Chapter 5:

Privacy Safeguard 5 —

Notifying of the collection of CDR data

Consultation draft, September 2022

OAIC

Contents

Key points 3
What does Privacy Safeguard 5 say? 3
Why is this important? 3
Who does Privacy Safeguard 5 apply to? 3
How Privacy Safeguard 5 interacts with the Privacy Act 4
How must notification be given? 5
Who must be notified? 6
When must notification be given? 6
What matters must be included in the notification? 7
What CDR data was collected 8
When the CDR data was collected 8
From whom the CDR data was collected 9
Sponsorship arrangements 9
Other notification requirements under the CDR Rules 10
How does Privacy Safeguard 5 interact with the other privacy safeguards? 10

Key points

- An accredited data recipient of a consumer's CDR data must notify ~~that~~the consumer when they collect the data.
- This notification must occur through the consumer's dashboard as soon as practicable after the accredited data recipient has received the consumer's CDR data.

What does Privacy Safeguard 5 say?

5.1 If an accredited data recipient collected a consumer's CDR data under Privacy Safeguard 3, the accredited data recipient must notify that 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 rule 7.4 of the CDR ~~Rule 7.4~~Rules, an accredited data recipient of a consumer's CDR data 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 or accredited data recipient. Where the CDR data was collected by a sponsor on behalf of an affiliate under a sponsorship arrangement, the sponsor and affiliate may choose which of them will update the dashboard.[2]

5.4 For information about the concept of 'collects' refer to Chapter B (Key concepts). For information about seeking to collect CDR data under Privacy Safeguard 3, see Chapter 3 (Privacy Safeguard 3).

Why is this important?

5.5 Notification of collection of CDR data is an integral element of the CDR ~~regime~~system 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 accredited data recipients.

Who does Privacy Safeguard 5 apply to?

5.7 Privacy Safeguard 5 applies to accredited data recipients of a consumer's CDR data. It does not apply to data holders or designated gateways.

---

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

[2] CDR Rules, paragraph 7.4(2)(a).

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),~~APPs, including APP 3 and APP 5, when collecting personal information.

5.9 Data holders must also ensure they adhere to Privacy Safeguard 10,[3] which requires them to notify consumers of the disclosure of their CDR data.

5.10 Where:

- a sponsor collects a consumer's CDR data on behalf of an affiliate under a sponsorship arrangement, the sponsor and affiliate may decide which of them will be responsible for notifying the consumer of that collection under Privacy Safeguard 5[4]
- a CDR principal collects a consumer's CDR data on behalf of a CDR representative under a CDR representative arrangement, the CDR principal must notify the consumer of that collection under Privacy Safeguard 5 (but may delegate this responsibility to their CDR representative)[5]
- an outsourced service provider collects a consumer's CDR data on behalf of a principal under a CDR outsourcing arrangement, the principal must notify the consumer of that collection under Privacy Safeguard 5.[6]

How Privacy Safeguard 5 interacts with the Privacy Act

~~5.10~~5.11 It is important to understand how Privacy Safeguard 5 interacts with the Privacy Act and the APPs.[7]

~~5.11~~5.12 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~~5.13 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 data recipient	**Privacy Safeguard 5** For accredited data recipients of a consumer's CDR data, the Privacy Safeguard 5 notification requirements apply to any of that

[3] See Chapter 10: Privacy Safeguard 10 — Notifying of the disclosure of CDR data for more information.

[4] CDR Rules, subrule 7.4(2).

[5] CDR Rules, subrule 1.14(5).

[6] CDR Rules, rule 7.4(1) Note 2 and subrule 1.16(2). Subrule 1.16(2) provides that where a principal under a CDR outsourcing arrangement uses an accredited person to collect CDR data on its behalf, rule 7.4 applies only in relation to the principal. Where a collecting OSP is not an accredited person, the principal must still notify the consumer of the collection under Privacy Safeguard 5. Additionally, if an OSP uses other OSPs to satisfy a consumer data request, the original principal must notify the consumer of the collection under Privacy Safeguard 5. For information on 'CDR outsourcing arrangements', see Chapter B (Key concepts).

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

CDR entity	Privacy protections that apply in the CDR context
	consumer's CDR data that has been collected in accordance with Privacy Safeguard 3.[8] APP 5 does not apply in relation to that CDR data.[9]
Designated gateway	**APP 5** Privacy Safeguard 5 does not apply to a designated gateway.
Data holder[10]	**APP 5** Privacy Safeguard 5 does not apply to a data holder.

How must notification be given?

5.135.14 An accredited data recipient must provide the notification by updating ~~the~~a consumer's consumer dashboard ~~for a consumer~~ to include the matters discussed in paragraphs ~~5.24~~5.25 to ~~5.35~~5.38 as soon as practicable after collecting CDR data relating to that consumer.[11]

5.145.15 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, use and/or disclosure of their CDR data. Accredited persons are required by CDR Rule 1.14 to include within the consumer's dashboard certain details of each consent to collect, use and disclose CDR data that has been given by the consumer. ~~12~~13 If a CDR principal makes a consumer data request at the request of a CDR representative under a CDR representative

[8] Privacy Safeguard 5 applies from the point when the accredited person becomes an accredited data recipient of the CDR data. An accredited person becomes an accredited data recipient for CDR data when:

- CDR data is held by (or on behalf of) the person
- the CDR data, or any other CDR data from which it was directly or indirectly derived, was disclosed to the person under the ~~consumer data rules~~CDR Rules, and
- the person is neither a data holder, nor a designated gateway, for the first mentioned CDR data. See ~~s 56EK of the~~ Competition and Consumer Act, section 56AK.

[9] The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data ~~– s 56EC(4)(a) of the~~: Competition and Consumer Act~~.~~, paragraph 56EC(4)(a). However, ~~s~~subsection 56EC(4) does not affect how the APPs apply to accredited persons and accredited data recipients who are APP entities, in relation to the handling of personal information outside the CDR system. (Note: 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~~.) Section~~, subsection 6E(1D).) Subsection 56EC(4) of the Competition and Consumer Act also does not affect how the APPs apply to an accredited person who does not become an accredited data recipient of the CDR data (other than for Privacy Safeguards 1 – 4). See ~~s 56EC(5)(aa) of the~~ Competition and Consumer Act~~.~~, paragraph 56EC(5)(aa).

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

[11] CDR ~~Rule~~Rules, subrule 7.4~~.~~(1).

~~[12] This includes the CDR data to which the consents relate and when the consents will expire. For further information regarding the requirements for an accredited person's consumer dashboard, see CDR Rule 1.14, Chapter C (Consent) and Chapter B (Key concepts).~~

[13] This includes the CDR data to which the consents relate and when the consents will expire. For further information regarding the requirements for an accredited person's consumer dashboard, see CDR Rules, rule 1.14, Chapter C (Consent) and Chapter B (Key concepts).

arrangement, the CDR principal may arrange for the CDR representative to provide the consumer dashboard and to notify the consumer on its behalf.[14]

~~5.15 Where an accredited data recipient collected CDR data on behalf of another accredited person (the 'principal') under a CDR outsourcing arrangement, only the principal needs to notify the relevant consumer/s of collection by updating the relevant dashboard/s.[15]~~

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

Who must be notified?

5.17 The accredited data recipient must notify the consumer who gave the consent to collect the CDR data.

5.18 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~~an account. In this example, the accredited data recipient is required by CDR Rule 7.4 to update only the consumer dashboard of the requesting joint account holder.[16]

When must notification be given?

5.19 An accredited data recipient must notify the consumer as soon as practicable after the CDR data is collected.

5.20 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).

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

5.22 In determining what is 'as soon as practicable', the accredited data recipient 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).

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

5.24 Notifications about collections should remain on a consumer's consumer dashboard, even where the relevant consent has expired.

---

[14] CDR Rules, subrule 1.14(5).

[15] ~~CDR Rule 1.16(2)(a). For information on 'CDR outsourcing arrangements', see Chapter B (Key concepts).~~

[16] Different dashboard obligations apply to data holders: see rule 4A.13 of the CDR Rules for further information.

Risk point: Delays in notification of collection may result in confusion for a consumer, and non-compliance for an accredited data recipient.

Privacy tip: Accredited data recipients 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?

~~5.24~~5.25 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 or accredited data recipient from which the CDR data was collected, and
- where applicable, that the data was collected by a sponsor on behalf of an affiliate.[17]

~~5.25~~5.26 Accredited data recipients 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.

~~5.26~~5.27 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 data recipient should ensure that the notification is as simple and easy to understand as possible. To do this, an accredited data recipient 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 data recipient 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.

[17] CDR ~~Rule~~Rules, subrules 7.4~~.~~(1) and (2).

What CDR data was collected

~~5.27~~5.28 The accredited data recipient must notify the consumer of what CDR data was collected.[18]

~~5.28~~5.29 In doing so, the accredited data recipient should ensure CDR data is described in a manner that allows the consumer to easily understand what CDR data was collected.

~~5.29~~5.30 The accredited data recipient must use the Data Language Standards when describing what CDR data was collected.[19] 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

~~5.30~~5.31 The accredited data recipient must notify the consumer of when the CDR data was collected.[20]

'One-off' collection[21]

~~5.31~~5.32 The accredited data recipient should include the date on which the CDR data was collected.

Ongoing collection[22]

~~5.32~~5.33 The accredited data recipient 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 the consent to collect expires.

~~5.33~~5.34 Where an accredited data recipient is unsure of the end date, they may put the date the consent to collect expires, but must update the end date as soon as practicable after it becomes known.[23]

~~5.34~~5.35 The accredited data recipient 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 [e.g. data holder] each time you make a transaction'), and / or

---

[18] CDR Rules, subrule 7.4(1)(a).

[19] The Data Language Standards are contained within the Consumer Experience Standards~~.~~: Data Language Standards: Common. 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~~system. See ~~s 56FA of the~~ Competition and Consumer Act~~.~~, section 56FA and CDR ~~Rule~~Rules, rule 8.11.

[20] CDR Rules, paragraph 7.4(1)(b). Note this requirement refers to dates of collection, not the date that consent was provided or expired.

[21] This is where the accredited person indicated the CDR data would be collected on a single occasion (CDR ~~Rule~~Rules, paragraph 4.11(1)(b)(i)).

[22] This is where the accredited person indicated the CDR data would be collected over a specified period of time (CDR ~~Rule~~Rules, paragraph 4.11(1)(b)(ii)).

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

- if known, the frequency of any ongoing collection (e.g. 'We'll continue to collect your transaction details from [e.g. data holder] up to ~~three~~3 times per day').

5.36 If collection of particular CDR data stops (because a collection consent or disclosure authorisation is withdrawn for that data), but collection later recommences under an amended consent or authorisation, then the collection is not continuous and 2 separate date ranges should be included.

From whom the CDR data was collected

~~5.35~~5.37 In its notification to the consumer, the accredited data recipient must indicate from whom the CDR data was collected. There may be multiple data holders and/or accredited data recipients from whom the CDR data was collected.

Sponsorship arrangements

5.38 Where the CDR data was collected by a sponsor on behalf of an affiliate under a sponsorship arrangement:

- the sponsor and the affiliate may choose which of them will notify the consumer, and
- the notification to the consumer must identify that the CDR data was collected by the sponsor on behalf of the affiliate.[24]

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.

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~~collects Zoe's transaction details from Bank Belle on 1 July 2020 and becomes an accredited data recipient for this CDR data.

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.

[24] CDR Rules, subrule 7.4(2).

Other notification requirements under the CDR Rules

~~5.36~~5.39 In addition to the Privacy Safeguard 5 notification requirements in relation to collection, there are other notification requirements relating to consent that accredited persons must ~~be complied~~comply with:[25]

- providing CDR receipts to the consumer (~~CDR Rule~~rule 4.18 of the CDR Rules)
- notification requirements where certain consents expire or are amended (~~CDR Rules~~rules 4.18A, 4.18B and 4.18C of the CDR Rules)
- general obligation to update the consumer dashboard (~~CDR Rule~~rule 4.19 of the CDR Rules), and
- ongoing notification requirements for consents to collect and use (~~CDR Rule~~rule 4.20 of the CDR Rules).

5.40 Where CDR data has been collected under a sponsorship arrangement, the sponsor and affiliate may choose which will give these notices.[26]

~~5.37~~5.41 For further information regarding these notification requirements, see Chapter C (Consent).

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

~~5.38~~5.42 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)).

~~5.39~~5.43 While Privacy Safeguard 5 relates to notification on *collection*, Privacy Safeguard 10 sets out when an accredited data recipient and data holder must notify consumers about the *disclosure* of their CDR data. See Chapter 10 (Privacy Safeguard 10).

[25] For an accredited data recipient who collected CDR data on behalf of a principal in a CDR outsourcing arrangement, note the effect of ~~CDR Rule~~subrule 1.7(5) of the CDR Rules which provides that, in the CDR Rules, 'unless the contrary intention appears, a reference to an accredited person making a consumer data request, collecting CDR data, obtaining consents, providing a consumer dashboard, or using or disclosing CDR data does not include a reference to an accredited person doing those things on behalf of a principal in its capacity as the provider in an outsourced service arrangement, in accordance with the arrangement'.

For information on 'CDR outsourcing arrangements', see Chapter B (Key concepts), 'Outsourced service provider'.

[26] CDR Rules, rule 4.20A.