Chapter 5:

Privacy Safeguard 5 —

Notifying of the collection of CDR data

Consultation draft, October 2019

OAIC

Contents

Key points

- An accredited person must notify the relevant consumer when they collect Consumer Data Right (CDR) data.
- This notification must occur through their consumer dashboard as soon as practicable after the accredited person has received the CDR data.

What does Privacy Safeguard 5 say?

5.1 If an accredited person collects CDR data under Privacy Safeguard 3, the accredited person must notify the consumer/s of the collection by taking the steps identified in the Consumer Data Rules.[1]

5.2 The notification must:

- be given to the consumers whom the Consumer Data Rules require to be notified
- cover the matters set out in the Consumer Data Rules, and
- be given at or before the time specified in the Consumer Data Rules.

5.3 Under Consumer Data Rule 7.4, an accredited person must notify the CDR consumer through their consumer dashboard as soon as practicable after CDR data is collected from a CDR participant.

5.4 For information about the concept of 'collects' refer to Chapter B, Key Concepts.

Why is this important?

5.5 Notification of collection of CDR data is an integral element of the CDR regime as it provides confirmation to the consumer that their CDR data has been collected in accordance with their valid request.

5.6 This ensures consumers are informed when their CDR data is collected and builds trust between consumers and CDR participants.

Risk point: Clear and prompt communication to consumers will promote trust in the CDR scheme. If a consumer has a poor experience, they may not be interested in continuing to participate.

Privacy tip: In addition to notifying the CDR consumer of the collection of their CDR data via the consumer dashboard, an accredited person must provide the consumer with a 'CDR receipt' as soon as practicable after the consumer consents to the collection and use of their CDR data.[2] This 'CDR receipt' must be given in writing but not through the consumer dashboard (e.g. via text or email).

[1] Section 56EH

[2] Consumer Data Rule 4.18. A 'CDR receipt' is a notice that sets out certain details of the consent to collect and use, the name of each data holder that the consumer has consented to the collection of CDR data from and any other information the accredited person provided to the consumer when asking for their consent. A copy of the CDR receipt may be included in the consumer's consumer dashboard.

This will encourage engagement and maximise the chance that a consumer is informed (given that a consumer may not actively check their consumer dashboard).

Who does Privacy Safeguard 5 apply to?

5.7 Privacy Safeguard 5 applies to accredited persons. It does not apply to data holders or designated gateways.

5.8 Data holders and designated gateways must ensure that they are adhering to their obligations under the *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles (APPs), including APP 3 and APP 5, when collecting personal information.

How does Privacy Safeguard 5 interact with the Privacy Act and APP 5?

5.9 It is important to understand how Privacy Safeguard 5 interacts with the Privacy Act and the APPs.[3]

5.10 Like Privacy Safeguard 5, APP 5 outlines when an entity that collects information must tell an individual about certain matters.

5.11 The Privacy Act and APP 5 provide protection where collected data is personal information but not CDR data.

Summary of application of Privacy Safeguard 5 by CDR entity

CDR entity	Privacy principle that applies
Accredited person	**Privacy Safeguard 5** APP 5 applies in parallel to Privacy Safeguard 5. Privacy Safeguard 5 applies instead of APP 5 when notifying consumers of the collection of CDR data. APP 5 will continue to apply to any personal information handled by the accredited person that is not CDR data.
Accredited data recipient	**Privacy Safeguard 5** Privacy Safeguard 5 applies instead of APP 5, meaning APP 5 will not apply to CDR data that an accredited data recipient receives through the CDR regime. APP 5 will continue to apply to any personal information handled by the accredited data recipient that is not CDR data.

[3] The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies.

CDR entity	Privacy principle that applies
Designated gateway	**Australian Privacy Principle 5** Privacy Safeguard 5 does not apply to a designated gateway.
Data holder	**Australian Privacy Principle 5** Privacy Safeguard 5 does not apply to a data holder.

How must notification be given?

5.12 Accredited persons must provide notification by updating the consumer dashboard of a consumer.

5.13 Further guidance about the consumer dashboard is set out in Chapter B (Key concepts) and Chapter C (Consent).

Who must be notified?

5.14 The accredited person must notify the consumer who gave the accredited person consent to collect the CDR data.

5.15 There may be more than one CDR consumer to whom a set of CDR data applies, for example, where there are joint account holders of a bank account. In this example, the accredited person is only required by the Consumer Data Rule 7.4 to update the consumer dashboard of the requesting joint account holder.

When must notification be given?

5.16 An accredited person must notify the consumer as soon as practicable after the CDR data is collected.

5.17 Notification should generally occur in as close to real time as possible (i.e. as close to the time of first collection as possible).

5.18 However, whether the notification occurs 'as soon as practicable' will depend on the circumstances, and the following factors may be relevant:

- time and cost involved
- technical matters
- any individual needs of the consumer (for example, additional steps required to make the content accessible).

5.19 It is the responsibility of the accredited person to be able to justify any delay in notification.

5.20 An accredited person is not excused from providing notification by reason only that it would be inconvenient, time consuming or costly to do so.

Risk point: Delays to notification of collection may result in confusion for a CDR consumer and non-compliance for an accredited person.

Privacy tip: Accredited persons should ensure that they have systems and processes in place to allow for real-time and automated notification.

What matters must be included in the notification?

5.21 The minimum matters that must be noted in a CDR consumer's consumer dashboard are:

- what CDR data was collected
- when the CDR data was collected
- the data holder of the CDR data.[4]

What CDR data was collected

5.22 The accredited person must ensure CDR data is described with enough specificity to allow the CDR consumer to easily understand what CDR data was collected.

5.23 An accredited person should have regard to the Data Language Standards when implementing this requirement.[5] This will aid consumer comprehension by ensuring consistency between how CDR data was described in the consent-seeking process and how CDR data is described in the consumer dashboard.

When the CDR data was collected

Where the CDR data was collected on a 'one-off' basis:[6]

5.24 The accredited person should include the date on which the CDR data was collected.

5.25 Where CDR data was collected at different times, the accredited person should include the date on which each dataset was collected.

5.26 Examples of where an accredited person collects CDR data at different times include where:

- the CDR data is held by more than one data holder, and those data holders disclose CDR data to the accredited person on different dates
- the CDR data is held by one data holder, and that data holder discloses CDR data to the accredited person on different dates

[4] Consumer Data Rule 7.4.

[5] The Data Language Standards can be found within the Consumer Experience Guidelines. They provide descriptions of the types of data to be used by accredited data recipients when making and responding to requests. Adherence to the Data Language Standards will help ensure there is a consistent interpretation and description of the consumer data that will be shared in the CDR regime.

[6] This is where the accredited person indicated the CDR data would be collected on a single occasion and used over a specified period of time (Consumer Data Rule 4.11(1)(b)(i)).

Where the CDR data was collected and will continue to be collected over a period of time:[7]

5.27 The accredited person should include the date range between which CDR data will be collected, with the starting date being the date on which the CDR data was first collected.

5.28 The accredited person should, in addition to stating the time period for collection, note the frequency of data collection for ongoing collection.

5.29 The accredited person should have regard to the Consumer Experience Guidelines when implementing this requirement.[8]

The data holder of the CDR data

5.30 Where an accredited person is authorised to make consumer data requests on the CDR consumer's behalf to multiple data holders, an accredited person should indicate the CDR data that relates to each data holder.

5.31 An accredited person must have regard to the Consumer Experience Guidelines relating to the data recipient dashboard landing page when implementing this requirement.

Other notification requirements under the Consumer Data Rules

5.32 In addition to the Privacy Safeguard 5 notification requirements in relation to collection, there are other notification requirements relating to consent that must be complied with:

- providing CDR receipts to the CDR consumer (Rule 4.18)[9]
- general obligation to update the consumer dashboard (Consumer Data Rule 4.19)
- ongoing notification requirements for CDR consumer consents (Rule 4.20).

How does Privacy Safeguard 5 interact with other Privacy Safeguards?

5.33 CDR participants must comply with Privacy Safeguard 1 by taking reasonable steps to implement practices, procedures and systems that will ensure they comply with the CDR legislation, including Privacy Safeguard 5. See Chapter 1 (Privacy Safeguard 1).

5.34 The Privacy Safeguard 5 requirement to notify consumers about the collection of their CDR data relates to all CDR data collected under Privacy Safeguard 3 (see Chapter 3 (Privacy Safeguard 3)).

[7] This is where the accredited person indicated the CDR data would be collected and used over a specified period of time (Consumer Data Rule 4.11(1)(b)(ii)).

[8] See the examples of implementation of the data recipient dashboard regarding 'data sharing arrangement' in the Consumer Experience Guidelines.

[9] A 'CDR receipt' is a notice that sets out certain details of the consent to collect and use, the name of each data holder that the consumer has consented to the collection of CDR data from and any other information the accredited person provided to the consumer when asking for their consent. A copy of the CDR receipt may be included in the consumer's consumer dashboard.

5.35 While Privacy Safeguard 5 only relates to notification on *collection*, Privacy Safeguard 10 sets out when CDR participants must notify consumers about the *disclosure* of their CDR data. See Chapter 10 (Privacy Safeguard 10).