

Chapter 13:
Privacy Safeguard 13 —
Correction of CDR data

Version 1.0, February 2020



Contents

Key points	3
What does Privacy Safeguard 13 say?	3
Why is it important?	3
Who does Privacy Safeguard 13 apply to?	4
How Privacy Safeguard 13 interacts with the Privacy Act	4
When must an entity correct CDR data?	5
Actioning and responding to correction requests	6
Acknowledging receipt of correction requests	6
Taking action to correct, or qualify, the CDR data	6
When action is not necessary in response to a request	7
How must a correction notice be provided to consumers?	9
What must be included in a correction notice to consumers?	9
What are the correction considerations?	10
Accurate	10
Up to date	11
Complete	11
Not misleading	11
Charges to correct CDR data	12
Interaction with other privacy safeguards	12
Privacy Safeguard 5	12
Privacy Safeguard 10	12
Privacy Safeguard 11	13
Privacy Safeguard 12	13

Key points

- Privacy Safeguard 13, together with consumer data rules (CDR Rules) 7.14 and 7.15, sets out obligations for data holders and accredited data recipients to:
 - respond to correction requests made by consumers in respect of consumer data right (CDR) data, and to take certain steps to correct or include a qualifying statement in respect of the data, and
 - give the consumer notice of any correction or statement made in response to their request, or reasons why a correction or statement is unnecessary or inappropriate.

What does Privacy Safeguard 13 say?

13.1 Privacy Safeguard 13 requires data holders and accredited data recipients who:

- receive a request from a consumer to correct CDR data, and
- in the case of data holders, were earlier required or authorised under the CDR Rules to disclose the CDR data¹

to respond to the request by taking the relevant steps set out in the CDR Rules.

13.2 CDR Rule 7.15 requires an entity to acknowledge receipt of the request as soon as practicable and sets out how the entity must, to the extent it considers appropriate:

- correct the CDR data, or
- qualify the data by including a statement with it, and
- give the consumer a notice setting out how the entity responded to the request, as well as the complaint mechanisms available to the consumer.

13.3 CDR Rule 7.14 prohibits charging a fee for responding to or actioning a correction request.

Why is it important?

13.4 The objective of Privacy Safeguard 13 is to ensure consumers have trust in and control over the accuracy of their CDR data that is disclosed and used as part of the CDR regime.

13.5 For consumers to have proper control over their data, they must be given the power to require the entities that have disclosed or collected their data to correct inaccuracies in that data.

13.6 Privacy Safeguard 13 does this by ensuring entities are required to correct CDR data in certain circumstances when requested to do so by the consumer.

¹ The reason for this requirement in respect of data holders is that a CDR Rule can only affect a data holder and relate to the accuracy of CDR data if the rule also relates to the disclosure of the CDR data under the CDR Rules (s 56BD(3)(b) of the Competition and Consumer Act).

- 13.7 This allows consumers to enjoy the benefits of the CDR regime, such as receiving competitive offers from other service providers, as the data made available to sector participants can be relied upon.

Who does Privacy Safeguard 13 apply to?

- 13.8 Privacy Safeguard 13 applies to data holders and accredited data recipients for the CDR data. It does not apply to designated gateways.
- 13.9 Importantly, Privacy Safeguard 13 only applies to the CDR data a data holder was required or authorised to disclose under the CDR Rules.²

Note: Currently, there are no designated gateways in the CDR regime responsible for facilitating the transfer of information between data holders and accredited persons ([see Chapter B \(Key concepts\) for the meaning of designated gateway](#)).

How Privacy Safeguard 13 interacts with the Privacy Act

- 13.10 It is important to understand how Privacy Safeguard 13 interacts with the *Privacy Act 1988* (the Privacy Act) and Australian Privacy Principles (APPs).³
- 13.11 APP 13 requires an APP entity to correct personal information held by the entity in certain circumstances.

CDR entity	Privacy protections that apply in the CDR context
Accredited person / accredited data recipient	<p>Privacy Safeguard 13</p> <p>Privacy Safeguard 13 applies instead of APP 13 to CDR data collected by an accredited data recipient under the CDR regime.⁴</p> <p>APP 13 will continue to apply to any personal information held by an accredited person or accredited data recipient that is not CDR data.⁵</p>

² Section 56EP(1)(c) of the Competition and Consumer Act.

³ The Privacy Act includes 13 APPs that regulate the handling of personal information by certain organisations and Australian Government agencies (APP entities).

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

⁵ 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.

CDR entity	Privacy protections that apply in the CDR context
Data holder	<p>Privacy Safeguard 13 or APP 13</p> <p>Privacy Safeguard 13 applies instead of APP 13 where a consumer has requested that a data holder correct their CDR data, and the data holder was earlier authorised or required to disclose it under the CDR Rules.</p> <p>APP 13 will continue to apply to:</p> <ul style="list-style-type: none"> • CDR data that is personal information in all other circumstances, and • personal information that is not CDR data.
Designated gateway	<p>APP 13</p> <p>Privacy Safeguard 13 does not apply to designated gateways.</p>

When must an entity correct CDR data?

13.12 Privacy Safeguard 13 and CDR Rule 7.15 require an entity to correct or include a qualifying statement with CDR data after the CDR consumer has requested their CDR data be corrected, unless the entity does not consider a correction or statement to be appropriate.⁶

Example

Money Mattress Ltd is a data holder of Alex's CDR data. Alex requests that Money Mattress correct her recent transaction data after she becomes a victim of credit card fraud. The request is made over the phone.

The Money Mattress phone operator acknowledges receipt of the request immediately, over the phone. Money Mattress also decides to update Alex's consumer dashboard to reflect that the request was made. Money Mattress's systems show that Money Mattress was earlier required to disclose the data to an accredited person, Safer Money Pty Ltd, under CDR Rule 4.6(4), before the fraud was detected but after the fraudulent transactions were recorded in the CDR data.

Money Mattress determines that for one month, incorrect as well as correct transaction data has been recorded. In order to correct the data, Money Mattress considers the appropriate course is to clarify that the fraudulent transactions recorded were unauthorised.

⁶ For data holders, this obligation only arises if the entity was required or authorised under the CDR Rules to disclose the CDR data.

Actioning and responding to correction requests

Acknowledging receipt of correction requests

- 13.13 When a consumer makes a request to correct their CDR data, CDR Rule 7.15(a) requires the entity to acknowledge receipt of a correction request as soon as practicable.
- 13.14 An entity must acknowledge they have received the correction request. It is best practice for an entity to update the consumer dashboard to reflect that a correction request has been received, provided the consumer dashboard has such a functionality.
- 13.15 However, it is not a requirement that this acknowledgement be in writing or through the dashboard. For example, acknowledgement provided by other electronic means or over the phone is sufficient. Where an entity acknowledges receipt over the phone, it could also make a record of this as evidence that it has complied with CDR Rule 7.15(a).
- 13.16 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 acknowledging receipt of a request.

Taking action to correct, or qualify, the CDR data

- 13.17 CDR Rule 7.15 requires an entity that receives a correction request to either:
- correct the CDR data, or
 - both:
 - include a qualifying statement with the data to ensure that, having regard to the purpose for which it is held, the data is accurate, up to date, complete and not misleading, and
 - where practicable, attach an electronic link to a digital record of the data in such a way that the statement will be apparent to any users of the data.
- to the extent that the entity considers appropriate.
- 13.18 An entity must first consider the extent to which it considers it appropriate to act to correct or qualify the information. Once it determines this, it must undertake either to correct the data or to include a qualifying statement with the data. Such corrections or qualifying statements must make the data accurate, up to date, complete and not misleading (to the best of the entity's knowledge).
- 13.19 The requirement to, where practicable, attach an electronic link to a digital record of the data helps to ensure that any qualifying statement included with the data is clear to those who access the data. An entity's systems should be set up so that the data cannot be accessed without the correction statement or a link to that statement being immediately apparent.
- 13.20 If an entity requires further information or explanation before it can determine which action to take, the entity should clearly explain to the consumer what additional information or explanation is required and/or why the entity cannot act on the information already provided. The entity could also advise where additional material may be obtained.

The consumer should be given a reasonable opportunity to comment on the refusal or reluctance of the entity to make a correction without further information or explanation from the consumer.

- 13.21 An entity should also be prepared in an appropriate case to search its own records and other readily accessible sources that it reasonably expects to contain relevant information, to find any information in support of, or contrary to, the consumer's request. However, an entity need not conduct a full, formal investigation into the matters about which the consumer requests correction. The extent of the investigation required will depend on the circumstances, including the seriousness of any adverse consequences for the consumer if the CDR data is not corrected as requested.

When action is not necessary in response to a request

- 13.22 An entity may consider that it is not appropriate to make any correction or qualifying statement at all, because (for instance) the CDR data as it exists is accurate, up to date, complete and not misleading, for the purpose it is held.
- 13.23 In such circumstances, the entity must give the CDR consumer a notice in accordance with CDR Rule 7.15(c) detailing the reasons why it considered that no correction or statement was necessary or appropriate and setting out the available complaint mechanisms.⁷
- 13.24 Reasons for not correcting CDR data or including a qualifying statement with the data may include:
- while there are inaccuracies in the data, it is nevertheless correct for the purpose for which it is held
 - the CDR consumer is mistaken and has made the correction request in error
 - the CDR consumer is attempting to prevent an accredited person from collecting accurate CDR data that is unfavourable to the consumer
 - the entity is an accredited data recipient of the data, but the request is in respect of data the entity has collected from a data holder (rather than data the entity may have derived from collected data),⁸ with the effect that the consumer should make the request to the data holder, or
 - the CDR data has already been corrected, or a qualifying statement already included with the data, on a previous occasion.

Example

Jessica defaults on her credit card repayments with data holder, BankaLot Ltd. Jessica authorises BankaLot to disclose her CDR data to accredited person, CreditCardFinder Pty Ltd, which sends BankaLot a consumer data request on Jessica's behalf. Shortly after Jessica is notified that the data has been collected, Jessica requests CreditCardFinder to correct her repayment history to show that no default was made with BankaLot. *cont*

⁷ Section 56EP(3)(b) of the Competition and Consumer Act.

⁸ Note that data derived from CDR data collected by an accredited data recipient continues to be 'CDR data': see s 56AI of the Competition and Consumer Act.

CreditCardFinder acknowledges receipt of the request the following business day through the consumer dashboard.

CreditCardFinder determines that because the CDR data was collected from BankaLot and CreditCardFinder has no method of independently determining the correctness of the data, it is not appropriate for it to make any corrections or include any qualifying statements with the data.

CreditCardFinder then gives Jessica a notice through her consumer dashboard that states this finding, and that if Jessica wants the data to be corrected, she should request that BankaLot make the relevant correction.

The notice also sets out the complaint mechanisms available to Jessica, which are in line with the corresponding section in CreditCardFinder's CDR policy.

How to respond to a correction request

Entity receives a correction request from consumer



Entity acknowledges receipt of request as soon as practicable



Within 10 business days after receiving the request, and to the extent the entity considers appropriate:



Entity corrects the CDR data



Entity includes a statement with the CDR data



Where practicable, entity attaches an electronic link to the digital record of the CDR data



Entity takes no action



Entity provides consumer with a written notice, by electronic means, setting out:

- What the entity did
- If the entity did not consider it appropriate to take any action, why a correction or statement is unnecessary or inappropriate
- Complaint mechanisms available to the consumer

How must a correction notice be provided to consumers?

- 13.25 CDR Rule 7.15(c) requires an entity that receives a request from a CDR consumer to correct CDR data to give the consumer a written notice by electronic means. The written notice must contain the matters set out in paragraph 13.29 below.
- 13.26 The requirement for written notices to be given by electronic means will be satisfied if the notice is given, for example, over email or over the consumer's dashboard.
- 13.27 The written notice may be in the body of an email or in an electronic file attached to an email.
- 13.28 While SMS is an electronic means of communicating notice, practically it is unlikely to be appropriate as the number of matters that the written notice must address under CDR Rule 7.15(c) would likely make the SMS very long.

What must be included in a correction notice to consumers?

- 13.29 The correction notice to the consumer must set out:
- what the entity did in response to the request
 - if the entity did not consider it appropriate to take any action, why a correction or statement is unnecessary or inappropriate, and
 - the complaint mechanisms available to the consumer.
- 13.30 The complaint mechanisms available to the consumer that must be included in the notice are:
- the entity's internal dispute resolution processes relevant to the consumer, including any information from the entity's CDR policy about the making of a complaint relevant to the entity's obligations to respond to correction requests, and
 - external complaint mechanisms the consumer is entitled to access, including the consumer's right to complain to the Australian Information Commissioner under Part V of the Privacy Act,⁹ and any external dispute resolution schemes recognised by the Australian Competition and Consumer Commission under s 56DA(1) of the Competition and Consumer Act.
- 13.31 An entity may, but is not required to, advise the consumer that if they have suffered loss or damage by the entity's acts or omissions in contravention of the privacy safeguards or CDR Rules, they have a right to bring an action for damages in a court of competent jurisdiction under s 56EY of the Competition and Consumer Act.

⁹ Section 56ET(4) of the Competition and Consumer Act.

Example

This example follows the example under paragraph 13.12 above.

After Money Mattress corrects Alex’s CDR data, Money Mattress sends Alex a notice over the consumer dashboard within the required 10 business day period. The notice explains the steps that Money Mattress took to ensure the fraudulent transactions were clearly marked as unauthorised, and sets out the complaint mechanisms available to Alex.

What are the correction considerations?

- 13.32 Privacy Safeguard 13 requires that any statement included with CDR data in response to a correction request is to ensure that, having regard to the purpose for which it is held, the CDR data is ‘accurate’, ‘up to date’, ‘complete’ and ‘not misleading’.¹⁰ Held’ is discussed in [Chapter B \(Key concepts\)](#).
- 13.33 Whether or not CDR data is accurate, up to date, complete and not misleading must be determined with regard to the purpose for which it is held.
- 13.34 When working out the purpose for which the CDR data is or was held, entities must disregard the purpose of holding the CDR data so that it can be disclosed as required under the CDR Rules.¹¹ For example, a data holder that is an authorised deposit-taking institution collects transaction data for the purpose of providing a banking service to its customer. It does not hold transaction data for the purpose of being required to disclose the data under the CDR regime. ‘Purpose’ is discussed further in [Chapter B \(Key concepts\)](#).
- 13.35 These four terms are not defined in the Competition and Consumer Act or the Privacy Act.¹²
- 13.36 The following analysis of each term draws on the ordinary meaning of the terms, APP Guidelines and Part V of the *Freedom of Information Act 1982*.¹³ As the analysis indicates, there is overlap in the meaning of the terms.

Accurate

- 13.37 CDR data is inaccurate if it contains an error or defect or is misleading. An example is factual information about a consumer’s income, assets, loan repayment history or employment status which is incorrect for the purpose it is held.
- 13.38 CDR data that is derived from other CDR data is not inaccurate by reason only that the consumer disagrees with the method or result of the derivation.¹⁴ For the purposes of Privacy Safeguard 11, derived data may be ‘accurate’ if it is presented as such and accurately records the method of derivation (if appropriate). For instance, an accredited data recipient may use the existing information it holds on a consumer to predict their

¹⁰ Section 56EP(3)(a)(ii) of the Competition and Consumer Act.

¹¹ Section 56EP(4) of the Competition and Consumer Act.

¹² These terms ‘accurate’, ‘up to date’ and ‘complete’ are also used in Privacy Safeguard 11 in respect of the quality considerations of CDR data. See [Chapter 11 \(Privacy Safeguard 11\)](#) for further information and for an example of an entity determining the purpose for which it holds CDR data at paragraph 11.13.

¹³ See [Chapter 10: APP 10 — Quality of personal information of the APP Guidelines](#).

¹⁴ Data derived from CDR data continues to be ‘CDR data’: see s 56AI of the Competition and Consumer Act.

projected income over a certain period of time. If the data is presented as the estimated future income for the consumer for that period, and states the bases of the estimation (that is, it is based on the consumer's income over the previous certain number of financial years), this would not be inaccurate solely because, for instance, the consumer believes their income will be higher or lower during the projected period.

- 13.39 CDR data may be inaccurate even if it is consistent with a consumer's instructions or if the inaccuracy is attributable to the consumer.

Up to date

- 13.40 CDR data is not up to date if it contains information that is no longer current. An example is a statement that a consumer has an active account with a certain bank, where the consumer has since closed that account. Another example is an assessment that a consumer has a certain ability to meet a loan repayment obligation, where in fact the consumer's ability has since changed.¹⁵
- 13.41 CDR data about a past event may have been up to date at the time it was recorded but has been overtaken by a later development. Whether that data is up to date will depend on the purpose for which it is held. If, for instance, a consumer has had their second child but their CDR data records them as only having one child, the CDR data will still be up to date if the data that records the consumer as having one child is held simply for the purpose of recording whether the consumer is a parent.
- 13.42 In a similar manner to accuracy, CDR data may not be up to date even if it is consistent with a consumer's instructions or if the inaccuracy is attributable to the consumer.

Complete

- 13.43 CDR data is incomplete if it presents a partial or misleading picture of a matter of relevance, rather than a true or full picture.
- 13.44 An example is data from which it can be inferred that a consumer owes a debt, which in fact has been repaid. The CDR data will be incomplete under Privacy Safeguard 13 if the data is held, for instance, for the purpose of determining the borrowing capacity of the consumer. Where the CDR data is held for a different purpose for which the debt is irrelevant, the fact that the debt has been repaid may not of itself render the CDR data incomplete. If, however, the accredited person has requested a consumer's CDR data for a specific period, and in that period the consumer owed a debt which is recorded in the CDR data, and that debt was repaid in a later period, the CDR data will still be 'complete' in respect of that specific period.

Not misleading

- 13.45 CDR data will be misleading if it conveys a meaning that is untrue or inaccurate or could lead a user, receiver or reader of the information into error. An example is a statement that is presented as a statement of fact but in truth is a record of the opinion of a third-party. In some circumstances an opinion may be misleading if it fails to include information about

¹⁵ Such an assessment will likely be 'materially enhanced information' under section 10 of the designation instrument and therefore not 'required consumer data' under the CDR Rules.

the facts on which the opinion was based, or the context or circumstances in which the opinion was reached.

- 13.46 Data may also be misleading if other relevant information is not included. An example is a statement that a consumer is involved in litigation to recover a debt, without including the fact that the consumer is the plaintiff rather than the defendant in the action.

Example

Angelica consents to XYZ Solutions Pty Ltd (XYZ) (an accredited person), collecting her CDR data from Good Faith Banking and Insurance Ltd (GFBI) (a data holder). Angelica has consented to XYZ collecting and using the data for the purpose of providing Angelica with recommendations for various insurance products.

Angelica has previously spoken with GFBI employee, Bert, about insurance products offered by GFBI and mistakenly advised that she has mortgage protection when she does not. Bert had recorded, as part of Angelica's CDR data, that Angelica has mortgage protection insurance.

If Angelica requests that XYZ or GFBI correct her CDR data, the entity may include a statement with the data that Angelica does not have the insurance product. Alternatively, the entity may delete or alter the relevant part of the data to make clear that Angelica does not have the insurance product. If any one of these actions was taken, the data would no longer be inaccurate or misleading.

Charges to correct CDR data

- 13.47 CDR Rule 7.14 prohibits an entity from charging a fee for responding to, or actioning, a request under Privacy Safeguard 13.

Interaction with other privacy safeguards

Privacy Safeguard 5

- 13.48 Privacy Safeguard 5 requires an accredited data recipient to notify a consumer of the collection of their CDR data by updating the consumer's dashboard.
- 13.49 Where an accredited person has collected CDR data, and then collects corrected data after the data holder complies with the consumer's requests to correct and disclose corrected data under Privacy Safeguards 11 and 13, the accredited person must notify that consumer under Privacy Safeguard 5 in respect of both collections.

Privacy Safeguard 10

- 13.50 Privacy Safeguard 10 requires a data holder to notify a CDR consumer of the disclosure of their CDR data by updating the consumer's dashboard.
- 13.51 Where a data holder has disclosed CDR data and then discloses corrected data as the result of the consumer's requests to correct and disclose corrected data under Privacy Safeguards

11 and 13, the data holder must notify that consumer under Privacy Safeguard 10 in respect of both disclosures.

Privacy Safeguard 11

- 13.52 Privacy Safeguard 13 does not apply where an entity knows CDR information is incorrect, but the consumer has not made a correction request.
- 13.53 However, data holders and accredited data recipients will still have obligations under Privacy Safeguard 11 to take reasonable steps to ensure the quality of CDR data they are required or authorised to disclose under the CDR Rules.
- 13.54 This includes an obligation for accredited data recipients and data holders to advise consumers that some or all of their CDR data disclosed was incorrect if, at the time of disclosure, the data was not accurate, up to date and complete, having regard to the purposes for which the data was held.
- 13.55 An entity that corrects CDR data, or includes a qualifying statement with it in accordance with Privacy Safeguard 13, must consider whether the consumer must be advised of any previous disclosures of the CDR data where the data was incorrect when it was disclosed, in accordance with Privacy Safeguard 11.¹⁶ The consumer may then request the entity disclose corrected CDR data to the recipient of the earlier disclosure, in accordance with Privacy Safeguard 11.¹⁷

Risk point: If a data holder corrects CDR data only in response to consumer requests, rather than taking reasonable steps under Privacy Safeguard 11 to ensure the quality of CDR data they are required or authorised to disclose under the CDR Rules, the entity may breach Privacy Safeguard 11 when disclosing the CDR data.

Privacy tip: Data holders should ensure that whenever they become aware that CDR data is incorrect, steps are taken to correct the data or include a qualifying statement with the data.

Privacy Safeguard 12

- 13.56 Where an accredited data recipient corrects CDR data to comply with Privacy Safeguard 13, it should consider whether it needs to take action under Privacy Safeguard 12 to destroy or de-identify the original data.

¹⁶ Section 56EN(3) of the Competition and Consumer Act.

¹⁷ Section 56EN(4) of the Competition and Consumer Act.