Chapter 4:

Privacy Safeguard 4 —

Dealing with unsolicited CDR data from CDR participants

Consultation draft, October 2019

OAIC

Contents

Key points

- Privacy Safeguard 4 requires an accredited person to destroy unsolicited Consumer Data Right (CDR) data that the entity 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, but 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.

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 control and ownership consumers have over their data 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 and APP 4 when dealing with unsolicited personal information.

[1] 56EG(1).

[2] 56EG(2).

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

4.8 It is important to understand how Privacy Safeguard 12 interacts with the Privacy Act 1988 (the Privacy Act) and Australian Privacy Principles (APPs).[3]

4.9 Like Privacy Safeguard 4, APP 4 relates 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]

Summary of application of Privacy Safeguard 4 by CDR entity

CDR Entity	Privacy principle that applies to CDR data
Accredited person	**Privacy Safeguard 4** Although APP 4 applies in parallel with Privacy Safeguard 4, an accredited person will be an 'accredited data recipient' for the CDR data purportedly collected under the Consumer Data Rules, which means that APP 4 will not apply in respect of that data. APP 4 will continue to apply to any personal information handled by the accredited person that is not CDR data.
Accredited data recipient	**Privacy Safeguard 4** Privacy Safeguard 4 applies instead of APP 4, meaning APP 4 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime. APP 4 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data. This is because all accredited data recipients are subject to the Privacy Act and the APPs for any personal information, even if it is not CDR data.
Designated gateway	**Australian Privacy Principle 4** Privacy Safeguard 4 does not apply to a designated gateway.
Data holder	**Australian Privacy Principle 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 Consumer Data Rules.

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

[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.

- the accredited person makes a consumer data request on a CDR consumer's behalf to collect CDR data from a data holder, in accordance with Privacy Safeguard 3 and Consumer Data Rule 4.4
- the data holder has or receives authorisation from the CDR 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).[5]

4.12 A discussion of how an accredited person may properly seek to collect CDR data is contained in Chapter 3 (Privacy Safeguard 3) at [3.14].

What circumstances does Privacy Safeguard 4 apply to?

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

- purportedly under the Consumer Data Rules; but
- not as the result of seeking to collect that CDR data under the Consumer Data Rules.[6]

Where CDR data is collected outside the Consumer Data Rules

4.14 Neither Privacy Safeguard 3 nor Privacy Safeguard 4 apply where an accredited person seeks to collect CDR data outside of the Consumer Data Rules. This is because Privacy Safeguard 3 only applies where an accredited person seeks to collect data under the Consumer Data Rules, and Privacy Safeguard 4 only applies where an accredited person collects CDR data purportedly under the Consumer Data Rules.

4.15 An accredited person who collects CDR data outside of the Consumer Data Rules is not an 'accredited data recipient' as defined in s 56AK, as the CDR data will not be disclosed to the person under the Consumer Data Rules. Therefore, Privacy Safeguard 6 (which concerns use of disclosure of CDR data) and Privacy Safeguard 12 (which concerns security of CDR data) do not apply in such circumstances.

4.16 Instead, the accredited person will be a data holder of that CDR data, if they are an accredited data recipient of 'other CDR data'.[7] In respect of the CDR data received outside the Consumer Data Rules, the person must comply with the privacy safeguards applicable to data holders, and if the person is an APP entity, the Privacy Act and APPs in respect of personal information, to the extent not overridden by the Privacy Safeguards.

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

[6] s 56EG(1)(a).

[7] 56AJ(3)(b). 'Other CDR data' is CDR data other than the CDR data that the accredited person has collected outside of the Consumer Data Rules: see Notes 1 and 2 regarding s 56AJ(3).

Example

Penny makes a valid consumer data request of her bank to disclose all of her CDR data under Consumer Data Rule 3.3. Her bank then discloses all her CDR data it holds pursuant to Consumer Data Rule 3.4.

Penny has a mortgage broker, Brent, who is registered as an accredited person. Penny gives Brent her CDR data via a USB and asks him to find the best deal to refinance her loan on the market. Brent agrees and takes the USB.

Brent has collected CDR data outside of the Consumer Data Rules. Neither Privacy Safeguard 3 nor Privacy Safeguard 4 apply.

Brent is, however, a 'data holder' of the CDR data under section 56AJ(1) and (3). He must comply with Privacy Safeguards 1, 10, 11 and 13.

If Brent is an APP entity, he must also comply with the Privacy Act and relevant APPs in respect of the personal information he has collected from Penny.

What is the obligation to destroy unsolicited data?

'Destroy'

4.17 Privacy Safeguard 4 requires unsolicited CDR data to be 'destroyed'. Destruction of CDR data is discussed in detail in Chapter 12 (Privacy Safeguard 12).

As soon as practicable

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

4.19 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.

4.20 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.

4.21 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.

4.22 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

4.23 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.[8]

[8] 56EG(1)(b).

4.24 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 other Privacy Safeguards?

4.25 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 CDR consumer, and in compliance with the Consumer Data Rules (see Chapter 3 (Privacy Safeguard 3)).

4.26 Privacy Safeguard 12 requires an accredited data recipient to destroy or de-identify redundant CDR 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)).

4.27 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).