Chapter 3:

Privacy Safeguard 3 —

Seeking to collect CDR data from CDR participants

Version 3.0, June 2021

OAIC

Contents

Key points 3
What does Privacy Safeguard 3 say? 3
Why is it important? 4
Who does Privacy Safeguard 3 apply to? 4
How Privacy Safeguard 3 interacts with the Privacy Act 4
What is meant by 'seeking to collect' CDR data? 5
When can an accredited person seek to collect CDR data? 5
What is a 'valid request?' 5
Process for asking for consent 6
Consumer data request 7
Data minimisation principle 8
Can an accredited person engage a third party to seek to collect CDR data on their behalf? 8
Interaction with other privacy safeguards 11

Key points

- Privacy Safeguard 3 prohibits an accredited person from attempting to collect data under the consumer data right (CDR) regime unless it is in response to a 'valid request' from the consumer.
- The consumer data rules (CDR Rules) set out what constitutes a valid request, including requirements and processes for seeking the consumer's consent.
- The accredited person must also comply with all other requirements in the CDR Rules for collection of CDR data. This includes the 'data minimisation principle', which requires that an accredited person must not seek to collect data beyond what is reasonably needed to provide the good or service to which a consumer has consented, or for a longer time period than is reasonably needed.

What does Privacy Safeguard 3 say?

3.1 An accredited person must not seek to collect CDR data from a CDR participant (i.e. a data holder or an accredited data recipient) unless:

- the consumer has requested the accredited person's good or service and provided a valid request under the CDR Rules, and
- the accredited person complies with all other requirements in the CDR Rules for the collection of CDR data from the CDR participant.[1]

3.2 Under the CDR Rules:

- the valid request must meet specific requirements, including compliance with the CDR Rules regarding consent,[2] and
- accredited persons must have regard to the data minimisation principle,[3] which limits the scope of a consumer data request that an accredited person may make on behalf of a consumer.

3.3 The requirement in Privacy Safeguard 3 applies where an accredited person seeks to collect CDR data directly from a CDR participant, or via a designated gateway.[4] Privacy Safeguard 3 will also apply to an accredited person where they engage an accredited outsourced service provider to seek to collect CDR data on their behalf.[5]

[1] Section 56EF of the Competition and Consumer Act.

[2] CDR Rule 4.3.

[3] CDR Rule 4.12(2).

[4] Section 56EF(2) of the Competition and Consumer Act.

[5] The CDR Rules requirements for engaging an accredited outsourced service provider to collect data on an accredited person's behalf are outlined in paragraphs 3.30 – 3.35.

Why is it important?

3.4 The CDR regime is driven by consumers. Consumer consent for the collection of their CDR data is at the heart of the CDR regime.

3.5 By adhering to Privacy Safeguard 3, an accredited person will ensure consumers have control over what CDR data is collected, and for what purposes and time-period. This will assist in enhancing consumer trust, as well as minimise the possibility of over-collection.

Who does Privacy Safeguard 3 apply to?

3.6 Privacy Safeguard 3 applies to accredited persons.

3.7 Privacy Safeguard 3 does not apply to data holders and designated gateways. These entities must continue to ensure that they are adhering to their obligations under the *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles (APPs), including APP 3 and APP 5, when collecting personal information.

How Privacy Safeguard 3 interacts with the Privacy Act

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

3.9 APP 3 outlines when an entity may collect solicited personal information (See Chapter 3: APP 3 – Collection of solicited personal information of the APP Guidelines).

CDR entity	Privacy protections that apply in the CDR context
Accredited person	**Privacy Safeguard 3** When an accredited person is seeking to collect CDR data under the CDR Rules, Privacy Safeguard 3 applies. APP 3 does not apply to the accredited person in relation to that CDR data.[7]
Designated gateway	**APP 3** Privacy Safeguard 3 does not apply to a designated gateway.

[6] The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities). See also Chapter B: Key concepts of the APP Guidelines.

[7] See ss 56EC(4) and 56EF the Competition and Consumer Act.

Note: If Privacy Safeguard 3 does not apply, APP 3 may continue to apply to other collections of the individual's personal information where the accredited person is an APP entity (see s 56EC(4) and (5)(aa) of the Competition and Consumer Act). 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.

CDR entity	Privacy protections that apply in the CDR context
Data holder	**APP 3** Privacy Safeguard 3 does not apply to a data holder.

What is meant by 'seeking to collect' CDR data?

3.10 Privacy Safeguard 3 applies when an accredited person 'seeks to collect CDR data' (before the CDR data is actually collected).

3.11 'Seeking to collect' CDR data refers to any act of soliciting CDR data, which includes explicitly requesting another entity to provide CDR data, or taking active steps to collect CDR data.

3.12 The main way in which an accredited person will 'seek to collect' CDR data under the CDR Rules is by making a 'consumer data request' to a CDR participant on behalf of the consumer. Consumer data requests are explained at paragraphs 3.22–3.26. The point at which an accredited person makes a consumer data request is demonstrated by the flow chart on page 10 of this Chapter.

3.13 The term 'collect' is discussed in detail in Chapter B (Key concepts). An accredited person 'collects' information if they collect the information for inclusion in a 'record' or a 'generally available publication'.[8] 'Record'[9] and 'generally available publication'[10] have the same meaning as within the Privacy Act.

When can an accredited person seek to collect CDR data?

3.14 An accredited person must not seek to collect CDR data from a CDR participant unless it is in response to a valid request from a consumer, and the accredited person complies with all other requirements in the CDR Rules for the collection of CDR data.

What is a 'valid request?'

3.15 Under CDR Rule 4.3, a consumer gives an accredited person a 'valid' request to seek to collect their CDR data from a CDR participant if:

[8] Section 4(1) of the Competition and Consumer Act.

[9] Section 6(1) of the Privacy Act: 'record' includes a document or an electronic (or other) device. Some items are excluded from the definition, such as anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition, and Commonwealth records in the open access period. [10] Section 6(1) of the Privacy Act: 'generally available publication' means a 'magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public', regardless of the form in which it is published and whether it is available on payment of a fee.

[10] Section 6(1) of the Privacy Act: 'generally available publication' means a 'magazine, book, article, newspaper or other publication that is, or will be, generally available to members of the public', regardless of the form in which it is published and whether it is available on payment of a fee.

- the request is for the accredited person to provide goods or services
- the accredited person needs to collect the consumer's CDR data from a CDR participant and use it in order to provide the requested goods or services
- the accredited person asks the consumer for a collection consent and a use consent,[11] in accordance with Division 4.3 of the CDR Rules (see paragraphs 3.18–3.21 for further information), and
- the consumer expressly consents to this collection and use of their CDR data.

3.16 A request ceases to be 'valid' if the consumer withdraws their collection consent.[12]

3.17 Entities should also be mindful that the Competition and Consumer Act prohibits persons from engaging in conduct that misleads or deceives another person into believing certain matters, including that the person is making a valid request or has given their consent.[13]

Process for asking for consent

3.18 Division 4.3 of the CDR Rules outlines the requirements for consent for the purposes of making a valid request for the collection and use of CDR data.

3.19 Specifically, the CDR Rules provide the following processes and requirements must be met to ensure that consent is voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn:

- **Processes for asking for consent** (CDR Rule 4.10): to ensure that the consent is as easy to understand as practicable.
- **Requirements when asking for consent** (CDR Rules 4.11, 4.16 and 4.17): including to allow the consumer to actively select the types and uses of data to which they provide consent, and provide express consent for the accredited person to collect and use the selected data for those specified purposes. Additional requirements apply where the accredited person is seeking consent to de-identify CDR data (CDR Rule 4.15).
- **Restrictions on seeking consent** (CDR Rule 4.12): including that an accredited person cannot seek to collect or use CDR data for a period exceeding 12 months.
- Obligations about **managing the withdrawal of consent** (CDR Rule 4.13): including that a consumer may withdraw the consent at any time through their consumer dashboard or by using a simple alternative method made available by the accredited person.

---

[11] The consumer must provide a collection consent for the accredited person to collect their data from a CDR participant and a use consent for the accredited person to use that CDR data. See Chapter C (Consent) for further information.

[12] CDR Rule 4.3(4). If the consumer does not also withdraw their use consent, the accredited person may continue to use the CDR data it has already collected to provide the requested goods or services. See the note under CDR Rule 4.3(4). See further Rule 4.18A for ongoing notification requirements in this circumstance.

If the consumer also withdraws their use consent, the CDR data is likely to become redundant data that the accredited person is required to delete or de-identify in accordance with Privacy Safeguard 12 (unless an exception applies). More information on 'redundant data' and the requirement to destroy or de-identify redundant data is in Chapter 12 (Privacy Safeguard 12).

[13] Sections 56BN and 56BO of the Competition and Consumer Act.

- Time of **expiry of consent** (CDR Rule 4.14): consent generally expires upon withdrawal of consent or at the end of the specified period in which the consumer gave consent for the accredited person to collect the CDR data (which cannot be longer than 12 months).

3.20 The accredited person is also required to have regard to the Consumer Experience Guidelines[14] when asking a consumer to give consent.

3.21 These specific requirements and processes for the above CDR Rule requirements are explained in Chapter C (Consent).

Consumer data request

3.22 If a consumer has given an accredited person a valid request (see paragraph 3.15 above), and the consumer's consent for the accredited person to collect and use their CDR data is current,[15] the accredited person may request the relevant CDR participant to disclose some or all of the CDR data that:

- is the subject of the relevant collection consent and use consent, and
- it is able to collect and use in compliance with the data minimisation principle.[16]

3.23 In doing so, the accredited person makes a 'consumer data request' to a CDR participant on behalf of the consumer.[17] The accredited person may make consumer data requests to more than one CDR participant where the relevant CDR data required to provide the requested goods or services is held by different CDR participants. The accredited person may also need to make repeated consumer data requests over a period of time in order to provide the requested goods or services.

3.24 When the accredited person makes a consumer data request on behalf of a consumer, they must not seek to collect more CDR data than is reasonably needed, or for a longer time period than reasonably needed, in order to provide the requested goods or services.[18]

3.25 When an accredited person makes a consumer data request to a data holder, they must make the request:

- using the data holder's accredited person request service, and
- in accordance with the data standards.[19]

3.26 An accredited person complies with Privacy Safeguard 3 after giving the relevant CDR participant/s a consumer data request in the manner set out above at paragraph 3.25.[20]

---

[14] CDR Rule 4.10(1)(a)(ii). The Consumer Experience Guidelines provide best practice interpretations of the CDR Rules relating to consent and are discussed in Chapter B (Key concepts).

[15] See paragraph 3.15 above.

[16] CDR Rules 4.4(1) and 4.7A(1).

[17] CDR Rules 4.4(2) and 4.7A(2).

[18] CDR Rules 1.8(a), 4.4(1)(d) and 4.7A(1)(d).

[19] CDR Rule 4.4(3).

[20] The effect of CDR Rules 4.4(2) and 4.7A(2) is that a request for CDR data from an accredited person on behalf of a consumer that does not comply with CDR Rule 4.4(1) or CDR Rule 4.7A(1) is not a 'consumer data request'.

Data minimisation principle

3.27 Collection of CDR data is limited by the data minimisation principle,[21] which requires that an accredited person:

- must not collect more data than is reasonably needed in order to provide the requested goods or services or for a time period longer than what is reasonably needed, and
- may only use the collected data consistently with the consent provided, and only as reasonably needed in order to provide the requested goods or services or to fulfill any other purpose as consented to by the consumer.

3.28 The data minimisation principle is relevant both when an accredited person seeks consent from the consumer to collect their CDR data, and then when the accredited person gives a CDR participant a consumer data request.

3.29 The data minimisation principle is discussed further in Chapter B (Key concepts).

Example

MiddleMan Ltd, an accredited person, makes a consumer data request on behalf of a consumer, Athena, to seek information about Athena's eligibility to open a bank account.

MiddleMan has asked Athena for her consent to collect information about her transaction history from the data holder (in addition to other data), when this information would not be required to determine her eligibility for the service.

MiddleMan will likely be in breach of Privacy Safeguard 3 as it has sought to collect CDR data beyond what is reasonably needed to provide the requested service (as required by the data minimisation principle) and therefore has not sought to collect Athena's CDR data from a CDR participant in accordance with the CDR Rules.

Can an accredited person engage a third party to seek to collect CDR data on their behalf?

3.30 An accredited person may engage another accredited person to seek to collect CDR data on their behalf, in accordance with the CDR Rules.[22] This is currently the only type of third party that can be engaged for this purpose under the CDR Rules.

3.31 CDR Rule 1.10 requires the accredited person (the 'principal') to have a CDR outsourcing arrangement with the other accredited person (the 'outsourced service provider', or

[21] CDR Rule 4.12(2). There are no equivalent requirements for how an accredited person makes a consumer data request to an accredited data recipient.

[22] CDR Rule 1.10(2)(a)(i).

'provider'). A CDR outsourcing arrangement is a written contract between the principal and provider which meets the requirements set out in CDR Rule 1.10(2).[23]

3.32 Where an accredited person intends to use an accredited provider to seek to collect a consumer's CDR data, 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,[24] and
- include certain information about outsourced service providers in its CDR policy.[25]

3.33 The accredited person must ensure the accredited provider complies with its requirements under the CDR outsourcing arrangement.[26]

3.34 The CDR data collected by an accredited provider in accordance with 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.[27]

3.35 Any use or disclosure of such service data by the accredited provider will be taken to have been by the accredited person. This occurs regardless of whether the use or disclosure is in accordance with the CDR outsourcing arrangement.[28]

Risk point: Entities that fail to take prudent and robust measures in their CDR outsourcing arrangements risk non-compliance by their third parties.

Privacy tip: To ensure the third party complies with the outsourcing arrangement, the accredited person should ensure that:

- the relevant CDR outsourcing arrangement requires the third party to adhere to the accredited person's privacy safeguard obligations, and
- the contract provides an appropriate level of transparency to allow them to monitor the third party where relevant, and audit the CDR outsourcing arrangement.

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

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

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

[26] CDR Rule 1.16(1). The requirements for a CDR outsourcing arrangement are set out in CDR Rule 1.10(2).

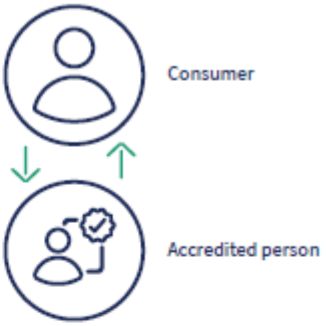
[27] CDR Rule 1.10(4).

[28] CDR Rule 7.6(2).

Consent and collection process for accredited persons

Obtaining consumer consent for the collection and use of CDR data

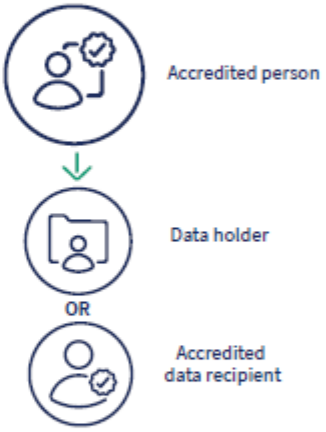
- Accredited person offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- Accredited person asks the consumer to consent to the collection and use of their CDR data for this purpose, for up to 12 months
- Consumer provides their express consent to the collection and use of their CDR data



The consumer has given the accredited person a valid request ✓

Making a consumer data request on behalf of the consumer

- Consumer gives accredited person a valid request
- Accredited person asks the CDR participant [1] to disclose the consumer's CDR data
- Where the request is to a data holder, the accredited person makes the request using the data holder's 'accredited person request service', and in accordance with the data standards [2]



CDR participant sends the consumer's CDR data to the accredited person after obtaining:

- the consumer's authorisation (in the case of a data holder)
- the consumer's AP disclosure consent (in the case of an accredited data recipient)

The accredited person becomes an accredited data recipient for the consumer's CDR data.

[1] This may be a data holder or accredited data recipient

[2] Note: there are no equivalent requirements for how an accredited person must make a request to another accredited data recipient

Interaction with other privacy safeguards

Privacy Safeguard 4

3.36 The privacy safeguards distinguish between an accredited person collecting solicited CDR data (Privacy Safeguard 3) and unsolicited CDR data (Privacy Safeguard 4).

3.37 Privacy Safeguard 4 requires an accredited person to destroy unsolicited CDR data collected from a data holder, unless an exception applies (see Chapter 4 (Privacy Safeguard 4)).

3.38 Where an accredited person seeks to collect data in accordance with Privacy Safeguard 3 but additional data that is not requested is nonetheless disclosed by the data holder, Privacy Safeguard 4 applies to that additional data.

Privacy Safeguard 5

3.39 Privacy Safeguard 5 requires an accredited data recipient who collected data in accordance with Privacy Safeguard 3 to notify the consumer of the collection in accordance with the CDR Rules (see Chapter 5 (Privacy Safeguard 5)).