Chapter 13:

Privacy Safeguard 13 —

Correction of CDR data

Consultation draft, October 2019

OAIC

Contents

Key points

- Privacy Safeguard 13, together with Consumer Data Rules 7.14 and 7.15, sets out obligations for data holders and accredited data recipients to:
  - respond to correction requests made by CDR consumers in respect of CDR data, and to take certain steps to correct or include a qualifying statement in respect of the data, and
  - give the CDR 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 CDR consumer to correct CDR data, and
- in the case of data holders, were earlier required or authorised under the Consumer Data Rules to disclose the CDR data,[1]

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

13.2 Consumer Data 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 Consumer Data 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 inaccurate CDR data in certain circumstances when requested to do so by the consumer.

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.

[1] The reason for this requirement in respect of data holders is that a Consumer Data 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 Consumer Data Rules (s 56BD(3)(b)).

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 Consumer Data Rules.[2]

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 Like Privacy Safeguard 13, APP 13 requires an APP entity to correct personal information held by the entity in certain circumstances.

Summary of application of Privacy Safeguard 13 by CDR entity

CDR entity	Privacy principle that applies to CDR data
Accredited person	**Australian Privacy Principle 13** APP 13 applies to any personal information held by accredited persons who are not yet accredited data recipients.[4]
Accredited data recipient	**Privacy Safeguard 13** Privacy Safeguard 13 applies instead of APP 13,[5] meaning APP 13 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime. APP 13 will continue to apply to any personal information collected by the accredited person that is not CDR data.[6]

[2] 56EP(1)(c).

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

[4] An accredited person will become an accredited data recipient of CDR data following receipt of CDR data under the Consumer Data Rules (unless they are a data holder or designated gateway for the data) (see s 56AK).

[5] 56EC(4)(a).

[6] 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. This means that non-CDR personal information handling by accredited persons is covered by the Privacy Act and the APPs, while the handling of CDR data is covered by the CDR regime and the Privacy Safeguards. See s 6E(1D) of the Privacy Act.

CDR entity	Privacy principle that applies to CDR data
Data holder	**Australian Privacy Principle 13 and Privacy Safeguard 13** (depending on the circumstances) APP 13 applies to CDR data that is also personal information unless a consumer requests the data holder to correct CDR data. Where a consumer requests the data holder correct CDR data: • Privacy Safeguard 13 applies instead of APP 13[7] for CDR data disclosed under the Consumer Data Rules • APP 13 applies for CDR data which was disclosed otherwise than under the Consumer Data Rules[8], where that CDR data is personal information. This means that APP 13 continues to apply to all personal information (and CDR data that is personal information): • where a data holder has not received a correction request, and • that a data holder discloses otherwise than under the Consumer Data Rules.
Designated gateway	**Australian Privacy Principle 13** Privacy Safeguard 13 does not apply to a designated gateway.

When must an entity correct CDR data?

13.12 Privacy Safeguard 13 and Consumer Data 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.[9]

Example

Kiefer requests his bank, Money Mattress Ltd, a data holder of his CDR data, to correct his recent transaction data after he 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, and arranges for Keifer's consumer dashboard to be updated to reflect that the request was made. Money Mattress' systems show that the bank was earlier required to disclose the data to accredited person, Safer Money Pty Ltd, under Consumer Data Rule 4.6(4).

[7] 56EC(4)(b).

[8] For instance, to a third party service provider.

[9] For data holders, this obligation only arises if the entity was required or authorised under the Consumer Data Rules to disclose the CDR data.

Money Mattress determines that for one month, incorrect as well as correct transaction data is recorded. In order to correct the data, Money Mattress considers the appropriate course is to delete the incorrect data and retain the correct data.

Actioning and responding to correct requests

Acknowledging receipt of correction requests

13.13 When a consumer makes a request to correct their CDR data, Consumer Data Rule 7.15(a) requires the entity to acknowledge receipt of a correction request as soon as practicable.

13.14 An entity should 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.

13.16 The concept, 'as soon as practicable' is discussed in Chapter B (Key Concepts). 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 be able to justify any delay in acknowledging receipt of the request.

Taking action to correct, or qualify, the CDR data

13.17 Consumer Data Rule 7.15 requires an entity that receives a correction request to either:

- correct the CDR data, or
- 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,

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 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.

13.20 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

13.21 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.

13.22 In such circumstances the entity must give the CDR consumer a notice in accordance with Consumer Data 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.[10]

13.23 Reasons for not correcting CDR data or including a qualifying statement with the data may include:

- 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 and 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), or
- the CDR data has already been corrected, or a qualifying statement already included with the data, on a previous occasion.

Example

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

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 Dolly a notice through her consumer dashboard that states that no correction or statement was made in relation to her CDR data, because CreditCardFinder did not think it appropriate for it to make such a correction or qualifying statement in relation to data it collected from BankaLot, and that if Dolly wishes the data be corrected, she should request BankaLot to make the relevant correction.

[10] 56EP(3)(b).

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

How must a correction notice be provided to consumers?

13.24 Consumer Data 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.

13.25 The requirement for written notices to be given by electronic means will be satisfied if the notice is given over email or over the CDR consumer's consumer dashboard.

13.26 The written notice may be in the body of an email or in an electronic file attached to an email.

13.27 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 Rule 7.15(c) would likely make the SMS very long.

What must be included in a correction notice to consumers?

13.28 The correction notice to the consumer must set out:

- what the entity did in response to the request, and
- complaint mechanisms available to the consumer.

13.29 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.
- 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,[11] and any external dispute resolution schemes recognised by the Australian Competition and Consumer Commission under s 56DA(1).

13.30 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 Consumer Data 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.

[11] 56ET(4).

Example

This example follows the example under paragraph 13.12 above.

After Money Mattress corrects Kiefer's CDR data, Money Mattress sends Kiefer a notice over the consumer dashboard within the required 10 business day period. The notice states that Money Mattress has corrected the data by deleting the incorrect data relating to fraudulent transactions and retaining the correct data, and sets out the complaint mechanisms available to Kiefer.

What are the correction considerations?

13.31 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'.

13.32 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**. Privacy Safeguard 13 requires that holding the CDR data so that it can be disclosed as required under the Consumer Data Rules is not a purpose when working out the purposes for which the data is or was held.[12] 'Purpose' is discussed further in Chapter B (Key Concepts).

13.33 These four terms are not defined in the Competition and Consumer Act or the Privacy Act.[13] 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.[14] As the analysis indicates, there is overlap in the meaning of the terms.

Accurate

13.34 CDR data is inaccurate if it contains an error or defect or is misleading. An example is incorrect factual information about a CDR consumer's income, assets, loan repayment history or employment status.

13.35 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. For the purposes of Privacy Safeguard 13, 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 an algorithm to determine a CDR consumer's 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, it will not be inaccurate because, for instance, the consumer believes their income will be higher or lower during the projected period.

[12] 56EP(4).

[13] 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 – Quality of CDR data for further information.

[14] See OAIC, Australian Privacy Principles Guidelines (22 July 2019), Chapter 10 APP 10 — Quality of personal information.

Up to date

13.36 CDR data is not up to date if it contains information that is no longer current. An example is a statement that a CDR consumer has an active account with a certain bank, where the consumer has 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]

13.37 For example, CDR data about a past event may have been accurate 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.

Complete

13.38 CDR data is incomplete if it presents a partial or misleading picture rather than a true or full picture.

13.39 An example is data from which it can be inferred that a CDR 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.

Not misleading

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

13.41 Data may also be misleading if other relevant information is not included. An example is a statement that a CDR 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

Accredited person, XYZ Solutions Pty Ltd (**XYZ**), has consent from Zorro to collect his CDR data from data holder, Good Faith Banking and Insurance Ltd (**GFBI**). Zorro has consented to XYZ collecting and using the data for the purposes of providing Zorro with recommendations for various insurance products (for which XYZ does not receive commissions and does not promote).

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

[15] Such an assessment will likely by 'materially enhanced information' under section 10 of the Designation Instrument and therefore not 'required consumer data' under the Consumer Data Rules.

If Zorro requests XYZ or GFBI to correct his CDR data, the entity may include a statement with the data that Zorro does not have the insurance product. The inclusion of such a statement would render the data no longer inaccurate or misleading.

Charges to correct CDR data

13.42 Consumer Data 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

13.43 Privacy Safeguard 5 requires an accredited data recipient to notify a CDR consumer of the collection of their CDR data by updating the CDR consumer's consumer dashboard.

13.44 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

13.45 Privacy Safeguard 10 requires a data holder to notify a CDR consumer of the disclosure of their CDR data by updating the CDR consumer's consumer dashboard.

13.46 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

13.47 Privacy Safeguard 13 does not apply where an entity knows CDR information is incorrect, but the CDR consumer has not made a correction request.

13.48 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 Consumer Data Rules.

13.49 This includes an obligation for accredited data recipients and data holders to advise CDR 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.

13.50 An entity that corrects CDR data or includes a qualifying statement with it in accordance with Privacy Safeguard 13 must consider whether the CDR 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 CDR 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 only corrects CDR data in response to CDR 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 Consumer Data 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

13.51 Where an accredited data recipient amends or creates new 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 redundant data that it holds (for example a copy of that information).

Example

Accredited data recipient of Morpheus' CDR data, NRGZ Pty Ltd, receives a correction request from Morpheus.

Data holder, Energetica Ltd was earlier required to disclose Morpheus' CDR data to NRGZ in response to a consumer data request.[18]

Morpheus's request is in respect of his energy usage data for the past year. The data is in respect of a shared house in which Morpheus lived with 5 other housemates, where the energy plan with Energetica was in Morpheus' name alone but payment of the bills was split among the housemates.

Morpheus requests his energy data be corrected to reflect this fact, or to be deleted from his CDR data held by NRGZ.

NRGZ considers that, as the service requested by Morpheus requires NRGZ to ascertain his individual energy usage over a certain period of time, and it is not possible to ascertain the usage from the data collected from Energetica, the data is not needed for this purpose and is not required to be retained under an Australian law or court/tribunal order. NRGZ determines that the data is redundant and should be destroyed under Privacy Safeguard 12.

NRGZ sends Morpheus a notice over his consumer dashboard indicating that NRGZ did not think it appropriate to correct or qualify it.

[16] See section 56EN(3).

[17] See section 56EN(4).

[18] under Consumer Data Rule 4.6(4).