Chapter 13:

# Privacy Safeguard 13 —

## Correction of CDR data

Version 3.0, June 2021



OAIC

# Contents

# 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 of CDR data to:
  - respond to correction requests made by consumers in respect of the 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 of a consumer's CDR data who:

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

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, within 10 business days after receipt of the request, and to the extent it considers appropriate:

- correct the CDR data, or
- qualify the data by including a statement with it.

13.3 The entity must also give the consumer a notice setting out how they responded to the request, as well as the complaint mechanisms available to the consumer.

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

# Why is it important?

13.5 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.

13.6 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.

13.7 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.

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

# Who does Privacy Safeguard 13 apply to?

13.9 Privacy Safeguard 13 applies to data holders and accredited data recipients of CDR data. It does not apply to designated gateways.

13.10 Importantly, in relation to data holders, Privacy Safeguard 13 only applies where a consumer has requested that a data holder correct their CDR data and the data holder was earlier required or authorised to disclose it under the CDR Rules.[1] APP 13 will continue to apply to CDR data that is personal information in all other circumstances. For example, where the consumer makes a correction request, but the data has not previously been disclosed under the CDR Rules.

***Note:*** *There are no designated gateways in the banking sector. See Chapter B (Key concepts) for the meaning of designated gateway.*

# How Privacy Safeguard 13 interacts with the Privacy Act

13.11 It is important to understand how Privacy Safeguard 13 interacts with the *Privacy Act 1988* (the Privacy Act) and the Australian Privacy Principles (APPs).[2]

13.12 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 data recipient** | **Privacy Safeguard 13**<br>For an accredited data recipient of CDR data, Privacy Safeguard 13 applies to the correction of that CDR data.[3]<br>APP 13 does not apply in relation to that CDR data.[4] |

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

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

[3] Privacy Safeguard 13 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, 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.

[4] 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. 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.

| CDR entity | Privacy protections that apply in the CDR context |
|---|---|
| **Data holder** | **Privacy Safeguard 13 or APP 13**<br><br>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 required or authorised to disclose it under the CDR Rules.<br><br>APP 13 will continue to apply to CDR data that is personal information in all other circumstances. This includes where:<br><br>• the consumer makes a correction request, but the data has not previously been disclosed under the CDR Rules, or<br><br>• the consumer has not made a correction request, but the APP entity is satisfied that the data it holds is incorrect.[5] |
| **Designated gateway** | **APP 13**<br><br>Privacy Safeguard 13 does not apply to designated gateways. |

# When must an entity correct CDR data?

13.13 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]

# Actioning and responding to correction requests

## Acknowledging receipt of correction requests

13.14 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.

13.15 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.

13.16 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).

[5] Specifically, a data holder who is also an APP entity must continue to take reasonable steps to correct CDR data that is personal information where it is inaccurate, out-of-date, incomplete, irrelevant or misleading for the purpose for which it is held under APP 13.

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

13.17 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

13.18 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.

The entity must take one of these steps within 10 business days after receipt of the request, and to the extent that the entity considers appropriate.

13.19 The 10 business day time period commences on the day after the entity receives the request.[7] For example, if the entity receives the request on 2 August, the 10 business day period begins on 3 August.

13.20 A 'business day' is a day that is not Saturday, Sunday or a public holiday in the place concerned.

13.21 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).

13.22 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.

13.23 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.

13.24 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

[7] See s 36 of the *Acts Interpretation Act 1901*.

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

13.25 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.

13.26 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.[8]

13.27 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),[9] 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.

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

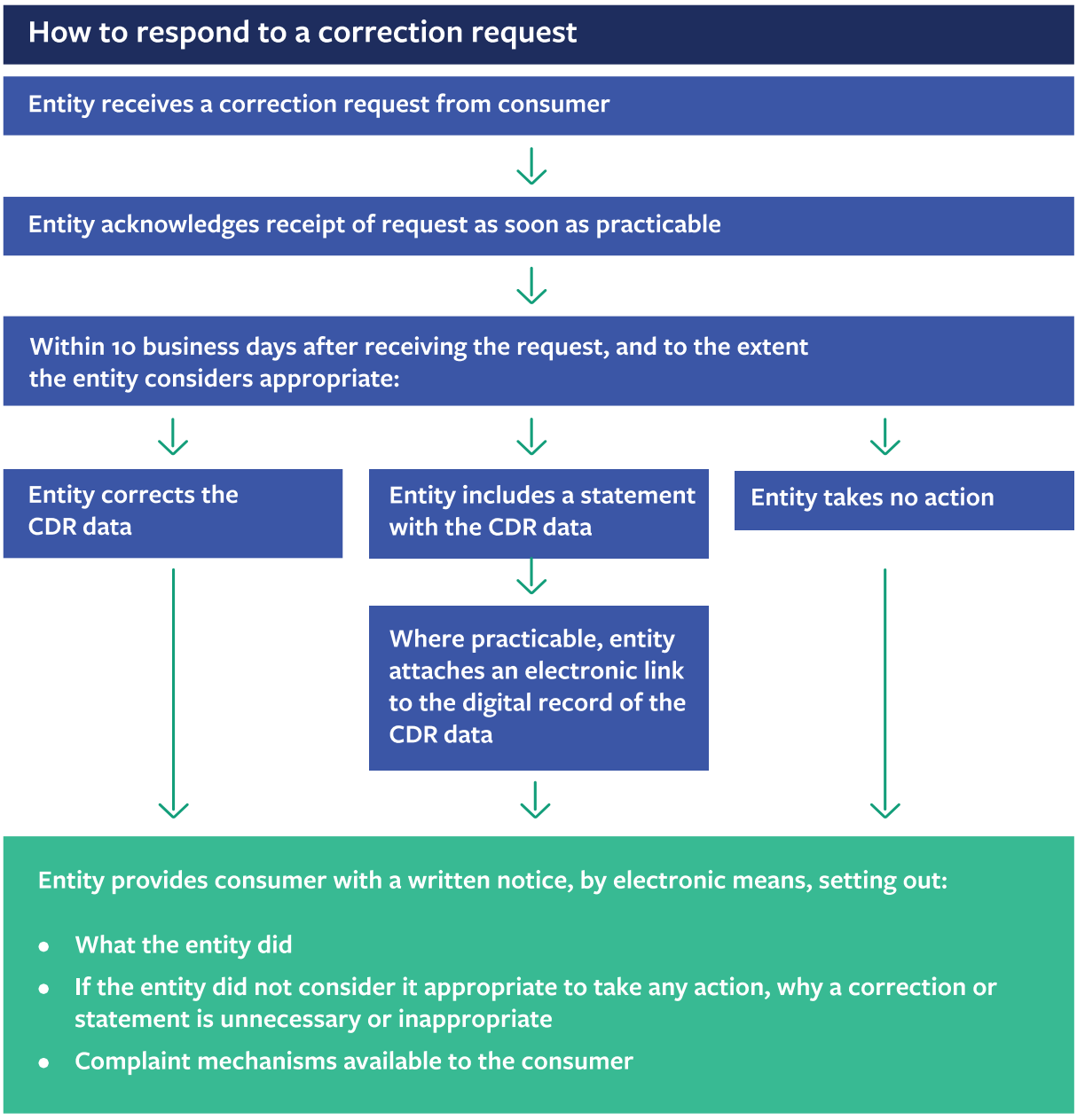
*cont*

[8] Section 56EP(3)(b) of the Competition and Consumer Act.

[9] 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.

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 must a correction notice be provided to consumers?

13.28 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 13.32 below.

13.29 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.

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

13.31 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?

13.32 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.

13.33 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,[10] and any external dispute resolution schemes recognised by the Australian Competition and Consumer Commission under s 56DA(1) of the Competition and Consumer Act.

13.34 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.

# What are the correction considerations?

13.35 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'.[11] 'Held' is discussed in Chapter B (Key concepts).

13.36 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.

13.37 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

[10] Section 56ET(4) of the Competition and Consumer Act.

[11] Section 56EP(3)(a)(ii) of the Competition and Consumer Act.

Rules.[12] 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).

13.38 These four terms are not defined in the Competition and Consumer Act or the Privacy Act.[13]

13.39 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

13.40 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.

13.41 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.[15] 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 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.

13.42 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

13.43 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.[16]

13.44 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

[12] Section 56EP(4) of the Competition and Consumer Act.

[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 (Privacy Safeguard 11) for further information and for examples of an entity determining the purpose for which it holds CDR data.

[14] See Chapter 10: APP 10 — Quality of personal information of the APP Guidelines.

[15] Data derived from CDR data continues to be 'CDR data': see s 56AI of the Competition and Consumer Act.

[16] Such an assessment will likely be 'materially enhanced information' under section 10 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 and therefore not 'required consumer data' under the CDR Rules.

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.

13.45 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

13.46 CDR data is incomplete if it presents a partial or misleading picture of a matter of relevance, rather than a true or full picture.

13.47 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

13.48 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.

13.49 Data may also be misleading if other relevant information is not included.

**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), and using that 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 been 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

13.50 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

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

13.52 Where an accredited person has collected CDR data, and then collects corrected data after the data holder or accredited data recipient 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

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

13.54 Where a data holder or accredited data recipient 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 entity must notify that consumer under Privacy Safeguard 10 in respect of both disclosures.

## Privacy Safeguard 11

13.55 A correction request made under Privacy Safeguard 13 may trigger a CDR entity's obligations under Privacy Safeguard 11 (Quality of CDR data).

13.56 Under Privacy Safeguard 11, data holders and accredited data recipients have an obligation to advise consumers if they disclose CDR data at a point in time, but then later become aware that some or all of the data disclosed was inaccurate, out of date or incomplete, having regard to the purpose for which the data was held at the time of disclosure.

13.57 A CDR entity may become aware of inaccuracies in CDR data in a range of ways – including pursuant to a correction request under Privacy Safeguard 13.

13.58 Therefore, an entity that corrects CDR data, or includes a qualifying statement with such data in accordance with Privacy Safeguard 13, must also consider whether the consumer must be advised of any previous disclosures of incorrect CDR data, in accordance with Privacy Safeguard 11.[17]

## Privacy Safeguard 12

13.59 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.

[17] Section 56EN(3) of the Competition and Consumer Act.