

## Chapter 3:

# Privacy Safeguard 3 —

## Seeking to collect CDR data from CDR participants

Consultation draft, October 2019

# Contents

<b>Key points</b>	<b>3</b>
<b>What does Privacy Safeguard 3 say?</b>	<b>3</b>
<b>Why is it important?</b>	<b>3</b>
<b>Who does Privacy Safeguard 3 apply to?</b>	<b>4</b>
<b>How does Privacy Safeguard 3 interact with the Privacy Act?</b>	<b>4</b>
Summary of application of Privacy Safeguard 3 by CDR participant	4
<b>What is meant by ‘seeking to collect’ CDR data?</b>	<b>5</b>
<b>When can an accredited person seek to collect CDR data?</b>	<b>5</b>
What is a ‘valid request?’	6
Process for asking for consent	6
Consumer data request	7
Data minimisation principle	7
<b>Interaction with other Privacy Safeguards</b>	<b>10</b>
Privacy Safeguard 4	10
Privacy Safeguard 5	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 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 Consumer Data Rules for collection of CDR data. This includes the ‘data minimisation principle’, where 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 required.

## 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 CDR consumer has requested the accredited person’s good or service and provided a valid request under the Consumer Data Rules, and
  - the accredited person complies with all other requirements in the Consumer Data Rules for the collection of CDR data from the CDR participant.<sup>1</sup>
- 3.2 Under the Consumer Data Rules:
- the valid request must meet specific requirements, including compliance with the Consumer Data Rules regarding consent, and
  - accredited persons must have regard to the data minimisation principle, which limits the scope of a consumer data request that an accredited person may make on behalf of a CDR 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.<sup>2</sup>

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

## 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.

---

<sup>1</sup> 56EF.

<sup>2</sup> 56EF(2).

- 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. It does not apply to data holders or designated gateways.
- 3.7 See [Chapter B \(Key Concepts\)](#) for the meaning of accredited persons.

## 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.<sup>3</sup>
- 3.9 Like Privacy Safeguard 3, 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](#)).

## Summary of application of Privacy Safeguard 3 by CDR participant

CDR entity	Privacy principle that applies
<b>Accredited person</b>	<p><b>Privacy Safeguard 3 and Australian Privacy Principle 3</b></p> <p>APP 3 applies in parallel to Privacy Safeguard 3.</p> <p>Privacy Safeguard 3 applies instead of APP 3 when an accredited person is seeking to collect CDR data.</p> <p>APP 3 will continue to apply to any personal information collected by an accredited person that is not CDR data.</p>
<b>Accredited data recipient</b>	<p><b>Privacy Safeguard 3</b></p> <p>Privacy Safeguard 3 applies instead of APP 3,<sup>4</sup> meaning APP 3 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime.</p> <p>APP 3 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data.<sup>5</sup></p>

<sup>3</sup> 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.

<sup>4</sup> 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).

<sup>5</sup> 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

CDR entity	Privacy principle that applies
<b>Designated gateway</b>	<b>Australian Privacy Principle 3</b> Privacy Safeguard 3 does not apply to a designated gateway.
<b>Data holder</b>	<b>Australian Privacy Principle 3</b> 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 from when the 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 Consumer Data Rules is by making a ‘consumer data request’ to a data holder on behalf of the consumer. Consumer data requests are explained below at paragraphs 3.21–3.25. The point at which an accredited person makes a consumer data request is demonstrated by the flow chart under paragraph 3.28.
- 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’. ‘Record’ and ‘generally available publication’ have the same meaning as within the Privacy Act.<sup>6</sup>

## 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 CDR consumer and the accredited person complies with all other requirements in the Consumer Data 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.

---

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.

<sup>6</sup> Privacy Act, s 6(1): ‘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.

Privacy Act, s 6(1): ‘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.

## What is a ‘valid request?’

3.16 Under Consumer Data Rule 4.3, a CDR 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 CDR consumer’s CDR data<sup>7</sup> to provide the requested goods or services
- the accredited person asks the consumer’s consent to the collection of their CDR data, in accordance with Subdivision 4.3.2 of the Consumer Data Rules (see paragraphs 3.17–3.20 below for further information) and
- the consumer expressly consents to this collection of their CDR data.

## Process for asking for consent

3.17 Subdivision 4.3.2 of the Consumer Data Rules outline the requirements for consent for the purposes of making a valid request for collection of CDR data.

3.18 Specifically, the 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** (Rule 4.10): to ensure that the consent is as easy to understand as practicable.
- **Requirements when asking for consent** (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 (Rule 4.15).
- **Restrictions on seeking consent** (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** (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** (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).

3.19 The accredited person is also required to have regard to the [Consumer Experience Guidelines](#)<sup>8</sup> when asking a CDR consumer to give consent.

3.20 These specific requirements and processes for the above Consumer Data Rule requirements are explained in [Chapter C \(Consent\)](#).

---

<sup>7</sup> Note that the data may be required consumer data or voluntary consumer data for these purposes.

<sup>8</sup> Consumer Data Rule 4.10(a)(ii). The ‘Consumer Experience Guidelines’ provide best practice interpretations of the Consumer Data Rules relating to consent and are discussed in Chapter B (Key Concepts).

## Consumer data request

- 3.21 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,<sup>9</sup> the accredited person may request the relevant data holder to disclose some or all of the CDR data that:
- 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.<sup>10</sup>
- 3.22 In doing so, the accredited person makes a 'consumer data request' to a data holder on behalf of the consumer.<sup>11</sup> 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.
- 3.23 When the accredited person makes a consumer data request on behalf of a CDR consumer, they must not seek to collect more CDR data than is reasonably needed, or that relates to a longer time period than reasonably required, in order to provide the requested goods or services.<sup>12</sup>
- 3.24 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.<sup>13</sup>
- 3.25 An accredited person complies with Privacy Safeguard 3 after giving a data holder a consumer data request in the manner set out above.<sup>14</sup>

## Data minimisation principle

- 3.26 Collection of CDR data is limited by the data minimisation principle (Rule 4.12(2)), where an accredited person:
- must not collect more data than is reasonably needed in order to provide the requested goods or services, and
  - may use the collected data only consistent with the consent provided, and only as reasonably needed in order to provide the requested goods or services.
- 3.27 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.
- 3.28 The data minimisation principle is discussed further in Chapter B (Key Concepts).

---

<sup>9</sup> 'Current consent' is discussed in Chapter B (Key Concepts).

<sup>10</sup> Consumer Data Rule 4.4(1).

<sup>11</sup> Consumer Data Rule 4.4(2).

<sup>12</sup> Consumer Data Rules 1.8(a), 4.4(1)(d).

<sup>13</sup> Consumer Data Rule 4.4(3).

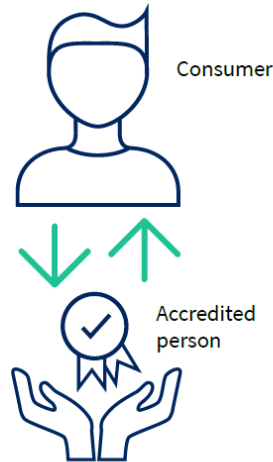
<sup>14</sup> The effect of Consumer Data Rule 4.4(2) is that a request for CDR data from an accredited person on behalf of a CDR consumer that does not comply with Consumer Data Rule 4.4(1) is not a 'consumer data request'.


**Example:** As part of a consumer data request to seek information about their eligibility to open a bank account, the accredited person asks a consumer for their consent to collect information about their marital status from the data holder, when this has no bearing on the applicant's eligibility for the service. This is a breach of the data minimisation principle.



Obtaining consumer consent for the collection and use of CDR data

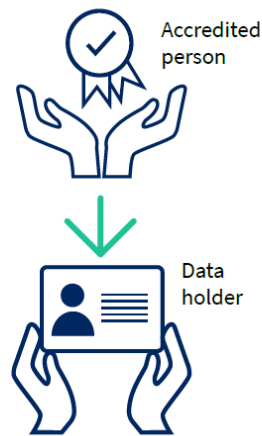
- Accredited person offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- Accredited person asks the consumer to consent to the collection and use of their CDR data for this purpose, for up to 12 months
- Consumer provides their express consent



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'



Data holder sends consumer data to accredited data recipient



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

# Interaction with other Privacy Safeguards

## Privacy Safeguard 4

- 3.29 The Privacy Safeguards distinguish between an accredited person collecting solicited CDR data (Privacy Safeguard 3) and unsolicited CDR data (Privacy Safeguard 4).
- 3.30 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)).
- 3.31 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

- 3.32 Privacy Safeguard 5 requires an accredited person who has collected data in accordance with Privacy Safeguard 3 to notify the CDR consumer of the collection in accordance with the Consumer Data Rules (See Chapter 5 (Privacy Safeguard 5)).