Chapter 4:

Privacy Safeguard 4 —

Dealing with unsolicited CDR data from CDR participants

Version 1.0, February 2020

Contents

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 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 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 data holder 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 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) 4 when dealing with unsolicited personal information.

[1] Section 56EG(1) of the Competition and Consumer Act. Note: The privacy safeguards only apply to CDR data for which there are one or more consumers (section 56EB(1) of the Competition and Consumer Act). This means that Privacy Safeguard 4 does not require an accredited person to destroy unsolicited CDR data for which there is no consumer (for instance, unrequested information about a product).

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

How does Privacy Safeguard 4 interact with the Privacy Act and APP 4?

4.8 It is important to understand how Privacy Safeguard 4 interacts with the Privacy Act and APPs.[3]

4.9 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.[4]

CDR Entity	Privacy protections that apply in the CDR context
Accredited person / accredited data recipient	**Privacy Safeguard 4 and APP 4** Privacy Safeguard 4 applies to accredited persons from the point when they collect CDR data. APP 4 will continue to apply to personal information collected that is not CDR data.[5]
Designated gateway	**APP 4** Privacy Safeguard 4 does not apply to a designated gateway.
Data holder	**APP 4** Privacy Safeguard 4 does not apply to a data holder.

Unsolicited CDR data

4.10 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.

4.11 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 CDR Rule 4.4
- 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).[6]

[3] 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.

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

[5] 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.

[6] 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.

4.12 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?

4.13 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.[7]

Meaning of 'purportedly under the CDR Rules'

4.14 Privacy Safeguard 4 applies to CDR data collected 'purportedly under the CDR Rules'[8]

4.15 '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'

4.16 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.[9]

4.17 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 data holder.

Example

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

Yellow Bank mistakenly discloses Salome's CDR data to Green Bank, rather than Friedrich's data. A Green Bank 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 discloses Friedrich's CDR data pursuant to the consumer data request. Unfortunately, Yellow Bank also discloses data outside the scope of the request. *cont*

[7] Section 56EG(1)(a) of the Competition and Consumer Act.

[8] Section 56EG(1)(a)(i) of the Competition and Consumer Act.

[9] Section 56EG(1)(a)(ii) of the Competition and Consumer Act.

Green Bank 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 does not take any steps to destroy the additional data. Green Bank has likely breached Privacy Safeguard 4.

What is the obligation to destroy unsolicited data?

'Destroy'

4.18 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).

As soon as practicable

4.19 Privacy Safeguard 4 requires unsolicited CDR data to be destroyed 'as soon as practicable'.

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

4.21 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.

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

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

Not required to retain the data

4.24 The obligation to destroy unsolicited data does not apply to CDR data that an entity is required to retain by or under an Australian law or court/tribunal order.[10]

4.25 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?

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

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

4.27 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)).

4.28 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).