Chapter 4:

Privacy Safeguard 4 —

Dealing with unsolicited CDR data from CDR participants

Consultation draft, September 2022

OAIC

Contents

Key points 3
What does Privacy Safeguard 4 say? 3
Why is it important? 3
Who does Privacy Safeguard 4 apply to? 3
How Privacy Safeguard 4 interacts with the Privacy Act 4
Unsolicited CDR data 5
In what circumstances does Privacy Safeguard 4 apply? 5
Meaning of 'purportedly under the CDR Rules' 5
Meaning of 'not as the result of seeking to collect that data under the CDR Rules' 6
What is the obligation to destroy unsolicited data? 6
'Destroy' 6
As soon as practicable 7
Not required to retain the data 7
How does Privacy Safeguard 4 interact with the other privacy safeguards? 7

Key points

- Privacy Safeguard 4 requires an accredited person to destroy unsolicited ~~consumer data right (~~CDR~~)~~ data that the entity collects and is not required to retain by Australian law or court/tribunal order.

What does Privacy Safeguard 4 say?

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

4.2 Privacy Safeguard 4 requires an accredited person to, as soon as practicable, destroy CDR data that the person has collected from a data holder or accredited data recipient ('CDR participant'), purportedly under the consumer data rules (CDR Rules), where the accredited person has not sought to collect that particular data and is not required to retain it by or under an Australian law or court/tribunal order.[1]

4.3 This obligation applies regardless of whether the accredited person collects the CDR data directly from a CDR participant or indirectly through a designated gateway.[2]

Why is it important?

4.4 The objective of Privacy Safeguard 4 is to ensure that CDR data collected by an accredited person is afforded appropriate privacy protection, even where the accredited person has not solicited the CDR data.

4.5 Privacy Safeguard 4 requires accredited persons to destroy CDR data they have collected but not requested, unless an exception applies. This destruction requirement strengthens the protections for consumers under the CDR ~~regime~~system and ensures that accredited persons cannot retain unsolicited CDR data unless another Australian law or court/tribunal order requires them to.

Who does Privacy Safeguard 4 apply to?

4.6 Privacy Safeguard 4 applies to accredited persons. It does not apply to data holders or designated gateways.

4.7 Data holders and designated gateways must ensure that they are adhering to their obligations under the *Privacy Act 1988* (Privacy Act) and ~~Australian Privacy Principle (APP)~~APP 4 when dealing with unsolicited personal information.

4.8 Although data holders do not have obligations under Privacy Safeguard 4, primary data holders (being, under current arrangements, retailers in the energy sector) must ensure that they comply with rule 1.25 of the CDR Rules in relation to SR data which they collect from a secondary data holder purportedly under the CDR rules, but not as the result of seeking to

[1] ~~Section 56EG(1) of the~~ Competition and Consumer Act~~.~~, subsection 56EG(1).

[2] ~~Section 56EG(2) of the~~ Competition and Consumer Act~~.~~, subsection 56EG(2).

collect that SR data under the CDR Rules.[3] Rule 1.25 of the CDR Rules provides that primary data holders must, as soon as practicable, destroy such SR data (provided that the primary data holder is not required to retain it by or under an Australian law or court/tribunal order).[4]

4.9 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 4. However, under the terms of the CDR representative arrangement with their CDR principal,[5] a CDR representative is required to comply with Privacy Safeguard 4 in its handling of service data as if it were the CDR principal.[6,7] A CDR principal breaches subrule 7.3A(1) of the CDR Rules if its CDR representative fails to comply with Privacy Safeguard 4 as if it were an accredited person who had collected the service data (regardless of whether the CDR representative's actions accord with the CDR representative arrangement).[8]

How Privacy Safeguard 4 interacts with the Privacy Act

~~4.8~~4.10 It is important to understand how Privacy Safeguard 4 interacts with the Privacy Act and APPs.[9]

~~4.9~~4.11 APP 4 applies to unsolicited personal information. APP 4 requires an APP entity to destroy or de-identify unsolicited personal information it receives if the entity determines that it could not have collected the information under APP 3.[10]

CDR Entity	Privacy protections that apply in the CDR context
Accredited person	Privacy Safeguard 4 When an accredited person collects unsolicited CDR data purportedly under the CDR Rules, Privacy Safeguard 4 applies. APP 4 does not apply to the accredited person in relation to that CDR data.[11]

[3] See Chapter B (Key concepts) for more information on SR data, primary data holder and secondary data holder.

[4] CDR Rules, rule 1.25.

[5] A CDR representative arrangement is a written contract between a CDR representative and their CDR principal that meets the minimum requirements listed in subrule 1.10AA(2) of the CDR Rules.

[6] CDR Rules, paragraph 1.10AA(2)(d)(i)(B).

[7] See Chapter B (Key concepts) for more information on 'CDR principal', 'CDR representative', 'CDR representative arrangement' and 'service data'.

[8] CDR Rules, rule 7.3A. See also rule 1.16A in relation to a CDR principal's obligations and liability.

[9] 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.

[10] See Chapter 3: APP 3 – Collection of solicited personal information of the APP Guidelines.

[11] See ~~ss 56EC(4) and 56EG the~~ Competition and Consumer Act, subsection 56EC(4) and section 56EG.

Note: If Privacy Safeguard 4 does not apply, APP 4 may continue to apply to other unsolicited 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, 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 ~~s 6E(1D) of the~~ Privacy Act~~.~~, subsection 6E(1D).

Designated gateway	APP 4 Privacy Safeguard 4 does not apply to a designated gateway.
Data holder[12]	APP 4 Privacy Safeguard 4 does not apply to a data holder. However, CDR Rule 1.25 does apply similar obligations to primary data holders in relation to unsolicited SR data (see above at paragraph 4.8).

Unsolicited CDR data

4.104.12 The term 'unsolicited' is used in the heading to Privacy Safeguard 4 and refers to CDR data collected by an accredited person who has not sought to collect that data under the CDR Rules.

4.114.13 An example of how an accredited person might collect such 'unsolicited' CDR data is where:

- the accredited person makes a consumer data request on a consumer's behalf to collect CDR data from a data holder, in accordance with Privacy Safeguard 3 and rule 4.4 of the CDR ~~Rule 4.4~~Rules
- the data holder has or receives authorisation from the consumer, and
- the data holder then discloses CDR data that includes data outside the scope of the consumer data request (and which may also be outside the data holder's authorisation).[13]

4.124.14 A discussion of how an accredited person may properly seek to collect CDR data is contained in Chapter 3 (Privacy Safeguard 3).

In what circumstances does Privacy Safeguard 4 apply?

4.134.15 Privacy Safeguard 4 applies to CDR data collected by an accredited person from a CDR participant:

- purportedly under the CDR Rules, but
- not as the result of seeking to collect that CDR data under the CDR Rules.[14]

Meaning of 'purportedly under the CDR Rules'

4.144.16 Privacy Safeguard 4 applies to CDR data collected 'purportedly under the CDR Rules'[15]

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

[13] In these circumstances the data holder may be in breach of APP 6 if personal information was disclosed outside the authorisation provided by the consumer.

[14] ~~Section 56EG(1)(a) of the~~ Competition and Consumer Act~~.~~, paragraph 56EG(1)(a).

[15] ~~Section 56EG(1)(a)(i) of the~~ Competition and Consumer Act~~.~~, paragraph 56EG(1)(a)(i).

4.154.17 'Purportedly' in this context means that the mechanisms of the CDR rules appear to have been used but this did not validly occur because the accredited person did not, in fact, seek to collect the CDR data.

Meaning of 'not as the result of seeking to collect that data under the CDR Rules'

4.164.18 Privacy Safeguard 4 applies to CDR data that is collected other than as a result of the accredited person seeking to collect it under the CDR Rules.[16]

4.174.19 In practice, Privacy Safeguard 4 will typically apply to CDR data received by the accredited person that is outside the scope of the accredited person's consumer data request to the CDR participant.

Example

Friedrich makes a valid request for Green ~~Bank~~Company (an accredited person) to collect his CDR data. Green ~~Bank~~Company then seeks to collect Friedrich's CDR data from Yellow ~~Bank~~Company, a data holder for Friedrich's CDR data, through a consumer data request in accordance with the CDR Rules.

Yellow ~~Bank~~Company mistakenly discloses Salome's CDR data to Green ~~Bank~~Company, rather than Friedrich's data. A Green ~~Bank~~Company employee realises the error and immediately arranges for the collected data to be destroyed, in compliance with Privacy Safeguard 4. The next day, Yellow ~~Bank~~Company discloses Friedrich's CDR data pursuant to the consumer data request. Unfortunately, Yellow ~~Bank~~Company also discloses data outside the scope of the request.

Green ~~Bank~~Company soon realises that additional CDR data outside the scope of the request has been disclosed to it, which it is not required to retain. However, Green ~~Bank~~Company does not take any steps to destroy the additional data. Green ~~Bank~~Company has likely breached Privacy Safeguard 4.

What is the obligation to destroy unsolicited data?

'Destroy'

4.184.20 Privacy Safeguard 4 requires unsolicited CDR data to be 'destroyed'. Destruction of CDR data should follow the CDR data deletion process discussed in detail in Chapter 12 (Privacy Safeguard 12).

[16] ~~Section 56EG(1)(a)(ii) of the~~ Competition and Consumer Act~~.~~, paragraph 56EG(1)(a)(ii).

As soon as practicable

4.194.21 Privacy Safeguard 4 requires unsolicited CDR data to be destroyed 'as soon as practicable'.[17]

4.204.22 The test of practicability is an objective test. It is the responsibility of the accredited person to be able to justify that it is not practicable to destroy unsolicited data promptly after its collection.

4.214.23 Accredited persons should ensure that they have systems and processes to quickly recognise and review CDR data collected which is outside the scope of a consumer data request.

4.224.24 In adopting a timetable that is 'practicable' an accredited person can take technical and resource considerations into account. However, it is the responsibility of the accredited person to justify any delay in destroying unsolicited CDR data.

4.234.25 The timeframe in which an accredited person must destroy unsolicited CDR data begins at the time the entity becomes aware that the data was not solicited. How quickly an accredited person becomes aware of unsolicited CDR data may depend on its available technical and other resources.

Not required to retain the data

4.244.26 The obligation to destroy unsolicited data does not apply to CDR data that an accredited person is required to retain by or under an Australian law or court/tribunal order.[18]

4.254.27 The concept 'required by or under another Australian law or court/tribunal order' is discussed in Chapter B (Key concepts).

How does Privacy Safeguard 4 interact with the other privacy safeguards?

4.264.28 Privacy Safeguard 3 prohibits an accredited person from seeking to collect CDR data from a CDR participant unless in response to a valid request from a consumer, and in compliance with the CDR Rules (see Chapter 3 (Privacy Safeguard 3)).

4.274.29 Privacy Safeguard 12 requires an accredited data recipient to destroy or de-identify redundant data unless the entity is required by or under an Australian law or court/tribunal order to retain it, or if the data relates to current or anticipated legal or dispute resolution proceedings to which the recipient is a party (see Chapter 12 (Privacy Safeguard 12)).

4.284.30 Privacy Safeguard 12 and Privacy Safeguard 4 together ensure that both unsolicited CDR data as well as solicited data that is no longer needed for CDR purposes are destroyed (or alternatively de-identified for the purposes of solicited data).

---

[17] Competition and Consumer Act, subsection 56EG(1).

[18] Section 56EG(1)(b) of the Competition and Consumer Act., paragraph56EG(1)(b).