Chapter 11:

Privacy Safeguard 11 —

Quality of CDR data

Version 3.0, June 2021

OAIC

Contents

Key points

- Privacy Safeguard 11, together with consumer data rule (CDR Rule) 7.10, sets out obligations for data holders and accredited data recipients of CDR data to:
  - ensure the quality of disclosed consumer data right (CDR) data
  - inform consumers in the event incorrect CDR data is disclosed, and
  - disclose corrected CDR data to the original recipient where requested by the affected consumer.

What does Privacy Safeguard 11 say?

11.1 Privacy Safeguard 11 requires:

- data holders who are required or authorised to disclose CDR data under the CDR Rules, and
- accredited data recipients of a consumer's CDR data who are disclosing that consumer's CDR data when required or authorised under the CDR Rules

to:

- take reasonable steps to ensure that the CDR data is, having regard to the purpose for which it is held, accurate, up to date and complete
- advise the consumer in accordance with the CDR Rules if they become aware that the CDR data disclosed was not accurate, up to date and complete when disclosed, and
- where incorrect CDR data was previously disclosed, comply with a request by the consumer to disclose corrected CDR data to the original recipient in accordance with the CDR Rules.[1]

11.2 Privacy Safeguard 11 provides that holding CDR data so that it can be disclosed as required under the CDR Rules is not to be regarded as a purpose when working out the purpose for which the CDR data is or was held.

11.3 CDR Rule 7.10 requires data holders and accredited data recipients of a consumer's CDR data who have disclosed CDR data that was incorrect at the time of disclosure to provide the consumer with a written notice by electronic means that identifies:

- the accredited person
- the CDR data that was incorrect, and
- the date of the disclosure.

11.4 The notice must also advise the consumer that they can request the entity to disclose the corrected data to the accredited person (to whom the incorrect CDR data was previously disclosed). The data holder or accredited data recipient must disclose the corrected data if the consumer requests them to do so.

[1] Both the consumer's request, and the actions taken by the CDR participant to correct the data under Privacy Safeguard 11, must be in accordance with the CDR Rules – see s 56EN(4). Further, the requirement to disclose corrected CDR data to the recipient under Privacy Safeguard 11 does not apply in circumstances specified in the CDR Rules (see section s 56EN 4A of the Competition and Consumer Act). However, no such Rules have been made.

11.5 This notice must be provided to the consumer as soon as practicable, but no more than five business days after becoming aware that some or all of the disclosed data was incorrect.

Why is it important?

11.6 The objective of Privacy Safeguard 11 is to ensure consumers have trust in and control over the quality of their CDR data disclosed as part of the CDR regime.

11.7 Privacy Safeguard 11 does this by ensuring entities are disclosing CDR data that is accurate, up to date and complete, and by giving consumers control over their data by allowing them to require entities to correct any inaccuracies in their data after it is shared.

11.8 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 on.

Who does Privacy Safeguard 11 apply to?

11.9 Privacy Safeguard 11 applies to data holders and accredited data recipients of CDR data. It does not apply to designated gateways.

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

How Privacy Safeguard 11 interacts with the Privacy Act

11.10 It is important to understand how Privacy Safeguard 11 interacts with the *Privacy Act 1988* (the Privacy Act) and Australian Privacy Principles (APPs).[2]

11.11 APP 10 requires APP entities to take reasonable steps to ensure the quality of personal information in certain circumstances.

11.12 APP 10 requires an APP entity to take reasonable steps to ensure the quality of personal information at the time of the *collection* and *use* as well as the disclosure of the information.

11.13 Although Privacy Safeguard 11 applies only in relation to the *disclosure* of CDR data, good practices and procedures by data holders that ensure the quality of personal information collected, used and disclosed under APP 10 will also help to ensure the quality of CDR data that is *disclosed under the CDR regime.*

11.14 Data holders should also be aware that APP 13 (correction of personal information) obligations under the Privacy Act continue to apply in certain circumstances. For example, where the data holder becomes aware of incorrect CDR data, but the data holder has not disclosed that data to an accredited data recipient, the data holder must continue to comply with APP 13 and take steps that are reasonable to correct CDR data.[3]

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

[3] See Chapter 13 (Correction of personal information) of the OAIC's APP Guidelines for further information.

CDR entity	Privacy protections that apply in the CDR context
Accredited data recipient	**Privacy Safeguard 11** For accredited data recipients of a consumer's CDR data, Privacy Safeguard 11 applies to the disclosure of CDR data and for corrections of that data once disclosed. [4] APP 10 does not apply to in relation to that CDR data. [5]
Data holder	**Privacy Safeguard 11, APP 10 and APP 13** Privacy Safeguard 11 applies instead of APP 10 to *disclosures* of CDR data that are required or authorised under the CDR Rules. APP 10 continues to apply to CDR data that is also personal information in all other circumstances, including: • the collection and use of CDR data, and • disclosures of CDR data outside the CDR regime. **Note:** APP 13 continues to apply when the data holder becomes aware of incorrect CDR data, but the data has not been disclosed to an accredited data recipient.[6]
Designated gateway	**APP 10** Privacy Safeguard 11 does not apply to a designated gateway.

What are the quality considerations?

11.15 The three quality considerations under Privacy Safeguard 11 are that data should be 'accurate, up to date and complete'. Whether or not CDR data is accurate, up to date and complete must be determined with regard to the purpose for which it is held. 'Held' is discussed in Chapter B (Key concepts).

[4] Privacy Safeguard 11 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.

[5] 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.

[6] APP 13 requires that APP entities must take reasonable steps to correct personal information where the entity is satisfied, independently of any request, that personal information it holds.

11.16 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.

11.17 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).

Example 1 – data holder

Bright Bank is a data holder and is regularly required or authorised to disclose consumers' CDR data under the CDR Rules.

Bright Bank receives a consumer data request from Leighton, requesting that Bright Bank share their account balance and details with Innobank.

Bright Bank holds this data for the purposes of providing a bank account service to Leighton.

When Bright Bank is required or authorised to disclose Leighton's CDR data under the CDR Rules to Innobank, Privacy Safeguard 11 requires Bright Bank to take reasonable steps to ensure the data is accurate, up to date and complete having regard to this purpose.

Example 2 – accredited data recipients

Vikingforce is an accredited data recipient who collects and uses Hamish's CDR data to provide him with a product comparison service, and recommendations about suitable products. With Hamish's consent, Vikingforce transfers Hamish's CDR data to Turtledoor so he can acquire the recommended product.

Vikingforce holds Hamish's CDR data for the purpose of providing Hamish with a product comparison service and product recommendations, and must take reasonable steps to ensure the data is accurate, up to date and complete having regard to this purpose.

Vikingforce does not hold Hamish's CDR data for the purpose of transferring it to Turtledoor for Hamish to acquire a product, and must disregard this purpose when taking reasonable steps to ensure the data is accurate, up to date and complete under Privacy Safeguard 11.

11.18 The three terms listed in Privacy Safeguard 11, 'accurate', 'up to date', and 'complete', are not defined in the Competition and Consumer Act or the Privacy Act.[7]

11.19 The following analysis of each term draws on the ordinary meaning of the terms and the APP Guidelines.[8] As the analysis indicates, there is overlap in the meaning of the terms.

Accurate

11.20 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 having regard to the purpose for which it is held.

[7] These terms are also used in Privacy Safeguard 13 in respect of the requirement for a data holder, as an alternative to correcting the CDR data, to include a statement with CDR Data to ensure that it is accurate, up to date, complete and not misleading, after receiving a request from the consumer to correct the CDR data (see Chapter 13 (Privacy Safeguard 13)).

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

11.21 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.[9] 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 basis for that estimation (i.e. it is based on the consumer's income over previous financial years), this would not be inaccurate solely because the consumer believes their income will be higher or lower during the projected period.

11.22 CDR data may be inaccurate even if it is consistent with a consumer's instructions or if the inaccuracy is attributable to the consumer. For example, if a consumer has provided an incorrect mobile number which is held by the data holder for the purpose of being able to contact the consumer, and the data holder discloses this, the CDR data may be inaccurate and the data holder may later become aware of this inaccuracy.

Up to date

11.23 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.[10]

11.24 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. For example, if a consumer has had a second child but their CDR data records them as having only one child, the CDR data will still be up to date if that data is held for the purpose of recording whether the consumer is a parent.

11.25 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

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

11.27 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 11 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.

---

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

[10] 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.

Taking reasonable steps to ensure the quality of CDR data

When must an entity take reasonable steps?

11.28 Privacy Safeguard 11 requires an entity to take reasonable steps to ensure the quality of CDR data at the following points in time:

- **for data holders:** at the time the entity is required or authorised, or throughout the period in which the entity is required or authorised, to disclose CDR data under the CDR Rules. This includes when a data holder discloses CDR data:
  - to accredited data recipients under CDR Rule 4.6, and
  - to consumers under CDR Rule 3.4
- **for accredited data recipients:** at the time the entity discloses CDR data when required or authorised under the CDR Rules. This includes (but is not limited to) when an accredited data recipient discloses CDR data to:
  - an accredited data recipient under CDR Rules 7.5(1)(g)[11]
  - the consumer under CDR Rule 7.5(1)(c), and
  - an outsourced service provider under CDR Rule 7.5(1)(d).

11.29 At other times, regular reviews of the quality of CDR data held by the entity may also ensure the CDR data is accurate, up-to-date and complete at the time it is disclosed.

11.30 Entities should also be aware that Privacy Safeguard 11 only requires accredited data recipients to take reasonable steps when disclosing CDR data *under the CDR Rules*. It does not apply in relation to other disclosures of CDR data, for example where an accredited data recipient is required or authorised under another Australian law or court/tribunal order to disclose CDR data. The concept, 'required or authorised to use or disclose CDR data under the CDR Rules' is discussed in Chapter B (Key concepts).

Risk point: If a data holder takes steps to ensure the quality of CDR data only at the time of the disclosure or authorisation, there is a greater risk that the data will be incorrect.

Privacy tip: While the obligation to ensure the quality of CDR data under Privacy Safeguard 11 applies only at the time a data holder is required or authorised to disclose the data, data holders should have processes and procedures in place to periodically update and confirm the accuracy of the CDR data that they hold, during periods in which they are not required or authorised to disclose the data. As CDR data that falls under the privacy safeguards is also personal information, data holders should already have in place such processes and procedures to ensure the accuracy of personal information they collect and use for the purposes of APP 10.

[11] Disclosure of CDR data to an accredited person is not a permitted use or disclosure until the earlier of 1 July 2021 or the day a consumer experience data standard is made for the disclosure of CDR data to accredited persons. See CDR Rule 7.5A.

What constitutes 'reasonable steps'?

11.31 The requirement to ensure the quality of CDR data is qualified by a 'reasonable steps' test.

11.32 This test requires an objective assessment of what is considered reasonable, having regard to the purpose for which the information is held, which could include:

- **The nature of the entity.** The size of the entity, its resources, the complexity of its operations and its business model are all relevant to determining what steps would be reasonable for the entity to take to ensure the quality of the CDR data it is authorised or required to disclose.
- **The sensitivity of the CDR data held and adverse consequences for the consumer if the quality of CDR data is not ensured.** An entity should consider the sensitivity of the data and possible adverse consequences for the consumer concerned if the CDR data is not correct for the purpose it is held. A data holder should take more extensive steps to ensure the quality of highly sensitive data that it might be required or authorised to disclose. More rigorous steps may be required as the risk of adversity increases.
- **Whether the CDR data has been inferred.** Entities may be required to take more rigorous steps to ensure the quality of CDR data that has been created, generated or inferred through analytics processes.
- **The practicability of taking action, including time and cost involved.** A 'reasonable steps' test recognises that privacy protection must be viewed in the context of the practical options available to entities. The time, cost and resources involved in ensuring the quality of CDR data are relevant considerations. However, an entity is not excused from taking certain steps by reason only that it would be inconvenient, time-consuming, or impose some cost to do so. Whether these factors make it unreasonable to take a particular step will depend on whether the burden is excessive in all the circumstances.

11.33 In some circumstances, it will be reasonable for an accredited data recipient to take no steps to ensure the quality of CDR data. For example, where an accredited data recipient collects CDR data from a data holder known to be reliable, and the accredited data recipient has not created, generated, or inferred any further CDR data, it may be reasonable to take no steps to ensure the quality of that data. It is the responsibility of the entity to be able to justify that this is reasonable.

Examples of reasonable steps

11.34 The following are given as examples of reasonable steps that an entity should consider:

- Implementing internal practices, procedures and systems to verify, audit, monitor, identify and correct poor-quality CDR data to ensure that CDR data is accurate, up to date and complete at the point of disclosure.
- Ensuring internal practices, procedures and systems are commensurate with reasonable steps to ensure the quality of CDR data the entity is authorised or required to disclose.

- Ensuring updated or new CDR data is promptly added to the relevant existing records as appropriate.[12]
- For a data holder, implementing protocols to ensure that the CDR data is accurate, up to date and complete both before and once it has been converted to the format required by the Data Standards.
- For an accredited data recipient, ensuring that any analytic processes used are operating appropriately and are fit for purpose, and not creating inaccurate or unjustified results. This is because data derived from CDR data collected by an accredited data recipient continues to be 'CDR data'.[13]

Advising a consumer when disclosed CDR data is incorrect

11.35 Under Privacy Safeguard 11, if a data holder or accredited data recipient becomes aware that disclosed CDR data was not accurate, up to date and complete, they must advise the consumer in accordance with the CDR Rules.[14]

11.36 CDR Rule 7.10 sets out the requirements for notifying the consumer where a data holder or accredited data recipient becomes aware that disclosed CDR data was not accurate, up to date and complete. These requirements are summarised below.

In what circumstances must a consumer be advised that disclosed CDR data was incorrect?

11.37 Data holders and accredited data recipients must advise a consumer that some or all of the CDR data was incorrect if the entity:[15]

- has disclosed CDR data after being required or authorised to do so under the CDR Rules, and
- then later becomes aware that the CDR data, when disclosed, was not accurate, up to date and complete, having regard to the purpose for which the data was held.

11.38 Data holders and accredited data recipients may 'become aware' of inaccuracies in CDR data that was previously disclosed if it discovers an inconsistency during normal business practices. Examples include but are not limited to circumstances where:

- information provided by the consumer is inconsistent with CDR data previously disclosed,
- the entity is notified by the consumer or another entity that the CDR data is incorrect, or a practice, procedure or system that the entity has implemented to ensure compliance with the safeguards (such as a periodic audit or monitoring program) indicates that the CDR data previously disclosed was incorrect.

---

[12] Compliance with Privacy Safeguard 13 (correction of CDR data) and where relevant, APP 13 (correction of personal information) for data holders, can also support this example for taking reasonable steps to ensure quality of CDR data.

[13] See section 56AI of the Competition and Consumer Act.

[14] See section 56EN(3) of the Competition and Consumer Act.

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

11.39 When considering whether to advise the consumer that incorrect CDR data was disclosed, it is not relevant whether the entity failed to take reasonable steps. It is sufficient that the CDR data was not accurate, up to date and complete when disclosed.

What information must be provided to the consumer when incorrect CDR data has been disclosed?

11.40 CDR Rule 7.10 requires a data holder or accredited data recipient that has disclosed incorrect CDR data to an accredited person to provide the consumer with a written notice that:

- identifies the accredited person,
- states the date of the disclosure,
- identifies which CDR data was incorrect, and
- states that the data holder must disclose the corrected data to that accredited person if the consumer requests that they do so.

11.41 Where the data holder or accredited data recipient disclosed the incorrect CDR data to an accredited person who was collecting that CDR data on behalf of another accredited person (the 'principal') under a CDR outsourcing arrangement, the data holder or accredited data recipient only needs to identify the principal accredited person in the notice.[16]

11.42 A notice may deal with one or more disclosures of incorrect CDR data.

How must a notice be provided?

11.43 CDR Rule 7.10 requires a data holder to notify the consumer in writing by electronic means after disclosing incorrect data.

11.44 The requirement for this notice to be given by electronic means will be satisfied if the notice is given over email or over the consumer's dashboard.

11.45 The written notice may, for instance, be in the body of an email or in an electronic file attached to an email.

How quickly must the consumer be notified?

11.46 Data holders and accredited data recipients must provide notices to the consumer as soon as practicable, but no more than five business days after the entity becomes aware that some or all of the disclosed data was incorrect.

11.47 The test of practicability is an objective test. The entity should be able to justify that it is not practicable to give notification promptly after becoming aware of the disclosure of incorrect CDR data.[17]

11.48 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 providing the notice.

---

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

[17] Options for providing early notification should, so far as practicable, be built into the entity's processes and systems. For example, processes and systems should be in place to promptly notify a consumer that incorrect CDR data has been disclosed if the entity corrects CDR data (such as in response to a consumer's correction request) that it had disclosed prior to it being corrected.

11.49 The maximum time of five business days will rarely be an appropriate period of time before a notice is given. This maximum period would only be appropriate in circumstances such as where a system error has caused a data holder to disclose incorrect data to a large number of accredited persons in respect of a large number of consumers.

11.50 The five business day period commences on the day after the entity becomes aware that some or all of the disclosed data was incorrect.[18] For example, if the entity becomes aware on 2 August, the five business day period begins on 3 August.

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

Example

Free Bank Ltd is a data holder for a large number of consumers. Hazel authorises Free Bank to disclose her CDR data relating to her residential mortgage product to an accredited person, Credibility Pty Ltd. Soon after the data is disclosed on 1 July, Credibility queries whether the variable interest rate relating to Hazel's repayments is correct.

Free Bank then becomes aware that some of the data was incorrect when disclosed, because the applicable variable interest rate was not correct for a certain period. Within a number of hours, Free Bank is able to provide a notice to Hazel over her consumer dashboard which states that:

- incorrect CDR data was given to Credibility on 1 July
- the data relating to her mortgage repayments was incorrect due to a mistake in the rate contained in the data, and
- Free Bank will be required to disclose the corrected data to Credibility if Hazel requests that they do so.

Free bank has provided Hazel with the notice required under CDR Rule 7.10 and Privacy Safeguard 11, as soon as practicable. (Free bank also ensures that it updates its own data holdings promptly, upon becoming aware of the inaccuracy. Ensuring that known errors are corrected promptly, regardless of how they are identified, is a reasonable step required by s 56EN(1).)

Free Bank then realises that the error is systemic and has caused Free Bank to disclose incorrect CDR data in respect of all similar disclosures to accredited persons since the variable rate change a number of months ago.

Free Bank hires experts to undertake an urgent review of its CDR disclosures and determine the extent of the error. It takes Free Bank almost five business days before it is in a position to send all affected CDR consumers a notice similar to the one given to Hazel.

Free Bank would need to be able to demonstrate that it has sent the affected consumers the required notices as soon as practicable, to ensure compliance with CDR Rule 7.10 and Privacy Safeguard 11.

[18] See section 36 of the *Acts Interpretation Act 1901*.

In what circumstances must an entity disclose corrected CDR data to the original recipient?

11.52 Privacy Safeguard 11 requires data holders and accredited data recipients to disclose corrected CDR data, in accordance with the CDR Rules, to the original recipient[19] of the disclosure if:[20]

- the entity has advised the consumer that some or all of the CDR data was incorrect when the entity disclosed it, and
- the consumer requests in accordance with the CDR rules for the entity to disclose the corrected CDR data.

11.53 The obligation to disclose corrected CDR data applies regardless of whether the entity failed to take reasonable steps to ensure the quality of the CDR data disclosed.

11.54 The term 'corrected CDR data' is not defined in the Competition and Consumer Act. For the purposes of the obligation to disclose corrected CDR data under Privacy Safeguard 11, 'corrected CDR data' includes:

- CDR data which has been corrected in accordance with s 56EP(3)(a)(i), and
- CDR data for which a qualifying statement has been included in accordance with s 56EP(3)(a)(ii).

Record keeping requirements

11.55 If an entity discloses corrected CDR data in accordance with Privacy Safeguard 11,[21] the entity (and, if the data is disclosed to an accredited person, the recipient) must comply with the record keeping requirements under CDR Rule 9.3.

11.56 For data holders, CDR Rule 9.3(1) requires the entity to keep and maintain various records relating to CDR data, including records of disclosures of CDR data made in response to consumer data requests.[22] If corrected data is disclosed, the data holder must keep and maintain a record of both the initial disclosure in which incorrect CDR was disclosed, and the subsequent disclosure in which the corrected data was disclosed. This is because both disclosures are made in response to the original consumer data request. There is no requirement, however, to record the disclosure as either 'correct' or 'incorrect'.

11.57 For accredited data recipients, CDR Rule 9.3(2) requires the recipient to keep and maintain various records relating to CDR data, including records of collections of CDR data under the CDR Rules.[23] This means that, similarly to data holders, accredited data recipients must keep

---

[19] The original recipient may be the consumer where the data holder disclosed the CDR data to the consumer in response to a valid consumer request in accordance with CDR Rule 3.4(2) or (3).

[20] Section 56EN(4) of the Competition and Consumer Act. Note that although this subsection is also expressed to apply to accredited data recipients, as there are no CDR Rules for such entities to advise consumers of disclosures of incorrect data under section 56EN(3) of the Competition and Consumer Act, the obligation in section 56EN(4) does not currently apply to those entities.

[21] Section 56EN(4) of the Competition and Consumer Act.

[22] CDR Rule 9.3(1)(d). For further information on record keeping requirements for data holders, see the Guide to privacy for data holders.

[23] CDR Rule 9.3(2)(e).

and maintain a record of both the initial collection of the incorrect CDR data and the subsequent collection of the corrected CDR data, in circumstances where corrected CDR data is disclosed under s 56EN(4).

How does Privacy Safeguard 11 interact with the other privacy safeguards?

Privacy Safeguard 5

11.58 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.

11.59 Where an accredited data recipient 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 data recipient must notify that consumer under Privacy Safeguard 5 in respect of both collections.

Privacy Safeguard 10

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

11.61 Where a data holder has disclosed CDR data, and then discloses corrected data as the result of the consumer's request 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.

Example

McCarthy Bank Ltd, a data holder, discloses Satoko's CDR data to accredited person, Watson and Co, in response to a consumer data request made on Satoko's behalf.

McCarthy Bank updates Satoko's consumer dashboard under Privacy Safeguard 10 and CDR Rule 7.9, and Watson and Co updates Satoko's consumer dashboard under Privacy Safeguard 5 and CDR Rule 7.4.

However, Satoko realises that the CDR data disclosed by McCarthy Bank is not accurate, and asks McCarthy Bank to disclose the correct data to Watson and Co.

McCarthy Bank corrects the CDR data in accordance with Privacy Safeguard 13 and CDR Rule 7.15. McCarthy Bank also takes reasonable steps to correct their own data holdings per Privacy Safeguard 11, as they are made aware of inaccuracies through Satoko's disclosure request.

McCarthy Bank then complies with Satoko's request to disclose corrected CDR data. Both Watson and Co and McCarthy Bank update Satoko's consumer dashboards accordingly.

Privacy Safeguard 12

11.62 Where an accredited data recipient amends CDR data to comply with Privacy Safeguard 11, it should consider whether it needs to take action under Privacy Safeguard 12 to destroy or de-identify the original data.

Privacy Safeguard 13

11.63 As set out in Chapter 13 (Correction of CDR data), a correction request made under Privacy Safeguard 13 may trigger the obligations under Privacy Safeguard 11.

11.64 Privacy Safeguard 13 requires data holders and accredited data recipients to respond to a consumer request for correction of their CDR data, where that data has previously been disclosed under the CDR Rules. In response to a consumer request under Privacy Safeguard 13, CDR entities must either correct the CDR data, include a qualifying statement with the CDR data to ensure it is accurate, up to date, complete and not misleading (having regard to the purpose for which it is held), or state why a correction is unnecessary or inappropriate.[24]

11.65 Where a data holder corrects CDR data or includes a qualifying statement with the data in accordance with Privacy Safeguard 13, they should also consider whether the consumer must be advised of any previous disclosures of the CDR data where the data may have been incorrect when it was disclosed, in accordance with Privacy Safeguard 11. In such circumstances, the data holder will be on notice that the CDR data was likely incorrect when disclosed.

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