

Chapter 3:

Privacy Safeguard 3 —

Seeking to collect CDR data from CDR participants

Version 1.0, February 2020

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 does Privacy Safeguard 3 interact 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	6
Data minimisation principle	7
Interaction with other privacy safeguards	10

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 that relates to 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:¹
- 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.²
- 3.2 Under the CDR Rules:
- the valid request must meet specific requirements, including compliance with the CDR Rules regarding consent,³ and
 - accredited persons must have regard to the data minimisation principle,⁴ 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.⁵

Note: *An accredited person can currently collect CDR data only from a data holder. An accredited person is not currently authorised under the CDR Rules to collect CDR data from an accredited data recipient.*

¹ Note: The privacy safeguards only apply to CDR data for which there are one or more CDR consumers (section 56EB(1) of the Competition and Consumer Act). This means that Privacy Safeguard 3 does not prevent an accredited person from seeking to collect CDR data for which there is no CDR consumer from a CDR participant.

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 where the CDR data does not 'relate to' the person ([see Chapter B \(Key Concepts\)](#)).

² Section 56EF of the Competition and Consumer Act.

³ CDR Rule 4.3.

⁴ CDR Rule 4.12(2).

⁵ Section 56EF(2) of the Competition and Consumer Act.

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 does Privacy Safeguard 3 interact 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 / accredited data recipient	<p>Privacy Safeguard 3 and APP 3</p> <p>Privacy Safeguard 3 applies to accredited persons from the point when they seek to collect CDR data.</p> <p>APP 3 will continue to apply to personal information collected that is not CDR data.⁷</p>
Designated gateway	<p>APP 3</p> <p>Privacy Safeguard 3 does not apply to a designated gateway.</p>
Data holder	<p>APP 3</p> <p>Privacy Safeguard 3 does not apply to a data holder.</p>

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 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.

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 means 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 data holder 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 9 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.
- 3.15 An accredited person is currently only authorised to seek to collect CDR data from a data holder.

What is a ‘valid request?’

- 3.16 Under CDR Rule 4.3, a consumer gives an accredited person a ‘valid’ request to seek to collect their CDR data from a data holder if:
- the request is for the accredited person to provide goods or services
 - the accredited person needs the consumer’s CDR data¹¹ to provide the requested goods or services
 - the accredited person asks for the consumer’s consent to the collection of their CDR data, in accordance with Subdivision 4.3.2 of the CDR Rules (see paragraphs 3.18–3.21 for further information), and

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.

¹¹ Note that the data may be required consumer data or voluntary consumer data for these purposes.

- the consumer expressly consents to this collection of their CDR data.

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 that the person is a consumer for CDR data, is making a valid request or has satisfied other criteria for the disclosure of CDR data.¹²

Process for asking for consent

3.18 Subdivision 4.3.2 of the CDR Rules outlines the requirements for consent for the purposes of making a valid request for collection 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 select or specify the types of data to which they provide consent and provide express consent for the accredited person to collect the selected data. 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 by communicating it in writing to the accredited person or by using the consumer dashboard.
- 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 Guidelines¹³ 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 3.16 above), and the consumer's consent for the accredited person to collect and use their CDR data is current,¹⁴ the accredited person may request the relevant data holder to disclose some or all of the CDR data that:

¹² Sections 56BN and 56BO of the Competition and Consumer Act.

¹³ CDR Rule 4.10(a)(ii). The Consumer Experience Guidelines provide best practice interpretations of the CDR Rules relating to consent and are discussed in [Chapter B \(Key concepts\)](#).

¹⁴ 'Current consent' is discussed in [Chapter B \(Key concepts\)](#).

- is the subject of the relevant consent to collect and use CDR data, and
 - it is able to collect and use in compliance with the data minimisation principle.¹⁵
- 3.23 In doing so, the accredited person makes a ‘consumer data request’ to a data holder on behalf of the consumer.¹⁶ The accredited person may make consumer data requests to more than one data holder where the relevant CDR data required to provide the requested goods or services is held by different data holders. 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 that relates to a longer time period than reasonably needed, in order to provide the requested goods or services.¹⁷
- 3.25 The accredited person must make the consumer data request:
- using the data holder’s accredited person request service, and
 - in accordance with the data standards.¹⁸
- 3.26 An accredited person complies with Privacy Safeguard 3 after giving a data holder a consumer data request in the manner set out above.¹⁹

Data minimisation principle

- 3.27 Collection of CDR data is limited by the data minimisation principle,²⁰ which requires that an accredited person:
- must not collect more data than is reasonably needed in order to provide the requested goods or services, 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.
- 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 data holder a consumer data request.
- 3.29 The data minimisation principle is discussed further in [Chapter B \(Key concepts\)](#).

¹⁵ CDR Rule 4.4(1).

¹⁶ CDR Rule 4.4(2).

¹⁷ CDR Rules 1.8(a) and 4.4(1)(d).

¹⁸ CDR Rule 4.4(3).

¹⁹ The effect of CDR Rule 4.4(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) is not a ‘consumer data request’.

²⁰ CDR Rule 4.12(2).

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 sought to collect Athena's CDR data from a data holder otherwise than in accordance with the CDR Rules.

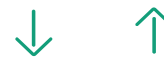
Consent and collection process for accredited persons

Obtaining consumer consent for the collection and use of CDR data

- Accredited person offers a good or service which requires CDR data
- Consumer wants 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



Consumer



Accredited person

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 data holder to disclose the consumer's CDR data
- Accredited person requests the data using the data holder's 'accredited person request service'



Accredited person



Data holder

Data holder sends the consumer's CDR data to the accredited person, after obtaining consumer authorisation to do so



Data holder



Accredited person



Accredited data recipient

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

Interaction with other privacy safeguards

Privacy Safeguard 4

- 3.30 The privacy safeguards distinguish between an accredited person collecting solicited CDR data ([Privacy Safeguard 3](#)) and unsolicited CDR data ([Privacy Safeguard 4](#)).
- 3.31 Privacy Safeguard 4 requires an accredited person to destroy unsolicited CDR data collected from a data holder, unless an exception applies ([see Chapter 4 \(Privacy Safeguard 4\)](#)).
- 3.32 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

- 3.33 Privacy Safeguard 5 requires an accredited person who has collected data in accordance with Privacy Safeguard 3 to notify the consumer of the collection in accordance with the CDR Rules ([see Chapter 5 \(Privacy Safeguard 5\)](#)).