compliant responses to CDR consumers' requests for CDR data, and ensures these responses do not exceed the limitations imposed by the data minimisation principle.

Deriving or indirectly deriving CDR data

6.28 An accredited data recipient is permitted to directly or indirectly derive CDR data from the collected CDR data for the purpose of providing goods or services requested by the

[12] Consumer Data Rule 7.5(1)(a).

[13] Consumer Data Rule 1.8(b).

consumer.[14] The accredited data recipient is not required to obtain the consumer's consent to do so.

6.29 However, where an accredited data recipient:

- 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.[15]

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

Disclosing CDR data to the consumer

6.31 An accredited data recipient is permitted to disclose to a CDR consumer any of their CDR data.[16]

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

6.33 This is a permitted disclosure and does not require the consent of the CDR consumer.[17]

Disclosing CDR data to an outsourced service provider

6.34 An accredited data recipient is permitted to disclose the CDR consumer's CDR data to an outsourced service provider for the purpose of:

- using the CDR consumer's CDR data to provide goods or services requested by the CDR consumer, including by directly or indirectly deriving CDR data from the CDR data, and
- disclosing, to the CDR consumer, any of their CDR data

to the extent reasonably needed to fulfil those purposes.[18]

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 categories so that SpendLess can provide tailored budgeting advice to consumers.

SpendLess discloses Oliver's account and transaction data to KnowYourMoney. However, KnowYourMoney only needs Oliver's transaction data for this purpose. KnowYourMoney does not need to analyse Oliver's account data in order to report upon Oliver's spending trends.

[14] Consumer Data Rule 7.5(1)(b).

[15] Consumer Data Rule 4.12(4).

[16] Consumer Data Rule 7.5(1)(c).

[17] Consumer Data Rules 7.5(1)(c) and 4.11.

[18] Consumer Data Rule 7.5(1)(d).

In doing so, SpendLess Pty Ltd has disclosed Oliver's CDR data to an outsourced service provider beyond the extent reasonably needed to fulfil the purpose of providing the service requested by Oliver. SpendLess Pty Ltd will be in breach of rule 7.5(1)(d).

6.35 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.

6.36 Disclosure of a CDR consumer's CDR data by an accredited data recipient to an outsourced service provider for the purpose outlined in paragraph 6.34 is a permitted disclosure and does not require the consent of the CDR consumer.

6.37 However, where an accredited data recipient intends to disclose CDR data of a CDR consumer to an outsourced service provider, the accredited data recipient must:

- provide certain information to the CDR consumer at the time of seeking the CDR consumer's consent to collect and use the CDR consumer's CDR data,[19] and
- include certain information about outsourced service providers in its CDR policy.[20]

6.38 An outsourced service provider is a person to whom an accredited data recipient discloses CDR data under a CDR outsourcing arrangement.[21]

6.39 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.

6.40 In order to meet this requirement, the accredited data recipient must ensure that the relevant CDR outsourcing arrangement requires the outsourced service provider to adhere to the accredited data recipient's Privacy Safeguard obligations.

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

6.42 Where an accredited data recipient 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 data recipient. This occurs regardless of whether the use or disclosure is in accordance with the arrangement.[22]

6.43 For further information, see Chapter B Key Concepts 'Outsourced service providers'.

Disclosing de-identified CDR data

6.44 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.[23]

---

[19] Consumer Data Rule 4.11(3)(f). See Chapter 3 (Privacy Safeguard 3).

[20] Consumer Data Rule 7.2(4). See Chapter 1 (Privacy Safeguard 1).

[21] Consumer Data Rule 1.10. A CDR outsourcing arrangement exists when an accredited data recipient discloses CDR data to another person if it does so under a written contract between the parties.

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

[23] Consumer Data Rule 7.5(1)(e).

6.45 In order to do so, however, the accredited data recipient must have first:

- received consent from the CDR consumer to de-identify some or all of the collected CDR data for the purpose of disclosing (including by selling) the de-identified data;[24] and
- provided the CDR consumer with additional information relating to the de-identification of CDR data.[25]

6.46 An accredited data recipient must ensure it complies with the CDR data de-identification process when de-identifying CDR data.[26] De-identification is discussed further in Chapter 12.

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

6.47 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.[27]

6.48 For the purposes of Privacy Safeguard 6, an Australian law does not include the APPs under the Privacy Act.[28]

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

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

6.51 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
- to whom the CDR data has been disclosed, if applicable.

[24] Consumer Data Rule 4.11(3)(e).

[25] Consumer Data Rule 4.15.

[26] Consumer Data Rule 1.17.

[27] Section 56EI(1)(c).

[28] Sections 56EI(1) (Note 3) and 56EC(4)(a).