Chapter 3:

Privacy Safeguard 3 —

Seeking to collect CDR data from CDR participants

Version ~~4~~5.0, November ~~2022~~2023

OAIC

Contents

Key points

- Privacy Safeguard 3[1] prohibits an accredited person from attempting to collect CDR data under the CDR system 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.
- Privacy Safeguard 3 applies whether the collection is directly from the CDR participant or indirectly through a designated gateway.[2]

What does Privacy Safeguard 3 say?

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

- the consumer has requested the accredited person seek to collect the relevant data by providing 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.[3]

3.2 Under the CDR Rules:

- the valid request must meet specific requirements, including compliance with the CDR Rules regarding consent,[4] and
- accredited persons must have regard to the data minimisation principle,[5] 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.[6] Privacy Safeguard 3

---

[1] Competition and Consumer Act, section 56EF.

[2] There are currently no designated gateways in the banking sector or energy sector. See Chapter B (Key concepts) for further information on designated gateways.

[3] Competition and Consumer Act, section 56EF.

[4] ~~CDR Rules, rule 4.3.~~ CDR Rules, rule 4.3 (for requests for accredited persons to seek to collect CDR data) and rule 4.3A (for requests for CDR representative principals to seek to collect CDR data on behalf of CDR representatives.

[5] CDR Rules, subrule 4.12(2~~).~~); see subrule 4.20F(2) which applies where a CDR representative is seeking the collection consent.

[6] Competition and Consumer Act, subsection 56EF(2).

will also apply to an accredited person where they engage an outsourced service provider (OSP) to seek to collect CDR data on their behalf.[7]

Why is it important?

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

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 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.[8]

3.9 APP 3 outlines when an entity may collect solicited personal information (See APP Guidelines, Chapter 3 (APP 3)).

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.[9]

[7] The CDR Rules requirements for engaging an outsourced service provider (OSP) to collect data on an accredited person's behalf are outlined in paragraphs 3.36– 3.41.

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

[9] See Competition and Consumer Act, subsection 56EC(4) and section 56EF.

CDR entity	Privacy protections that apply in the CDR context
Designated gateway	**APP 3** Privacy Safeguard 3 does not apply to a designated gateway.
Data holder[10]	**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 3.24 to 3.32. 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'.[11] 'Record'[12] and 'generally available publication'[13] have the same meaning as within the Privacy 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 Competition and Consumer Act, subsection 56EC(4) and paragraph 56EC(5)(aa)). 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 Privacy Act, subsection 6E(1D).

[10] In this chapter, references to data holders include AEMO. See Chapter B (Key concepts) for further information about how the privacy safeguards apply to AEMO.

[11] Competition and Consumer Act, subsection 4(1).

[12] Subsection 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.

[13] Subsection 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.

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, either directly or through a designated gateway,[14] 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 rule 4.3 of the CDR Rules, a consumer gives an accredited person a 'valid' request to seek to collect their CDR data from a CDR participant if:

- 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,[15] in accordance with Division 4.3 of the CDR Rules (see paragraphs 3.19–3.23 for further information), and
- the consumer expressly consents to this collection and use of their CDR data.

3.16 In relation to a CDR representative arrangement, under rule 4.3A of the CDR Rules, a consumer gives a CDR representative principal a 'valid' request to seek to collect their CDR data from a CDR participant if:

- the request is for the principal's CDR representative to provide goods or services
- the CDR representative needs to request its CDR representative principal to collect the consumer's CDR data from a CDR participant, and the CDR representative needs to use it in order to provide the requested goods or services, and
- the CDR representative asks the consumer for a collection consent (for the CDR representative principal to collect their data and disclose it to the CDR representative), and a use consent (for the CDR ~~principal to disclose that data to the CDR representative and for the CDR~~ representative to use it to provide the requested goods or services), in accordance with Division 4.~~3~~3A of the CDR Rules (see paragraphs 3.19 to 3.23 for further information), and the consumer expressly consents to this collection and use of their CDR data.

[14] There are currently no designated gateways in the banking sector or energy sector. See Chapter B (Key concepts) for further information on designated gateways.

[15] 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.

3.17 A request ceases to be 'valid' if the consumer withdraws their collection consent.[16]

3.18 Entities should also be mindful that the *Competition and Consumer Act 2010* (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.[17]

Process for asking for consent

3.19 Division 4.3 of the CDR Rules outlines the requirements for consentconsents given to accredited persons for the purposes of making a valid request for the collection and use of CDR data.

3.20 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** (rule 4.10 of the CDR Rules): 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 of the CDR Rules): 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 (rule 4.15 of the CDR Rules).
- **Restrictions on seeking consent** (rule 4.12 of the CDR Rules): including that an accredited person cannot seek to collect or use CDR data for a period exceeding 12 months. (or, in the case of a CDR business consumer, cannot seek consent to use CDR data for longer than 7 years).
- Obligations about **managing the withdrawal of consent** (rule 4.13 of the CDR Rules): including that a consumer may withdraw their consent at any time through their consumer dashboard or by using a simple alternative method made available by the accredited person. In the energy sector, rule 4.13 of the CDR Rules applies to primary data

[16] CDR Rules, subrules 4.3(4) and 4.3A(5). 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)), and the CDR representative principal could continue to disclose CDR data it had already collected to the CDR representative and the CDR representative could use it to provide the requested goods or services (see the note under CDR Rules, subrule 4.3A(5)). See further CDR Rules, rule 4.18Arules 4.18 and 4.18A (for the accredited person) and rules 4.20O and 4.20Q (for the CDR representative) 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).

[17] Competition and Consumer Act, sections 56BN and 56BO.

holders as if they were the data holder for any SR (shared responsibility) data covered by the SR data request.[18]

- Time of **expiry of consent** (rule 4.14 of the CDR Rules): 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).

3.21 The accredited person is also required to have regard to the Consumer Experience Guidelines[19] when asking a consumer to give consent.

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

3.23 In relation to a CDR representative arrangement, rule 4.3CDivision 4.3A of the CDR Rules modifies Division 4.3 ofoutlines the CDR Rules in relationrequirements for consents given to CDR representatives seeking consent. It contains similar requirements to those in Division 4.as outlined above in paragraphs 3.20 - 3.21. . A CDR representative principal must ensure that when their CDR representative asks for a consumer's consent, it does so in accordance with the modified requirements of Division 4.33A.[20]

Consumer data request

3.24 If a consumer has given an accredited person a valid request (see paragraphs 3.15 to 3.18 above),[21] and the consumer's consent for the accredited person to collect and use their CDR data is current,[22] 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.[23]

3.25 In doing so, the accredited person makes a 'consumer data request' to a CDR participant on behalf of the consumer.[24] 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.

---

[18] CDR Rules, subrule 1.23(10). For further information on SR data, see Chapter B (Key concepts).

[19] CDR Rules, paragraph 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).

[20] CDR Rules, rule subrule 1.16A(3) and (4.3C.).

[21] This includes valid requests given to a CDR representative principal to collect CDR data on behalf of a CDR representative.

[22] See paragraphs 3.15 and 3.16 above.

[23] CDR Rules, subrules 4.4(1) and 4.7A(1).

[24] CDR Rules, subrules 4.4(2) and 4.7A(2).

3.26 In relation to a sponsorship arrangement, a person with sponsored accreditation (affiliate) cannot make a consumer data request directly to a data holder. They may only make a consumer data request:

- to an accredited data recipient under rule 4.7A of the CDR Rules, or
- through its registered sponsor acting at its request under a sponsorship arrangement.[25]

3.27 Where a sponsor has collected CDR data at the request of a person with sponsored accreditation (affiliate), the CDR data is taken to have been also collected by the affiliate.[26]

3.28 An accredited person may also make a consumer data request to a CDR representative as if the CDR representative were an accredited data recipient.[27] CDR representatives that receive such a consumer data request are able to obtain a disclosure consent from the consumer.[28]

3.29 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.[29]

3.30 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.[30]

3.31 If a consumer data request includes SR data, an accredited person must make the consumer data request to the primary data holder (rather than the secondary data holder).[31] The primary data holder must then make a request for the SR data to the secondary data holder:

- using the secondary data holder's request service, and
- in accordance with the data standards.[32]

3.32 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 3.30.[33]

---

[25] CDR Rules, subrule 5.1B(3).

[26] CDR Rules, subrule 7.6(3).

[27] CDR Rules, subrule 4.3B(1).

[28] CDR Rules, subrule 4.3B(2).

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

[30] CDR Rules, subrule 4.4(3).

[31] CDR Rules, subrule 1.23(2). If a CDR consumer is eligible to initiate a consumer data request from an accredited person to a primary data holder for SR data, the CDR consumer is not also eligible to initiate a consumer data from an accredited person to the secondary data holder for that data: see CDR Rules, rule 1.19. Under current arrangements, this is only relevant to the energy sector as the only sector with SR data and a secondary data holder (AEMO). For further information on SR data and primary and secondary data holders, see Chapter B (Key concepts).

[32] CDR Rules, subrule 1.23(4).

[33] The effect of CDR Rules, subrules 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 subrules 4.4(1) or CDR Rule 4.7A(1) is not a 'consumer data request'.

Data minimisation principle

3.33 Collection of CDR data is limited by the data minimisation principle,[34] 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.

3.34 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.

3.35 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?

3.36 An accredited person (other than those with sponsored accreditation)[35] who is an OSP chain principal may engage a third party to seek to collect CDR data on their behalf, in accordance with the CDR Rules.[36]

3.37 Rule 1.10 of the CDR Rules requires the accredited person (the 'OSP chain principal') to have a CDR outsourcing arrangement with the third party (the '~~outsourced service provider',~~OSP'

[34] CDR Rules, subrule 4.12(2~~). There are no equivalent requirements~~) (for ~~how an~~ accredited ~~person makes a consumer data request to an accredited data recipient.~~persons), subrule 4.20F (for CDR representatives) and rule 1.8.

[35] CDR Rules, subrule 5.1B(4).

[36] CDR Rules, paragraph 1.10(~~23~~)(a)(i).

or 'provider'). A CDR outsourcing arrangement is a written contract between the OSP principal (in this collection scenario, an OSP chain principal) and provider which meets the requirements set out in subrule 1.10(23) of the CDR Rules.[37]

3.38 The level to which an entity is accredited affects the purpose for which they can engage a provider:

- entities accredited to the unrestricted level and who are OSP chain principals can engage providers to collect data (in addition to disclosing data to providers to enable them to provide goods or services to the entity), and
- entities accredited to the sponsored level cannot engage a provider to collect CDR data on their behalf[38] (but are permitted to disclose data to providers under a CDR outsourcing arrangement to enable them to provide goods or services to the entity).

3.39 Where an accredited person intends to use an ~~outsourced service provider~~OSP to seek to collect a consumer's CDR data, the accredited person must:

- at the time of seeking the consumer's consent to collect and use the consumer's CDR data, advise the consumer that CDR data may be disclosed to, or collected by, an ~~outsourced service provider~~OSP and that further information can be obtained from the accredited person's CDR policy (with the link to the accredited person's CDR policy provided),[39] and
- include certain information about ~~outsourced service providers~~OSPs in its CDR policy, including a list of providers, and for each provider, the nature of the services it provides and the CDR data that it may collect.[40]

~~3.40~~ The accredited person must ensure the provider complies with its requirements under the CDR outsourcing arrangement.~~[41]~~

~~3.41~~3.40 ~~The CDR data collected by a 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.[42]~~, and is in breach if the provider fails to comply with a required provision of the arrangement.[43]

~~3.42~~3.41 Rule 7.6 of the CDR Rules provides that where an accredited person has collected CDR data under the CDR Rules, it must not use or disclose the CDR data (or CDR data derived from it) other than for a permitted use or disclosure. For the purposes of this rule, any use, disclosure or collection of ~~service~~ data by the provider in a CDR outsourcing arrangement

---

[37] ~~'~~For more guidance on CDR outsourcing ~~arrangement' is discussed in~~arrangements, see Chapter B (Key Concepts~~).~~), CDR outsourcing arrangement: privacy obligations for an outsourced service provider and CDR outsourcing arrangement: privacy obligations for a principal of an outsourced service provider.

[38] CDR Rules, subrule 5.1B(4).

[39] CDR Rules, subrule 4.11(3)(f). See Chapter C (Consent).

[40] CDR Rules, subrule 7.2(4). See Chapter 1 (Privacy Safeguard 1).

~~[41] CDR Rules, subrule 1.16(1). The requirements for a CDR outsourcing arrangement are set out in CDR Rules, subrule 1.10(2).~~

~~[42] CDR Rules, subrule 1.10(4).~~

[43] CDR Rules, subrules 1.16(1) and (2). The requirements for a CDR outsourcing arrangement are set out in CDR Rules, subrule 1.10(3).

will be taken to have been by the principal under the arrangement. This occurs regardless of whether the use, disclosure or collection is in accordance with the CDR outsourcing arrangement.[44]

Risk point: Entities that fail to take 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.

*[**Note:** the three diagrams showing CDR consent and collection process for accredited persons, for sponsors and for CDR representative arrangements have been updated].*

[44] CDR Rules, subrules 7.6(2) and (5).

Interaction with other privacy safeguards

Privacy Safeguard 4

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

3.443.43 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)).

3.453.44 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

3.463.45 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)).