

Chapter 10:
Privacy Safeguard 10 —
Notifying of the disclosure of CDR data

Version 3.0, June 2021

Contents

Key points	3
What does Privacy Safeguard 10 say?	3
Why is it important?	3
Who does Privacy Safeguard 10 apply to?	3
How Privacy Safeguard 10 interacts with the Privacy Act	4
Who must be notified?	4
How must notification be given?	5
When must notification be given?	6
What matters must be included in the notification?	7
What CDR data was disclosed	7
When the CDR data was disclosed	8
To whom the CDR data was disclosed	8
Other notification requirements under the CDR Rules	9
Disclosure to a designated gateway	10
Interaction with other Privacy Safeguards	10

Key points

- Where a data holder or accredited data recipient of a consumer's CDR data discloses that data to an accredited person, they must notify the consumer by updating the consumer dashboard.
- The consumer data rules (CDR Rules) set out the matters that must be included in this notification.

What does Privacy Safeguard 10 say?

- 10.1 Where a data holder is required or authorised under the CDR Rules to disclose CDR data, they must notify the consumer by taking the steps identified in the CDR Rules.¹
- 10.2 Where an accredited data recipient of a consumer's CDR data discloses CDR data, they must notify that consumer by taking the steps identified in the CDR Rules.²
- 10.3 The notification must:
- be given to those consumers that the CDR Rules require to be notified
 - cover the matters set out in the CDR Rules, and
 - be given at or before the time specified in the CDR Rules.
- 10.4 Under CDR Rule 7.9, data holders and accredited data recipients of a consumer's CDR data must notify the consumer by updating each relevant consumer dashboard to include certain matters as set out in that Rule as soon as practicable after CDR data is disclosed to an accredited person.

Why is it important?

- 10.5 Notification of disclosure of CDR data is an integral element of the CDR regime, as it provides confirmation to consumers that their CDR data has been disclosed in response to a consumer data request.
- 10.6 This ensures consumers are informed when their CDR data is disclosed and builds trust between consumers, data holders and accredited data recipients.

Who does Privacy Safeguard 10 apply to?

- 10.7 Privacy Safeguard 10 applies to data holders and accredited data recipients of CDR data. It does not apply to designated gateways.

¹ Section 56EM(1) of the Competition and Consumer Act. For further information on 'required or authorised to use or disclose CDR data under the CDR Rules', refer to [Chapter B \(Key concepts\)](#).

² Section 56EM(2) of the Competition and Consumer Act.

How Privacy Safeguard 10 interacts with the Privacy Act

For data holders

- 10.8 Data holders must comply with Privacy Safeguard 10 when they are required or authorised to disclose CDR data under the CDR Rules.
- 10.9 There is no corresponding obligation under the *Privacy Act 1988* (the Privacy Act) or the Australian Privacy Principles (APPs) to notify an individual of the disclosure of their personal information.
- 10.10 However, APP 5 will continue to apply in relation to the notification of the collection of CDR data that is also personal information.³

For accredited data recipients

- 10.11 For an accredited data recipient of a consumer's CDR data, Privacy Safeguard 10 applies whenever they disclose that consumer's data.
- 10.12 The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data.⁴

Who must be notified?

For data holders

- 10.13 The data holder must notify each of the consumers for the CDR data that has been disclosed.⁵
- 10.14 There may be more than one consumer for the CDR data. In the banking sector, a key example is CDR data relating to a joint account. In this case, the data holder must notify each of the requesting and non-requesting joint account holders. However, a data holder will not be required to notify the non-requesting joint account holder/s where the data holder considers this necessary to prevent physical or financial harm or abuse.⁶

³ For example, the obligations in APP 5.2 (f), (i) and (j) to notify individuals of the situations in which their personal information may be disclosed in future.

⁴ Section 56EC(4)(a) of the Competition and Consumer Act. However, s 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 56EC(4) 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.

⁵ Section 56EM(1)(b) of the Competition and Consumer Act and CDR Rule 7.9(1).

⁶ CDR Rule 7.9 and clause 4.14(4) of Schedule 3 to the CDR Rules. Clause 4.14(4) of Schedule 3 provides that the data holder may decline to provide a relevant account holder with a consumer dashboard or update the consumer dashboard if the data holder considers it necessary to do either in order to prevent physical or financial harm or abuse.

10.15 This exception to notification is to accommodate existing procedures a data holder may have to protect consumers, for example particular arrangements relating to consumers that may be experiencing family violence.

10.16 Where the CDR data disclosed relates to an account with a secondary user,⁷ and the secondary user is also a consumer for the CDR data,⁸ the data holder must notify both the account holder and secondary user.⁹

10.17 Where the CDR data disclosed relates to a non-individual consumer or is in relation to a partnership account, the data holder must notify the relevant nominated representative.¹⁰

For accredited data recipients

10.18 The accredited data recipient must notify the consumer who provided the disclosure consent.¹¹

How must notification be given?

For data holders

10.19 A data holder must provide the notification by updating the consumer dashboard for a consumer (and, if applicable, the dashboard of the other joint account holder/s)¹² to include the matters discussed in paragraphs 10.31 to 10.42 as soon as practicable after CDR data relating to that consumer is disclosed.¹³

⁷ A person is a secondary user for an account with a data holder if the person has ‘account privileges’ in relation to the account, and the account holder has given the data holder an instruction to treat the person as a secondary user for the purposes of the CDR Rules (CDR Rule 1.7). ‘Account privileges’ for the banking sector are defined in clause 2.2 of Schedule 3 to the CDR Rules.

⁸ For a person to be a ‘CDR consumer’ that person must be identifiable, or ‘reasonably identifiable’, from the CDR data or other information held by the relevant entity (i.e. the data holder, accredited data recipient, or person holding data on their behalf) (s 56AI(3)(c) of the Competition and Consumer Act). See Chapter B (Key concepts) of the CDR Privacy Safeguard Guidelines for the full meaning of CDR consumer.

⁹ Any provisions in the CDR Rules which impose obligations on data holders in relation to secondary users only apply to initial data holders in respect of NAB, CBA, ANZ, Westpac branded products on and from 1 November 2021 (and for all other data holders, on and from 1 November 2022): see cl 6.7 of Schedule 3 to the CDR Rules.

¹⁰ A ‘nominated representative’ is the individual nominated by the non-individual consumer under CDR Rules 1.13(c)(i) or 1.13(d)(i) who is able to give, amend and manage authorisations to disclose CDR data on behalf of the non-individual consumer. There may be more than one nominated representative.

Note that any provisions in the CDR Rules which impose obligations on data holders in relation to consumers that are not individuals, nominated representatives or partnerships only apply to initial data holders in respect of NAB, CBA, ANZ, Westpac branded products on and from 1 November 2021 (and for all other data holders, on and from 1 November 2022): see cl 6.7 of Schedule 3 to the CDR Rules.

¹¹ A disclosure consent is a consent given by a consumer for the accredited data recipient to disclose CDR data to an accredited person: in response to consumer data request (an ‘AP disclosure consent’), or for the purposes of direct marketing: CDR Rule 1.10A(1)(c). For further information, see Chapter C (Consent).

¹² Where the CDR data disclosed relates to a joint account, the data holder must provide each relevant account holder with a consumer dashboard, and notify each of the joint account holders by updating their consumer dashboards to include those same matters as soon as practicable after the CDR data is disclosed. However, the data holder may decline to provide a relevant account holder with a consumer dashboard or update the consumer dashboard if the data holder considers it necessary to do either in order to prevent physical or financial harm or abuse. See clause 4.14 of Schedule 3 to the CDR Rules.

¹³ CDR Rule 7.9.

10.20 The data holder's consumer dashboard is an online service that must be provided by a data holder to each consumer (and, if applicable, the other joint account holder/s)¹⁴ where a consumer data request has been made on their behalf by an accredited person. Data holders must include within the dashboard certain details of each authorisation to disclose CDR data that has been given by the consumer.¹⁵

10.21 Further guidance about the data holder's consumer dashboard is set out in [Chapter B \(Key concepts\)](#) and the [Guide to privacy for data holders](#).

For accredited data recipients

10.22 An accredited data recipient must provide the notification by updating the consumer dashboard for the consumer who provided the disclosure consent.¹⁶

10.23 The accredited data recipient's consumer dashboard is an online service that must be provided by an accredited data recipient to each consumer who has provided a consent in relation to their CDR data. Accredited data recipients must include in the dashboard certain details of each consent that has been given by the consumer.¹⁷

10.24 Where an accredited data recipient disclosed CDR data that was collected on behalf of another accredited person (the 'principal') under a CDR outsourcing arrangement, only the principal needs to notify the relevant consumer/s by updating the relevant dashboard.¹⁸

10.25 Further guidance about the accredited data recipient's consumer dashboard is set out in [Chapter B \(Key concepts\)](#) and [Chapter C \(Consent\)](#).

When must notification be given?

10.26 Data holders and accredited data recipients must notify the consumer/s as soon as practicable after the CDR data is disclosed.¹⁹

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

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

¹⁴ Where the CDR data disclosed relates to a joint account, the data holder must provide each relevant account holder with a consumer dashboard, except where the data holder considers it necessary to decline to provide a relevant account holder with a dashboard in order to prevent physical or financial harm or abuse. See clause 4.14(4) of Schedule 3 to the CDR Rules.

¹⁵ The requirements are outlined in CDR Rule 1.15, and include requirements to provide details of the CDR data to which the authorisation relates and when the authorisation will expire.

¹⁶ A disclosure consent is a consent given by a consumer for the accredited data recipient to disclose CDR data to an accredited person: in response to consumer data request (an 'AP disclosure consent'), or for the purposes of direct marketing: CDR Rule 1.10A(1)(c). For further information, see Chapter C (Consent).

¹⁷ The requirements are outlined in CDR Rule 1.14, and include requirements to provide details of the CDR data to which each consent relates and when each consent will expire.

¹⁸ CDR Rule 1.16(2)(a). For information on 'CDR outsourcing arrangements', see [Chapter B \(Key concepts\)](#).

¹⁹ CDR Rules 7.9(1) and 7.9(2).

10.29 In determining what is ‘as soon as practicable’, data holders and accredited data recipients may take the following factors into account:

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

10.30 Data holders and accredited data recipients are not excused from providing prompt notification by reason only that it would be inconvenient, time consuming, or costly to do so.

What matters must be included in the notification?

10.31 The minimum matters that must be included by data holders and accredited data recipients in the notification, and provided via the consumer’s dashboard are:

- what CDR data was disclosed
- when the CDR data was disclosed, and
- the accredited person to whom the CDR data was disclosed.²⁰

10.32 Data holders and 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.

10.33 Guidance on each of the minimum matters follows.

Risk point: Consumers may not read or understand a notification if it is complex.

Privacy tip: Data holders and accredited data recipients should ensure that the notification is as simple and easy to understand as possible. To do this, entities should consider a range of factors when formulating a notification, such as:

- the audience
- 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, entities could consider providing a condensed summary of key matters in the notification and linking to a more comprehensive summary or, where it may assist the consumer, a full log of disclosure.

What CDR data was disclosed

10.34 Data holders and accredited data recipients must notify the consumer of what CDR data was disclosed.

²⁰ CDR Rules 7.9(1) and 7.9(2). The accredited person needs to be identified in accordance with any entry on the Register of Accredited Persons specified as being for that purpose.

10.35 In doing so, the entity should ensure the CDR data is described in a manner that allows the consumer to easily understand what CDR data was disclosed.

10.36 Data holders and accredited data recipients must use the Data Language Standards when describing what CDR data was disclosed.²¹ This will aid consumer comprehension by ensuring consistency between how CDR data was described in the authorisation/consent-seeking processes and how CDR data is described in the consumer dashboard.

When the CDR data was disclosed

10.37 Data holders and accredited data recipients must notify the consumer of when the CDR data was disclosed.

*‘One-off’ disclosure:*²²

10.38 The entity should include the date on which the CDR data was disclosed.

*Ongoing disclosure:*²³

10.39 The entity should, at a minimum, include the date range in which CDR data will be disclosed, with the starting date being the date on which the CDR data was first disclosed, and the end date being the date on which the entity will make its final disclosure. This end date might not necessarily be the same as the date that the authorisation (in the case of a data holder) or disclosure consent (in the case of an accredited data recipient) expires.

10.40 Where the entity is unsure of the end date they may put the date the authorisation or disclosure consent expires, but must update the end date as soon as practicable after it becomes known.²⁴

To whom the CDR data was disclosed

10.41 In its notification to the consumer, the entity must indicate the accredited person to whom the CDR data was disclosed.

10.42 The accredited person must be described in accordance with any entry on the Register of Accredited Persons specified as being for that purpose.²⁵

²¹ The Data Language Standards are contained within the Consumer Experience Guidelines. They provide descriptions of the types of data to be used by data holders and 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.

²² For data holders, this is where the accredited person made a consumer data request on behalf of the consumer for a collection of CDR data on a single occasion. For accredited data recipients, this is where the consumer’s disclosure consent applies for the disclosure of CDR data on a single occasion.

²³ For data holders, this is where the accredited person made a consumer data request on behalf of the consumer for collection of CDR data over a specified period of time. For accredited data recipients, this is where the consumer’s disclosure consent applies for the disclosure of CDR data over a specified period of time.

²⁴ CDR Rules 4.19 and 4.27 require data holders and accredited data recipients (respectively) to update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

²⁵ CDR Rule 7.9(2)(c).

Example

Bank Belle, a data holder, receives a consumer data request on 1 July 2020 from Watson and Co, an accredited person, to disclose Zoe's transaction details.

Bank Belle asks Zoe on 1 July 2020 to authorise the disclosure of her transaction details to Watson and Co for the sharing period specified in the consumer data request (i.e. 1 July 2020 to 1 January 2021).

Upon receiving Zoe's authorisation, Bank Belle discloses Zoe's transaction details to Watson and Co on 1 July 2020.

Bank Belle updates Zoe's consumer dashboard on 1 July 2020 to include the following notification statement:

We shared your transaction details with Watson and Co on 01.07.20. We'll continue to share your transaction details with Watson and Co until 01.01.21.

The above statement is an example of how Bank Belle, a data holder, could notify Zoe of the disclosure of her CDR data in accordance with CDR Rule 7.9(1).

Other notification requirements under the CDR Rules

For data holders

10.43 In addition to the Privacy Safeguard 10 notification requirements in relation to disclosure, the data holder must update a consumer's dashboard as soon as practicable after the information required to be contained on the dashboard changes.²⁶

For accredited data recipients

10.44 In addition to the Privacy Safeguard 10 notification requirements in relation to disclosure, there are other notification requirements relating to consent and collection that must be complied with by an accredited data recipient:²⁷

- providing CDR receipts to the consumer (CDR Rule 4.18)
- notification requirements where certain consents expire or are amended (CDR Rules 4.18A, 4.18B and 4.18C)

²⁶ CDR Rule 4.27.

²⁷ 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 1.7(5) 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 \(Key concepts\)](#).

- general obligation to update the consumer dashboard (CDR Rule 4.19)
- ongoing notification requirements for consents to collect and use (CDR Rule 4.20), and
- notifying the consumer of the collection of their CDR data under Privacy Safeguard 5 (CDR Rule 7.4).

10.45 For further information regarding the notification requirements for consent, see [Chapter C \(Consent\)](#). For further information regarding the notification requirement for collection, see [Chapter 5 \(Privacy Safeguard 5\)](#).

Disclosure to a designated gateway

Note: *There are currently no designated gateways in the banking sector.*

10.46 Privacy Safeguard 10 applies where a data holder or accredited data recipient discloses CDR data to a designated gateway as required or authorised under the CDR Rules.²⁸

10.47 There are currently no CDR Rules made for this circumstance.

Interaction with other Privacy Safeguards

10.48 Data holders and accredited data recipients must comply with Privacy Safeguard 1 by taking reasonable steps to implement practices, procedures and systems that will ensure they comply with the CDR regime, including Privacy Safeguard 10. See [Chapter 1 \(Privacy Safeguard 1\)](#).

10.49 Privacy Safeguard 11 mandates the steps which data holders and accredited data recipients must take to advise a consumer where they have disclosed CDR data that was incorrect. See [Chapter 11 \(Privacy Safeguard 11\)](#).

²⁸ CDR Rules may be made in relation to the notification requirements for that disclosure.