Chapter 5:

Privacy Safeguard 5 —

Notifying of the collection of CDR data

Version 1.0, February 2020

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 the consumer's 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 of the collection by taking the steps identified in the consumer data rules (CDR Rules).[1]

5.2 The notification must:

- be given to the consumer at whose request the CDR data was collected
- cover the matters set out in the CDR Rules, and
- be given at or before the time specified in the CDR Rules.

5.3 Under CDR Rule 7.4, an accredited person must notify the consumer by updating the consumer's dashboard to include certain matters as soon as practicable after CDR data is collected from a data holder.

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.

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.

5.9 Data holders must also ensure they adhere to Privacy Safeguard 10, which requires them to notify consumers of the disclosure of their CDR data.

[1] Section 56EH of the Competition and Consumer Act.

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

5.10 It is important to understand how Privacy Safeguard 5 interacts with the Privacy Act and the APPs.[2]

5.11 Like Privacy Safeguard 5, APP 5 outlines when an entity must notify of collection, as well as what information must be included in the notification.

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

CDR entity	Privacy protections that apply in the CDR context
Accredited person / accredited data recipient	**Privacy Safeguard 5** Privacy Safeguard 5 applies instead of APP 5 to CDR data that has been collected by an accredited data recipient in accordance with Privacy Safeguard 3. APP 5 will continue to apply to: • personal information collected that is not CDR data, [3] and • CDR data that is not collected in accordance with Privacy Safeguard 3.[4]
Designated gateway	**APP 5** Privacy Safeguard 5 does not apply to a designated gateway.
Data holder	**APP 5** Privacy Safeguard 5 does not apply to a data holder.

How must notification be given?

5.13 An accredited person must provide the notification by updating the consumer dashboard for a consumer to include the matters discussed in paragraphs 5.23 to 5.36 as soon as practicable after CDR data relating to that consumer is collected.[5]

5.14 The consumer dashboard is an online service that must be provided by an accredited person to each consumer who has provided consent to the collection and use of their CDR data. Accredited persons are required by CDR Rule 1.14 to include within the consumer's

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

[3] 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.

[4] With the exception of personal information that is also CDR data received by an accredited person who is a small business operator under the Privacy Act (see section 6E(1D) of the Privacy Act).

[5] CDR Rule 7.4.

dashboard certain details of each consent to collect and use CDR data that has been given by the consumer. [6]

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

Who must be notified?

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

5.17 There may be more than one 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 required by CDR Rule 7.4 to update only the consumer dashboard of the requesting joint account holder.

When must notification be given?

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

5.19 As a matter of best practice, notification should generally occur in as close to real time as possible (for example, in relation to ongoing collection, as close to the time of first collection as possible).

5.20 The test of practicability is an objective test. It is the responsibility of the accredited person to be able to justify any delay in notification.

5.21 In determining what is 'as soon as practicable', the accredited person may take the following factors into account:

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

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

[6] This includes the CDR data to which the consent relates and when the consent will expire.

Risk point: Delays in notification of collection may result in confusion for a 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?

5.23 The minimum matters that must be included in the notification, and provided via the consumer's dashboard, are:

- what CDR data was collected
- when the CDR data was collected, and
- the data holder of the CDR data.[7]

5.24 Accredited persons should provide information about these matters clearly and simply, but also with enough specificity to be meaningful for the consumer. How much information is required may differ depending on the circumstances.

5.25 Guidance on each of the minimum matters is provided below.

Risk point: Consumers may not read or understand a notification where the details of collection are complex.

Privacy tip: An accredited person should ensure that the notification is as simple and easy to understand as possible. To do this, an accredited person should consider a range of factors when formulating a notification, such as:

- what the data is being used for
- the language used (including the level of detail), and
- the presentation of the information (e.g. layout, format and any visual aids used). For more complex notifications, the accredited person could consider providing a condensed summary of key matters in the notification and linking to more comprehensive information or, where it may assist the consumer, a full log of access.

What CDR data was collected

5.26 The accredited person must notify the consumer of what CDR data was collected.

5.27 In doing so, the accredited person should ensure CDR data is described in a manner that allows the consumer to easily understand what CDR data was collected.

[7] CDR Rule 7.4.

5.28 The accredited person must use the Data Language Standards when describing what CDR data was collected.[8] 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

5.29 The accredited person must notify the consumer of when the CDR data was collected.

'Once-off' collection[9]

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

Ongoing collection[10]

5.31 The accredited person should, at a minimum, include the date range in which CDR data will be collected, with the starting date being the date on which the CDR data was first collected, and the end date being the date on which the accredited person will make its final collection. This end date might not necessarily be the same as the date consent expires.

5.32 Where an accredited person is unsure of the end date they may put the date consent expires, but must update the end date as soon as practicable after it becomes known.[11]

5.33 The accredited person should, in addition to stating the date range for collection, note:

- what activity will trigger ongoing collection (e.g. 'We'll continue to collect your transaction details from [data holder] each time you make a transaction'), and / or
- if known, the frequency of any ongoing collection (e.g. 'We'll continue to collect your transaction details from [data holder] up to three times per day').

The data holder of the CDR data

5.34 In its notification to the consumer, the accredited person must indicate from whom the CDR data was collected. There may be multiple data holders.

Example

Watson and Co is an accredited person that provides a budgeting service through its Watspend application. Watspend uses transaction details to provide real-time, accurate budgeting recommendations to its users. *cont*

[8] The Data Language Standards are contained within the Consumer Experience Standards. 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 is mandatory and will help ensure there is a consistent interpretation and description of the consumer data that will be shared in the CDR regime. See s 56FA of the Competition and Consumer Act and CDR Rule 8.11.

[9] 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 (CDR Rule 4.11(1)(b)(i)).

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

[11] CDR Rule 4.19 requires an accredited person to update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

Zoe wants to use the Watspend application, so provides Watson and Co with a valid request to collect her transaction details from Bank Belle. Zoe provides consent for Watson and Co to collect and use her transaction details for the provision of the Watspend service from 1 July 2020 to 1 January 2021.

Watson and Co collect Zoe's transaction details from Bank Belle on 1 July 2020.

Watson and Co updates Zoe's consumer dashboard on 1 July 2020 to include the following notification statement:

We collected your transaction details from Bank Belle on 01.07.20. We'll continue to collect your transaction details from Bank Belle each time you make a transaction until 01.01.21.

The above statement is an example of how Watson and Co could notify Zoe of the collection of her CDR data in accordance with CDR Rule 7.4.

Other notification requirements under the CDR Rules

5.35 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 consumer (CDR Rule 4.18)
- general obligation to update the consumer dashboard (CDR Rule 4.19), and
- ongoing notification requirements for consumer consents (CDR Rule 4.20).

5.36 For further information regarding these notification requirements, see Chapter C (Consent).

How does Privacy Safeguard 5 interact with the other privacy safeguards?

5.37 The requirement in Privacy Safeguard 5 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)).

5.38 While Privacy Safeguard 5 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).