Chapter 11:

Privacy Safeguard 11 —

Quality of CDR data

Version 5.0, November 2023

OAIC

Contents

Key points

- Privacy Safeguard 11,[1] together with rule 7.10 of the consumer data rules (CDR Rules), 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 if they become aware they disclosed incorrect CDR data, and
  - disclose corrected CDR data to the original recipient if requested to do so by the affected consumer.
- The Australian Energy Market Operator Limited (AEMO) is not subject to Privacy Safeguard 11 in its capacity as a data holder.[2] Accordingly, unless otherwise indicated, all references in this Chapter to data holders exclude AEMO.

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,[3] 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.[4]

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.[5]

---

[1] Competition and Consumer Act, section 56EN.

[2] Competition and Consumer Regulations, sub-regulation 28RA(4). For further information, see paragraph 11.10.

[3] Privacy Safeguard 11 does not apply to AEMO in its capacity as a data holder. Privacy Safeguard 11 does not apply to retailers for data AEMO holds that AEMO has disclosed to the retailer and that the retailer is required or authorised to disclose under the CDR Rules. See the Competition and Consumer Regulations and pages 3–4 of the Explanatory Statement to the Competition and Consumer Amendment (Consumer Data Right) Regulations 2021. For further information, see paragraph 11.10.

[4] 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 Competition and Consumer Act, subsection 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 Competition and Consumer Act, subsection 56EN(4A)). However, no such Rules have been made as at the date of publication of this Chapter 11.

[5] See Competition and Consumer Act, subsection 56EN(5). This is applicable to subsections 56EN(1), (2) and (3)(b).

11.3 Rule 7.10 of the CDR Rules requires data holders[6] 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 to whom the CDR data was disclosed
- 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.

11.5 This notice must be provided to the consumer as soon as practicable, but no more than 5 business days after the data holder or accredited data recipient becomes 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 system.

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 disclose corrected data to the relevant accredited person.

11.8 This allows consumers to enjoy the benefits of the CDR system, 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.

11.10 Privacy Safeguard 11 does not apply to designated gateways or AEMO. Data holders that are retailers in the energy sector also do not have Privacy Safeguard 11 obligations in relation to CDR data held by AEMO that AEMO has disclosed to them.[7] Retailers must comply with Privacy Safeguard 11 in respect to their own data holdings.

11.11 As a non-accredited entity, a CDR representative is not directly bound by Privacy Safeguard 11. However, under the terms of the CDR representative arrangement with their CDR representative principal,[8] a CDR representative is required to comply with Privacy Safeguard

[6] Privacy Safeguard 11 does not apply to AEMO in its capacity as a data holder. Privacy Safeguard 11 does not apply to retailers for data AEMO holds that AEMO has disclosed to the retailer and that the retailer is required or authorised to disclose under the CDR Rules. See the Competition and Consumer Regulations and pages 3–4 of the Explanatory Statement to the Competition and Consumer Amendment (Consumer Data Right) Regulations 2021. For further information, see paragraph 11.10.

[7] See the Competition and Consumer Regulations and pages 3–4 of the Explanatory Statement to the Competition and Consumer Amendment (Consumer Data Right) Regulations 2021.

[8] A CDR representative arrangement is a written contract between a CDR representative and their CDR representative principal that meets the minimum requirements listed in subrules 1.10AA(1), (3) and (4) in the CDR Rules.

11 in its handling of service data as if it were the CDR representative principal.[9,10] A CDR representative principal breaches subrule 7.10A(1) in the CDR Rules if its CDR representative fails to comply with Privacy Safeguard 11 (subsection 56EN(2)) as if it were an accredited person (regardless of whether the CDR representative's actions accord with the CDR representative arrangement).[11]

How Privacy Safeguard 11 interacts with the Privacy Act

11.12 It is important to understand how Privacy Safeguard 11 interacts with the *Privacy Act 1988* (the Privacy Act) and APPs.[12]

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

11.14 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.

11.15 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 system.

11.16 Data holders (including AEMO) 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.[13]

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 the disclosure of corrected CDR data. [14]

[9] CDR Rules, paragraph 1.10AA(4)(a)(iii).

[10] See Chapter B (Key concepts) for more information on 'CDR representative principal', 'CDR representative', 'CDR representative arrangement' and 'service data'.

[11] CDR Rules, rule 7.10A. See also rule 1.16A in relation to a CDR representative principal's obligations and liability.

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

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

[14] 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 Competition and Consumer Act, section 56AK.

CDR entity	Privacy protections that apply in the CDR context
	The APPs do not apply to accredited data recipients in relation to that CDR data. [15]
Data holder (other than AEMO)	**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 system. **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.[16]
Data Holder (AEMO)	**APP 10 and APP 13** Privacy Safeguard 11 does not apply to AEMO as a data holder.
Designated gateway	**APP 10 and APP 13** Privacy Safeguard 11 does not apply to a designated gateway.

What are the quality considerations?

11.17 The 3 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).

11.18 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.

11.19 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 system. 'Purpose' is discussed further in Chapter B (Key concepts).

[15] The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data: Competition and Consumer Act, paragraph 56EC(4)(a). However, subsection 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 Privacy Act, subsection 6E(1D)). Subsection 56EC(4) of the Competition and Consumer Act 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 Competition and Consumer Act, paragraph 56EC(5)(aa).

[16] 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 is inaccurate, out of date, incomplete, irrelevant or misleading.

Example 1 – data holder (banking sector)

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 – data holder (energy sector)

Eager Energy is a retailer and a data holder in the energy sector.

Eager Energy receives a consumer data request from Mustafa, requesting that Eager Energy share Mustafa's billing and metering information with OliveCompare.[17] Eager Energy follows the process in the CDR Rules to obtain the metering data for Mustafa's account from AEMO.[18]

When Eager Energy is required or authorised to disclose Mustafa's CDR data to OliveCompare under the CDR Rules, Privacy Safeguard 11 requires Eager Energy to take reasonable steps to ensure the billing data is accurate, up to date and complete having regard to its purpose. However, Eager Energy does not have to comply with Privacy Safeguard 11 with respect to the metering data it obtained from AEMO.[19]

Example 3 – accredited data recipient

Vikingforce is an accredited data recipient that 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.

11.20 The 3 terms listed in Privacy Safeguard 11, 'accurate', 'up to date', and 'complete', are not defined in the Competition and Consumer Act 2010 (Competition and Consumer Act) or the Privacy Act.[20]

[17] Metering data is a type of AEMO data: CDR Rules, clause 1.2 of Schedule 4.

[18] AEMO data is specified as SR data for the energy sector: see CDR Rules, clause 4.3 of Schedule 4. For the application of rules in relation to SR data, see Division 1.5 of Part 1 of the CDR Rules.

[19] Regulation 28RA(4) of the Competition and Consumer Regulations; pages 3–4 of the Explanatory Statement to the Competition and Consumer Amendment (Consumer Data Right) Regulations 2021.

[20] 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)).

11.21 The following analysis of each term draws on the ordinary meaning of the terms and the APP Guidelines.[21] As the analysis indicates, there is overlap in the meaning of the terms.

Accurate

11.22 CDR data is inaccurate if it contains an error or defect or is misleading. An example is factual information about a consumer's contact details, account, income, assets, payment or repayment history or employment status which is incorrect having regard to the purpose for which it is held.

11.23 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.[22] 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).

11.24 For instance, an accredited data recipient may use the existing information it holds about a consumer to predict their 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 (that is, 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.

11.25 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

11.26 CDR data is not up to date if it contains information that is no longer current at, or during, the time that the data holder is required or authorised to disclose the CDR data. An example is a statement that a consumer has an active account with a certain entity, where the consumer has closed that account before the time that the data disclosure occurred. Another example is an assessment that a consumer has the ability to meet a loan repayment obligation, where in fact the consumer's ability to do so changed in the period before the data disclosure was required or authorised.[23]

11.27 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 at the time it is disclosed 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.

11.28 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.

---

[21] See APP Guidelines, Chapter 10 (APP 10).

[22] Data derived from CDR data continues to be 'CDR data': see Competition and Consumer Act, section 56AI.

[23] Such an assessment will likely be 'materially enhanced information' under section 10 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, or section 11 of the Consumer Data Right (Energy Sector) Designation 2020, and therefore not 'required consumer data' under the CDR Rules.

Complete

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

11.30 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.

Taking reasonable steps to ensure the quality of CDR data

When must an entity take reasonable steps?

11.31 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 rule 4.6 in the CDR Rules, and
  - to consumers under rule 3.4 in the CDR Rules
- **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 paragraph 7.5(1)(i) in the CDR Rules[24]
  - the consumer under paragraph 7.5(1)(d) in the CDR Rules
  - an outsourced service provider (OSP) under paragraph 7.5(1)(f) in the CDR Rules
  - a sponsor or affiliate under paragraph 7.5(1)(f) in the CDR Rules
  - a trusted adviser under paragraph 7.5(1)(e) in the CDR Rules
  - a specified person (in the case of a CDR insight) under paragraph 7.5(1)(e) in the CDR Rules
  - a specified person (in the case of a business consumer disclosure) under paragraph 7.5(1)(e) in the CDR Rules, or
  - a CDR representative under paragraph 7.5(1)(j) in the CDR Rules.

[24] Disclosure of CDR data to an accredited person under an 'AP disclosure consent' has been permitted since 1 July 2021: CDR Rules, subrule 7.5A(1).

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

11.33 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 does not have systems in place to maintain data quality, and 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 at that time. There is also a greater risk that the consumer will later request that the data holder correct CDR data it disclosed, meaning the data holder will also need to follow the process in Privacy Safeguard 13.[25]

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, use and disclose for the purposes of APP 10.

What constitutes 'reasonable steps'?

11.34 The requirement to ensure the quality of CDR data is subject to a 'reasonable steps' test.

11.35 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. For example, 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.

[25] For further information, see paragraphs 11.66 to 11.68 and Chapter 13 (Privacy Safeguard 13).

- **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.

11.36 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 accredited data recipient in this example to be able to justify that this is reasonable.

Examples of reasonable steps

11.37 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 other reasonable steps the entity is taking 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.[26]
- 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'.[27]

Advising a consumer when disclosed CDR data is incorrect

11.38 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.[28]

[26] 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.

[27] See Competition and Consumer Act, section 56AI.

[28] See Competition and Consumer Act, subsection 56EN(3).

11.39 Rule 7.10 in the CDR Rules 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?

11.40 Data holders and accredited data recipients must advise a consumer that some or all of the CDR data was incorrect if the entity:[29]

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

11.41 Data holders and accredited data recipients may later 'become aware' of inaccuracies in CDR data that was previously disclosed if they discover 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, or
- the entity is notified by the consumer or another entity that the CDR data is incorrect (this may include a data holder providing corrected data to an accredited data recipient),[30] or
- a practice, procedure or system that the entity has implemented to ensure compliance with the privacy safeguards (such as a periodic audit or monitoring program) indicates that the CDR data previously disclosed was incorrect.

11.42 The obligation to notify the consumer that disclosed CDR data was incorrect is not affected by whether the entity took reasonable steps to ensure the quality of the data. Privacy Safeguard 11 and rule 7.10 of the CDR Rules require the consumer to be notified when, in fact, the CDR data was not accurate, up to date and complete when disclosed, regardless of the reason for the incorrect data.

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

11.43 Rule 7.10 of the CDR Rules requires a data holder or accredited data recipient that has disclosed incorrect CDR data to an accredited person to provide the consumer, via electronic means, with a written notice that:

- identifies the accredited person to whom the incorrect CDR data was disclosed
- states the date of the disclosure

[29] Competition and Consumer Act, subsection 56EN(3).

[30] If a consumer notifies a data holder or accredited data recipient that the CDR data it disclosed was incorrect, the consumer may also request that the entity correct that CDR data. When this happens, Privacy Safeguard 13 will also apply to the data holder or accredited data recipient. For further information see paragraphs 11.66 to 11.68 and Chapter 13 (Privacy Safeguard 13).

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

11.44 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 'OSP principal') as a direct or indirect OSP under a CDR outsourcing arrangement, the data holder or accredited data recipient only needs to identify in the notice the OSP principal accredited person on whose behalf the data was collected.[31]

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

How must a notice be provided?

11.46 Rule 7.10 of the CDR Rules requires a data holder or accredited data recipient to notify the consumer in writing by electronic means after disclosing incorrect data.

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

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

Privacy tip: In selecting an 'electronic means' for the notice, the data holder or accredited data recipient should consider the consumer's chosen method for receiving communications from the entity (if appliable) and whether the consumer is likely to receive the notice in a timely manner through a given 'electronic means'. For example, if a consumer has elected to receive communications from the entity by email, it may be most appropriate to deliver the notice through that means.

How quickly must the consumer be notified?

11.49 Data holders and accredited data recipients must provide notices to the consumer as soon as practicable, but no more than 5 business days after the entity becomes aware that some or all of the disclosed data was incorrect.

11.50 The test of practicability is an objective test. The entity should be able to justify that it is not practicable to give notification more quickly than 5 days after becoming aware of the disclosure of incorrect CDR data.[32]

11.51 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.

11.52 The maximum time of 5 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

[31] CDR Rules, paragraph 1.16(5)(b). For information on 'CDR outsourcing arrangements', see Chapter B (Key concepts).

[32] 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.

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.

11.53 The 5 business day period commences on the day after the entity becomes aware that some or all of the disclosed data was incorrect.[33] For example, if the entity becomes aware on 2 August, the 5 business day period begins on 3 August.

11.54 A 'business day' is a day that is not Saturday, Sunday or a public holiday in the place concerned.[34]

Example

Blue Book Ltd is a data holder for a large number of consumers. Hazel authorises Blue Book to disclose her CDR data to an accredited person, Credibility Pty Ltd. Soon after the data is disclosed on 1 July, Credibility queries whether Hazel's account data is correct.

Blue Book then becomes aware that some of the data was incorrect when disclosed because it showed the incorrect address for Hazel. Hazel's address was inaccurate for the purpose for which Blue Book held the information (contacting Hazel). Within a number of hours, Blue Book 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 account data was incorrect due to a mistake in Hazel's address, and
- Blue Book will be required to disclose the corrected data to Credibility if Hazel requests that they do so.

Blue Book has provided Hazel with the notice required under Rule 7.10 in the CDR Rules and Privacy Safeguard 11, as soon as practicable. (Blue Book 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 subsection 56EN(1) of the Competition and Consumer Act (i.e. Privacy Safeguard 11).

Blue Book then realises that the error is systemic and has caused it to disclose incorrect CDR data in respect of all similar disclosures to accredited persons.

Blue Book hires experts to undertake an urgent review of its CDR disclosures and determine the extent of the error. It takes Blue Book almost 5 business days before it is in a position to send all affected CDR consumers a notice similar to the one given to Hazel.

Blue Book 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 Rule 7.10 in the CDR Rules and Privacy Safeguard 11.

[33] See *Acts Interpretation Act 1901,* section 36.

[34] *Acts Interpretation Act 1901*, section 2B.

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

11.55 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[35] of the disclosure if:[36]

- 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, the entity to disclose the corrected CDR data.

11.56 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.

11.57 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 paragraph 56EP(3)(a)(i) of the Competition and Consumer Act, and
- CDR data for which a qualifying statement has been included in accordance with paragraph 56EP(3)(a)(ii) of the Competition and Consumer Act. [37]

Record keeping requirements

11.58 If an entity discloses corrected CDR data in accordance with Privacy Safeguard 11,[38] the entity (and, if the data is disclosed to an accredited person, the recipient) must comply with the record keeping requirements under rule 9.3 in the CDR Rules.

11.59 For data holders, subrule 9.3(1) of the CDR Rules 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.[39] If corrected data is disclosed, the data holder must keep and maintain a record of both the initial disclosure in which incorrect CDR data was disclosed, and the subsequent disclosure in which the corrected CDR 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'.

11.60 For accredited data recipients, subrule 9.3(2) of the CDR Rules requires the recipient to keep and maintain various records relating to CDR data, including records of collections of CDR data under the CDR Rules.[40] This means that, similarly to data holders, accredited data

---

[35] 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 subrules 3.4(2) or (3) in the CDR Rules.

[36] Competition and Consumer Act, subsection 56EN(4).

[37] See Chapter 13 (Privacy Safeguard 13).

[38] Competition and Consumer Act, subsection 56EN(4).

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

[40] CDR Rules, paragraph 9.3(2)(e).

recipients must keep 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 subsection 56EN(4) of the Competition and Consumer Act.

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

Privacy Safeguard 5

11.61 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.

11.62 Where an accredited data recipient has collected CDR data, and then collects corrected CDR data after the data holder complies with the consumer's request 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

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

11.64 Where a data holder has disclosed CDR data, and then discloses corrected CDR data as a result of the consumer's request to correct and disclose corrected CDR 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 rule 7.9 in the CDR Rules, and Watson and Co updates Satoko's consumer dashboard under Privacy Safeguard 5 and rule 7.4 in the CDR Rules.

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

McCarthy Bank corrects the CDR data in accordance with Privacy Safeguard 13 and rule 7.15 in the CDR Rules. McCarthy Bank also takes reasonable steps to correct its own data holdings as required by Privacy Safeguard 11, as it is made aware of inaccuracies through Satoko's request.

In accordance with Privacy Safeguard 11, McCarthy Bank then advises Satoko that Satoko may request that the corrected data be disclosed to Watson and Co. Satoko makes this request, and McCarthy Bank complies. Both Watson and Co and McCarthy Bank update Satoko's consumer dashboards accordingly.

Privacy Safeguard 12

11.65 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

11.66 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.

11.67 Privacy Safeguard 13 applies where a consumer requests that a data holder or accredited data recipient correct their CDR data, where that data has previously been disclosed under the CDR Rules. In most circumstances, Privacy Safeguard 13 requires the data holder or accredited data recipient to respond to the consumer's request by either correcting the CDR data, including 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 stating why a correction is unnecessary or inappropriate.[41]

11.68 Where a data holder corrects CDR data or includes a qualifying statement with the data in accordance with Privacy Safeguard 13, they should be aware that this may trigger Privacy Safeguard 11, meaning 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 such circumstances, the data holder will be on notice that the CDR data was likely incorrect when disclosed.

[41] Competition and Consumer Act, paragraph 56EP(3)(a); CDR Rules, rule 7.15. Privacy Safeguard 13 does not apply to AEMO: Competition and Consumer Regulations, paragraph 28RA(2)(a)(iii). Different obligations apply to retailers who receive a Privacy Safeguard request that relates to AEMO data: clause 6.1 of Schedule 4 to the CDR Rules. For further information, see Chapter 13 (Correction of CDR data).