Chapter 11:

Privacy Safeguard 11 —

Quality of CDR data

Consultation draft, October 2019

OAIC

Contents

Key points

- Privacy Safeguard 11, together with Consumer Data Rule 7.10, sets out obligations for data holders and accredited data recipients to:
  - ensure the quality of disclosed CDR data
  - inform CDR consumers in the event incorrect CDR data is disclosed, and
  - disclose corrected CDR data to the original recipient where requested by the affected CDR 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 Consumer Data Rules, and
- accredited data recipients who are disclosing CDR data when authorised or required under the Consumer Data 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 CDR consumer in accordance with the Consumer Data 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 CDR consumer to disclose corrected CDR data to the original recipient.

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

11.3 Consumer Data Rule 7.10 requires a data holder who has disclosed incorrect CDR data to an accredited person to provide the CDR consumer with a written notice that identifies the accredited person and the incorrect CDR data, states the date of the disclosure, and states that the data holder must disclose the corrected data to that accredited person if the consumer requests them to do so.

Why is it important?

11.4 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.

11.5 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.

11.6 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?

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

How does Privacy Safeguard 11 interact with the Privacy Act?

11.8 It is important to understand how Privacy Safeguard 11 interacts with the Privacy Act 1988 (the Privacy Act) and Australian Privacy Principles (APPs).[1]

11.9 Like Privacy Safeguard 11, APP 10 requires APP entities to take reasonable steps to ensure the quality of personal information in certain circumstances.

11.10 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.

11.11 Although Privacy Safeguard 11 applies only in relation to the *disclosure* of CDR data, good practices and procedures to 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.

Summary of application of Privacy Safeguard 11

CDR entity	Privacy principle that applies to CDR data
Accredited person	**Australian Privacy Principle 10** APP 10 applies to any personal information held by accredited persons who are not yet accredited data recipients.[2]
Accredited data recipient	**Privacy Safeguard 11** Privacy Safeguard 11 applies instead of APP 10,[3] meaning APP 10 will not apply to CDR data that has been received by an accredited data recipient through the CDR regime. APP 10 will continue to apply to any personal information collected by the accredited person that is not CDR data.[4]

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

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

[3] 56EC(4)(a).

[4] All accredited persons are subject to the Privacy Act and the APPs in relation to information that is personal information but is not CDR data. This means that non-CDR personal information handling by accredited persons is covered by the

CDR entity	Privacy principle that applies to CDR data
Data holder	**Privacy Safeguard 11** Privacy Safeguard 11 applies instead of APP 10 for a disclosure of CDR data, [5] meaning APP 10 will not apply to CDR data that a data holder is authorised or required to disclose under the Consumer Data Rules. However, APP 10 continues to apply to data holders in respect of the collection and use of CDR data that is also personal information, and in respect of CDR data that is also personal information which is disclosed otherwise than under the Consumer Data Rules (for instance, to a third party service provider). This means that APP 10 continues to apply to all personal information (and CDR data that is also personal information) that a data holder collects, uses or discloses where the entity is not required or authorised to disclose the data under the Consumer Data Rules.
Designated gateway	**Australian Privacy Principle 10** Privacy Safeguard 11 does not apply to a designated gateway, meaning the obligation to ensure the quality of personal information in APP 10 will continue to apply to a designated gateway that is an APP entity.

What are the quality considerations?

11.12 The three quality considerations under Privacy Safeguard 11 are '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**.

11.13 When working out the purpose for which the CDR data is or was held, entities should disregard the purpose of holding the CDR data so that it can be disclosed as required under the Consumer Data Rules. 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).

11.14 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.[6] The following analysis of each term draws on the ordinary meaning of the terms and the APP Guidelines.[7] As the analysis indicates, there is overlap in the meaning of the terms.

Privacy Act and the APPs, while the handling of CDR data is covered by the CDR regime and the Privacy Safeguards. See s 6E(1D) of the Privacy Act.

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

[6] 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 CDR consumer to correct the CDR data (see Chapter 13 (Privacy Safeguard 13)).

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

Accurate

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

11.16 CDR data that is derived from other CDR data is not inaccurate by reason only that the consumer disagrees with the method or result of the derivation. For the purposes of Privacy Safeguard 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 an algorithm to determine a CDR consumer's projected income over a certain period of time. If the data is presented as the estimated future income for the consumer for that period, and states the bases of the estimation, it will not be inaccurate because, for instance, the consumer believes their income will be higher or lower during the projected period.

Up to date

11.17 CDR data is not up to date if it contains information that is no longer current. An example is a statement that a CDR consumer has an active account with a certain bank, where the consumer has 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.[8]

11.18 For example, CDR data about a past event may have been accurate at the time it was recorded but has been overtaken by a later development. Whether that data is up to date will depend on the purpose for which it is held.

Complete

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

11.20 An example is data from which it can be inferred that a CDR consumer owes a debt, which in fact has been repaid. The CDR data will be incomplete under Privacy Safeguard 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.

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

Taking reasonable steps to ensure the quality of CDR data

When must an entity take reasonable steps?

11.21 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 Consumer Data Rules
- **for accredited data recipients**, at the time the entity discloses CDR data when required or authorised under the Consumer Data Rules.

11.22 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.

11.23 Entities should also be aware that Privacy Safeguard 11 only requires an accredited data recipient to take reasonable steps when disclosing CDR data under the Consumer Data 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 consumer data rules' is discussed in Chapter B (Key Concepts).

11.24 The obligation to take reasonable steps to ensure the quality of CDR data applies to accredited data recipients when disclosing CDR data:

- to the CDR consumer under Consumer Data Rules 7.5(1)(c) or 7.5(3), and
- to an outsourced service provider under Consumer Data Rule 7.5(1)(d).

Risk point: If a data holder only takes steps to ensure the quality of CDR data 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 only applies 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.

What constitutes 'reasonable steps'?

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

11.26 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.** An entity should consider the sensitivity of the data and possible adverse consequences for the consumer concerned if the CDR data is not correct. If a data holder is required or authorised to disclose data that is highly sensitive, the data holder would be required to take more extensive steps to ensure the quality of that data.
- **The possible adverse consequences for a consumer if the quality of CDR data is not ensured.** More rigorous steps may be required as the risk of adversity increases.
- **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.

11.27 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, 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

11.28 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.
- 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 (such as algorithms) are operating appropriately and are fit for purpose, and not creating biased, inaccurate, discriminatory or unjustified results. This is because data derived from CDR data collected by an accredited data recipient continues to be 'CDR data'.

Advising a CDR consumer when disclosed CDR data is incorrect

11.29 Consumer Data Rule 7.10 sets out the notice requirements with which a data holder must comply after disclosing incorrect CDR data to an accredited person. These notice requirements are summarised in paragraphs 11.31-11.42 below.

11.30 Consumer Data Rule 7.10 does not apply to accredited data recipients. There is no Consumer Data Rule in relation to accredited data recipients advising CDR consumers that disclosed CDR data was incorrect.

Data holders

When must a data holder advise a CDR consumer that disclosed CDR data was incorrect?

11.31 A data holder must advise a CDR consumer that some or all of the CDR data was incorrect if the entity[9]

- has disclosed CDR data after being required or authorised to do so under the Consumer Data Rules, and
- then 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.

11.32 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 outlined in paragraph 11.25-11.27 of this chapter. It is sufficient that the CDR data was not accurate, up to date and complete when disclosed.

What information must a data holder provide to the consumer when incorrect CDR data has been disclosed?

11.33 Consumer Data Rule 7.10 requires a data holder 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.

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

How must a notice be provided?

11.35 Consumer Data Rule 7.10 requires a data holder to notify the consumer by electronic means after disclosing incorrect data.

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

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

[9] 56EN(3).

How quickly must data holders give notification to the consumer?

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

11.39 The term 'as soon as practicable' is discussed in Chapter B (Key Concepts).

11.40 The test of practicability is an objective test. The data holder should be able to justify that it is not practicable to give notification promptly after becoming aware of the disclosure of incorrect CDR data.[10]

11.41 In adopting a timetable that is 'practicable' an entity can take technical and resource considerations into account. However, it is the responsibility of the data holder to be able to justify any delay in providing the notice.

11.42 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 CDR consumers.

Example

Free Bank Ltd is a data holder for a large number of CDR consumers. It is authorised by Yulia 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 Yulia's repayments is correct.

Free Bank then becomes aware that some of the disclosed 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 practicably able to provide a notice to Yulia 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 is required to disclose corrected data to Credibility if Yulia requests that they do so.

Free bank has electronically provided Yulia with the notice required under Consumer Data Rule 7.10 and Privacy Safeguard 11, as soon as practicable.

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

[10] 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 CDR 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.

Free Bank hires external counsel and other 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 Yulia.

Although Free Bank has taken almost 5 business days to send the affected CDR consumers the notices required by Consumer Data Rule 7.10 and Privacy Safeguard 11, it has done so as soon as practicable.

Accredited data recipients

Does an accredited data recipient need to advise CDR consumers if disclosed CDR data was incorrect?

11.43 For accredited data recipients, there is no Consumer Data Rule in relation to advising CDR consumers that disclosed CDR data was incorrect. This is because an accredited data recipient may only disclose CDR data if required or authorised under another Australian law or court/tribunal order,[11] or under the Consumer Data Rules to the consumer or an outsourced service provider.

11.44 If an accredited data recipient discloses CDR data:

- to the consumer, or an outsourced service provider in accordance with the Consumer Data Rules; or
- as required or authorised under another Australian law or court/tribunal order,

and that data is incorrect, the requirement to advise the CDR consumer does not apply as there are no Consumer Data Rules for the entity to follow.

Disclosing corrected CDR data to the original recipient

When must an entity disclose corrected CDR data to the original recipient?

11.45 Privacy Safeguard 11 requires a data holder to disclose corrected CDR data to the original recipient[12] of the disclosure if:[13]

- the entity has advised the CDR consumer that some or all of the CDR data was incorrect when the entity disclosed it, and

[11] 56EI(1)(c).

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

[13] 56EN(4). Note that although this subsection is also expressed to apply to accredited data recipients, as there are no Consumer Data Rules for such entities to advise CDR consumers of disclosures of incorrect data under 56EN(3), the obligation in 56EN(4) does not currently apply to those entities.

- the CDR consumer requests the entity to disclose the corrected CDR data.

11.46 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.

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

11.48 This means that if a data holder includes a qualifying statement with CDR data rather than correcting it in response to a request from the CDR consumer to correct the data, and the CDR data had been disclosed to an accredited person before the qualifying statement was included, Privacy Safeguard 11 requires the data holder to re-disclose that CDR data, which now includes the qualifying statement, to that accredited person.

Example

SuperGas Ltd is a data holder for CDR data. On 1 May, SuperGas discloses Gudny's CDR data to an accredited person in response to Gudny's valid request. The CDR data includes readings from a gas meter at Gudny's residence that, for reasons outside SuperGas' control, is faulty.

After receiving her latest gas bill, Gudny realises that the gas meter is faulty and notifies SuperGas through the customer service portal on its website. SuperGas arranges for the meter to be fixed.

SuperGas determines that the gas usage data it holds for Gudny is inaccurate, given that it is held for the purposes of billing Gudny under her gas contract and allowing Gudny to track her usage, among other things.

SuperGas notifies Gudny over her consumer dashboard in compliance with Consumer Data Rule 7.10. The notice states that the gas usage data disclosed to the accredited person was incorrect, due to the faulty readings.

Gudny requests SuperGas to disclose corrected data to the recipient.

This example is continued below.

Record keeping requirements

11.49 If an entity discloses corrected CDR data in accordance with Privacy Safeguard 11,[14] the entity (and, if the data is disclosed to an accredited person, the recipient) should ensure that they comply with the record keeping requirements under Consumer Data Rule 9.3.

11.50 For data holders, Consumer Data 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.[15]If corrected data is disclosed, the data holder must

[14] 56EN(4).

[15] Consumer Data Rule 9.3(1)(d).

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.

11.51 For accredited data recipients, Consumer Data Rule 9.3(2) requires the recipient to keep and maintain various records relating to CDR data, including records of the types of CDR data collected under the Consumer Data Rules.[16] There is no requirement for an accredited data recipient to keep and maintain a record of the collection of the corrected data. However, the accredited data recipient is required to notify the consumer of the collection (see 11.54 below).

How does Privacy Safeguard 11 interact with the other Privacy Safeguards?

Privacy Safeguard 1

11.52 Privacy Safeguard 1 requires entities to take reasonable steps to establish and maintain practices, procedures, and systems to ensure compliance with the Privacy Safeguards, including Privacy Safeguard 11.

Privacy Safeguard 5

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

11.54 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

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

11.56 Where a data holder has disclosed CDR data, and then discloses corrected data as the result of the consumer's requests to correct and disclose corrected data under Privacy Safeguards 11 and 13, the data holder must notify that consumer under Privacy Safeguard 10 in respect of both disclosures.

Example

Phoney Phones Ltd, a data holder, discloses Satoko's CDR data to accredited person, Bill Balancer Pty Ltd, in response to a consumer data request made on Satoko's behalf.

Phoney Phones updates Satoko's consumer dashboard under Privacy Safeguard 10 and Consumer Data Rule 7.9, and Bill Balancer updates Satoko's consumer dashboard under Privacy Safeguard 5 and Consumer Data Rule 7.4.

[16] Consumer Data Rule 9.3(2)(e).

Phoney Phones, through its own inquiries, then becomes aware that the data was incorrect when disclosed.

Pursuant to Privacy Safeguard 11 and Consumer Data Rule 7.10, Phoney Phones advises Satoko that incorrect data was disclosed, through her consumer dashboard.

Satoko requests Phoney Phones to disclose corrected CDR data to Bill Balancer under Privacy Safeguard 11.[17]

Phoney Phones corrects the CDR data in accordance with Privacy Safeguard 13 and Consumer Data Rule 7.15.

Phoney Phones complies with Satoko's request to disclose corrected CDR data. Both Bill Balancer and Phoney Phones update Satoko's consumer dashboards accordingly.

Privacy Safeguard 12

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

Privacy Safeguard 13

11.58 Privacy Safeguard 13 requires data holders and accredited data recipients to respond to a CDR consumer request for correction of their CDR data including by taking steps to correct the CDR data or by including a qualifying statement with the CDR data to ensure its accuracy.[18]

11.59 A data holder that corrects CDR data or includes a qualifying statement with the data in accordance with Privacy Safeguard 13 should consider whether the CDR 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 CDR data was likely incorrect when disclosed.

Example

This example follows the example under the heading 'When must an entity disclose corrected CDR data to the original recipient?', above.

SuperGas receives Gudny's request to disclose her corrected CDR data. A SuperGas customer service officer promptly sends Gudny an email acknowledging receipt of her request.

This request is necessarily also a request under Privacy Safeguard 13 to correct the data. SuperGas determines that it cannot correct the CDR data as there is no method of determining Gudny's actual gas usage for the period in which the gas meter was faulty.

[17] As explained in 13.50 of Chapter 13 (Privacy Safeguard 13), a request under section 56EN(4) is necessarily a request for the data holder to correct the CDR data under 56EP(1).

[18] 56EP(3)(a).

SuperGas therefore includes a statement with the CDR data that, for the particular period, there was a fault with the gas meter which recorded the data and the exact gas usage cannot be accurately determined. SuperGas also attaches an electronic link to its digital record of the data.

SuperGas then sends Gudny both an email and a message through her consumer dashboard explaining that SuperGas has included the statement with her data, as correction of the data was not possible, and sets out the complaint mechanisms available to her.

SuperGas then re-discloses the data, which now includes the qualifying statement, to the accredited person.