Chapter 10:

Privacy Safeguard 10 —

Notifying of the disclosure of CDR data

Version 5.0, November 2023

OAIC

Contents

Key points

- Where a data holder of a consumer's CDR data discloses that data to an accredited person as a result of a consumer data request, the data holder must notify the consumer by updating each consumer dashboard that relates to the request.[1]
- Where an accredited data recipient of a consumer's CDR data discloses that data to an accredited person or a trusted adviser, or discloses a CDR insight or a CDR business consumer's CDR data to a specified person, they must notify the consumer by updating each consumer dashboard that relates to the request.[2]
- The consumer data rules (CDR Rules) set out the matters that must be included in, and the timing of, these notifications.
- The Australian Energy Market Operator Limited (AEMO) is not subject to Privacy Safeguard 10 in its capacity as a data holder.[3] Accordingly, unless otherwise indicated, references in this Chapter to data holders exclude AEMO.

What does Privacy Safeguard 10 say?

10.1 Where a data holder is required or authorised under the CDR Rules to disclose CDR data, they must notify the consumer by taking the steps identified in the CDR Rules.[4]

10.2 Where an accredited data recipient of a consumer's CDR data discloses CDR data, they must notify that consumer by taking the steps identified in the CDR Rules.[5]

10.3 The notification must:

- be given to those consumers that the CDR Rules require to be notified
- cover the matters set out in the CDR Rules, and
- be given at or before the time specified in the CDR Rules.

10.4 Under rule 7.9 in the CDR Rules, data holders and accredited data recipients of a consumer's CDR data must notify the consumer by updating each relevant consumer dashboard to include certain matters as set out in that Rule as soon as practicable after CDR data is disclosed.[6]

---

[1] *Competition and Consumer Act 2010* (Competition and Consumer Act), subsection 56EM(1) and CDR Rules, subrule 7.9(1).

[2] Competition and Consumer Act, subsection 56EM(2) and CDR Rules, subrule 7.9(2)-(4).

[3] Competition and Consumer Regulations, paragraph 28RA(2)(b). For information about how Privacy Safeguard 10 applies to retailers who receive CDR data from AEMO, see paragraph 10.10.

[4] Competition and Consumer Act, subsection 56EM(1). For further information on 'required or authorised to use or disclose CDR data under the CDR Rules', refer to Chapter B (Key concepts).

[5] Competition and Consumer Act, subsections 56EM(2), (3) and (4).

[6] A CDR consumer in the energy sector may elect not to have a data holder dashboard: CDR Rules, clause 2.3 of Schedule 4. In these circumstances, as there is no data holder dashboard that relates to the consumer data request, the data holder would not be able to update any dashboard for the purposes of rule 7.9 in the CDR Rules.

Why is it important?

10.5 Notification of disclosure of CDR data is an integral element of the CDR system, as it provides confirmation to consumers that their CDR data has been disclosed in response to a consumer data request.

10.6 This ensures consumers are informed when their CDR data is disclosed and builds trust between consumers, data holders and accredited data recipients.

Who does Privacy Safeguard 10 apply to?

10.7 Privacy Safeguard 10 applies to data holders and accredited data recipients of CDR data. It does not apply to designated gateways.

10.8 Where an accredited data recipient is a CDR representative principal under a CDR representative arrangement, a disclosure of service data by a CDR representative (or by a direct or indirect outsourced service provider (OSP) of the CDR representative) is taken to be a disclosure by the CDR representative principal.[7] This means that, where a CDR representative (or their direct or indirect OSP) discloses a consumer's CDR data, the CDR representative principal must notify that consumer of the disclosure under Privacy Safeguard 10, although it may arrange for its CDR representative to do so on its behalf.[8]

10.9 If an accredited person who is a direct or indirect OSP discloses CDR data that was collected on behalf of another accredited person (the 'OSP principal') under a CDR outsourcing arrangement, only the OSP principal is required to notify the relevant consumer/s of the disclosure for the purposes of Privacy Safeguard 10.[9] Similarly, where an unaccredited person who is a direct or indirect OSP discloses CDR data under a CDR outsourcing arrangement, the OSP principal is required to notify the relevant consumer/s of the disclosure for the purposes of Privacy Safeguard 10.[10]

10.10 Privacy Safeguard 10 does not apply to AEMO in its capacity as a data holder.[11] Instead, data holders that are retailers in the energy sector (primary data holders)[12] must comply with Privacy Safeguard 10 in relation to AEMO data that they disclose (in addition to having Privacy Safeguard 10 obligations with respect to their own data holdings).[13]

[7] CDR Rules, subrule 7.9(5).

[8] CDR Rules, subrule 4.19(2).

[9] CDR Rules, subrule 1.16(5) and rule 7.9.

[10] CDR Rules, subrule 7.6(2) and rule 7.9.

[11] Competition and Consumer Regulations, paragraph 28RA(2)(b).

[12] See Chapter B (Key concepts) for further information about primary data holders.

[13] Competition and Consumer Regulations, paragraph 28RA(3)(b).

How Privacy Safeguard 10 interacts with the Privacy Act

For data holders

10.11 Data holders must comply with Privacy Safeguard 10 when they are required or authorised to disclose CDR data (including SR data)[14] under the CDR Rules.

10.12 There is no corresponding obligation under the *Privacy Act 1988* (the Privacy Act) or the APPs to notify an individual of the disclosure of their personal information.

10.13 However, APP 5 will continue to apply in relation to the notification of the collection of CDR data that is also personal information.[15]

For accredited data recipients

10.14 For an accredited data recipient of a consumer's CDR data, Privacy Safeguard 10 applies whenever they disclose that consumer's data.

10.15 The APPs do not apply to an accredited data recipient of CDR data, in relation to that CDR data.[16]

Who must be notified?

For data holders

10.16 The data holder must notify the consumer(s) for the disclosed CDR data by updating each consumer dashboard that relates to the request.[17]

10.17 There may be more than one consumer for the CDR data with a dashboard that relates to the request. A key example is CDR data relating to a joint account. In this case, the data holder must notify each of the requesting and non-requesting joint account holders. However, a data holder is not liable for a failure to notify the non-requesting joint account holder/s where the data holder considers this necessary to prevent physical, psychological or financial harm or abuse.[18]

---

[14] For further information on SR data, see Chapter B (Key concepts). In the energy sector, AEMO data in relation to a CDR consumer is SR data: CDR Rules, clause 4.3 of Schedule 4.

[15] For example, the obligations in APP 5.2 (f), (i) and (j) to notify individuals of the situations in which their personal information may be disclosed in future.

[16] 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) 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).

[17] Competition and Consumer Act, paragraph 56EM(1)(b) and CDR Rules, subrule 7.9(1). See paragraph 10.24for information about situations where there is no dashboard that relates to the request.

[18] Rule 4A.15 in the CDR Rules provides that the data holder is not liable under the CDR Rules for failure to comply with Part 4A (including the requirement to provide and update a dashboard) if the data holder considers that the relevant act or omission was necessary in order to prevent physical, psychological or financial harm or abuse.

10.18 This exception to notification is to accommodate existing procedures a data holder may have to protect consumers, for example particular arrangements relating to consumers that may be experiencing family violence.

10.19 Where the CDR data disclosed relates to an account with a secondary user[19] and the secondary user has a consumer dashboard that relates to the request,[20] the data holder must notify both the account holder and secondary user.[21]

10.20 Where the CDR data disclosed relates to a non-individual consumer or is in relation to a partnership account, the data holder must notify the relevant nominated representative.[22]

For accredited data recipients

10.21 The accredited data recipient must notify the consumer who provided the disclosure consent.[23]

How must notification be given?

For data holders

10.22 A data holder must provide the notification by updating each consumer dashboard that relates to the request (including, if applicable, the dashboard of the other joint account

[19] A person is a secondary user for an account with a data holder if the person has 'account privileges' in relation to the account, and the account holder has given the data holder an instruction to treat the person as a secondary user for the purposes of the CDR Rules (CDR Rules, rule 1.7). 'Account privileges' for the banking sector are defined in clause 2.2 of Schedule 3 to the CDR Rules. 'Account privileges' for the energy sector are defined in clause 2.2 of Schedule 4 to the CDR Rules.

[20] A data holder will provide a secondary user with a dashboard when the secondary user is the CDR consumer on whose behalf the accredited person made the consumer data request: CDR Rules, rule 1.15. See footnote 6 regarding when a data holder dashboard will be provided to a CDR consumer in the energy sector.

[21] The application of CDR Rules relating to secondary users is staged in the banking and energy sectors. For the meaning of staged application, see Chapter B (Key concepts). For staged application of CDR Rules in the banking sector, see CDR Rules, clause 6.7 of Schedule 3. For staged application of CDR Rules in the energy sector, see CDR Rules, clauses 8.16 and 8.6 of Schedule 4. Data holders should carefully review the staged application provisions relevant to each sector when considering their obligations under the Privacy Safeguards.

[22] The application of CDR Rules relating to partnerships is staged in the banking and energy sectors. For the meaning of staged application, see Chapter B (Key concepts). For staged application of CDR Rules in the banking sector, see CDR Rules, clause 6.7 of Schedule 3. For staged application of CDR Rules in the energy sector, see CDR Rules, clauses 8.1 and 8.6 of Schedule 4. Data holders should carefully review the staged application provisions relevant to each sector when considering their obligations under the Privacy Safeguards.

A 'nominated representative' is the individual nominated by the non-individual consumer under paragraphs 1.13(c)(i) or 1.13(d)(i) in the CDR Rules who is able to give, amend and manage authorisations to disclose CDR data on behalf of the non-individual consumer. There may be more than one nominated representative.

[23] CDR rules, subrules 7.9(2)-(4). A disclosure consent is a consent given by a consumer for the accredited data recipient to disclose CDR data to an accredited person: for example, in response to consumer data request (an 'AP disclosure consent', an 'insight disclosure consent', a business consumer disclosure consent or a 'TA disclosure consent'), or for the purposes of direct marketing: CDR Rules, paragraph 1.10A(1)(c). For further information, see Chapter C (Consent).

holder/s)[24] to include the matters discussed in paragraphs 10.36 and 10.40 to 10.51 as soon as practicable after CDR data relating to that consumer is disclosed.[25]

10.23 The data holder's consumer dashboard is an online service that must be offered, and in most circumstances must be provided, by a data holder to each consumer (and, if applicable, the other joint account holder/s)[26] where a consumer data request has been made on their behalf by an accredited person. Data holders must include within the dashboard certain details of each authorisation to disclose CDR data that has been given by the consumer.[27]

10.24 If a CDR consumer in the energy sector does not have online access to their account, they may elect not to have a data holder dashboard.[28] In these circumstances, there will be no dashboard that relates to the consumer data request and the data holder would not be able to update any dashboard for the purposes of subrule 7.9(1) in the CDR Rules.

10.25 Further guidance about the data holder's consumer dashboard is set out in Chapter B (Key concepts) and the Guide to privacy for data holders.

For accredited data recipients

10.26 An accredited data recipient must provide the notification by updating the consumer dashboard for the consumer who provided the disclosure consent.[29]

10.27 The accredited data recipient's consumer dashboard is an online service that must be provided by an accredited data recipient to each consumer who has provided a consent in relation to their CDR data. Accredited data recipients must include in the dashboard certain details of each consent that has been given by the consumer.[30]

10.28 Where an accredited data recipient disclosed CDR data that was collected on behalf of another accredited person (the 'principal') under a CDR outsourcing arrangement, only the principal needs to notify the relevant consumer/s by updating the relevant dashboard.[31]

10.29 Further guidance about the accredited data recipient's consumer dashboard is set out in Chapter B (Key concepts) and Chapter C (Consent).

---

[24] Where the CDR data disclosed relates to a joint account, and either the co-approval or pre-approval option applies to that account, the data holder must provide each relevant account holder with a consumer dashboard, and notify each of the joint account holders by updating their consumer dashboards to include those same matters as soon as practicable after the CDR data is disclosed. However, the data holder may decline to provide a relevant account holder with a consumer dashboard or update the consumer dashboard if the data holder considers it necessary to do either in order to prevent physical, psychological or financial harm or abuse. See C DR Rules, rule 4A.15.

[25] CDR Rules, rule 7.9.

[26] Where the CDR data disclosed relates to a joint account, and either the co-approval or pre-approval option applies to that account, the data holder must provide each relevant account holder with a consumer dashboard, except where the data holder considers it necessary to decline to provide a relevant account holder with a dashboard in order to prevent physical, psychological or financial harm or abuse. See CDR Rules, rules 4A.13 and 4A.15.

[27] The requirements are outlined in rule 1.15 in the CDR Rules, and include requirements to provide details of the CDR data to which the authorisation relates and when the authorisation will expire.

[28] CDR Rules, subclause 2.3(2) of Schedule 4.

[29] A disclosure consent is a consent given by a consumer for the accredited data recipient to disclose CDR data: for example, an 'AP disclosure consent', an 'insight disclosure consent', a 'business consumer disclosure consent', or a 'TA disclosure consent', or a direct marketing consent: CDR Rules, paragraph 1.10A(1)(c). For further information, see Chapter C (Consent).

[30] The requirements are outlined in rule 1.14 in the CDR Rules and include requirements to provide details of the CDR data to which each consent relates and when each consent will expire.

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

When must notification be given?

10.30 Data holders and accredited data recipients must notify the consumer/s as soon as practicable after the CDR data is disclosed.[32]

10.31 As a matter of best practice, notification should generally occur in as close to real time as possible (for example, in relation to ongoing disclosure, as close to the time of first disclosure as possible). In most cases, notification will occur on the same day as the CDR data is disclosed.

10.32 The test of practicability is an objective test. It is the responsibility of the data holder or accredited data recipient to be able to justify any delay in notification.

10.33 In determining what is 'as soon as practicable', data holders and accredited data recipients may take the following factors into account:

- the time and cost involved, in combination with other factors
- technical matters, and
- the individual needs of the consumer (for example, any additional steps required to make the content accessible).

10.34 Data holders and accredited data recipients are not excused from providing prompt notification by reason only that it would be inconvenient, time consuming, or costly to do so.

10.35 Notifications about disclosure should remain on a consumer's consumer dashboard, even where the relevant authorisation has expired.[33]

What matters must be included in the notification?

10.36 The minimum matters that must be included by data holders and accredited data recipients in a notification about disclosure to an accredited person, and provided via the consumer's dashboard are:

- what CDR data was disclosed
- when the CDR data was disclosed, and
- the accredited person to whom the CDR data was disclosed.[34]

[32] CDR Rules, subrules 7.9(1), 7.9(2), 7.9(3), 7.9(3A) and 7.9(4).

[33] CDR Rule 1.14(3)(h) and 1.15(3)(f) provide that the consumer dashboard must include certain information about a consent or authorisation (respectively), including where that consent or authorisation is not current. This includes information about when CDR data was collected or disclosed pursuant to the consent, or disclosed pursuant to the authorisation.

[34] CDR Rules, subrules 7.9(1) and 7.9(2). The accredited person needs to be identified in accordance with any entry on the Register of Accredited Persons specified as being for that purpose.

10.37 Where an accredited data recipient discloses CDR data to a person in accordance with a business consumer disclosure consent, the minimum matters that must be included in the notification provided via the consumer's dashboard are:

- what CDR data was disclosed
- when the CDR data was disclosed, and
- the person to whom it was disclosed.[35]

10.38 Where an accredited data recipient discloses CDR data to a trusted adviser, the minimum matters that must be included in the notification provided via the consumer's dashboard are:

- what CDR data was disclosed,
- when the CDR data was disclosed, and
- the identity of the trusted adviser.[36]

10.39 Where an accredited data recipient discloses a CDR insight, the minimum matters that must be included in the notification provided via the consumer's dashboard are:

- what CDR data was disclosed
- when the CDR data was disclosed, and
- the person to whom the CDR data was disclosed.[37]

10.40 Data holders and accredited data recipients should provide information about these matters clearly and simply, but also with enough specificity to be meaningful for the consumer. How much information is required may differ depending on the circumstances.

10.41 Guidance on each of the minimum matters follows.

[35] CDR Rules, subrule 7.9(3A).

[36] CDR Rules, subrule 7.9(3).

[37] CDR Rules, subrule 7.9(4).

Risk point: Consumers may not read or understand a notification if it is complex.

Privacy tip: Data holders and accredited data recipients should ensure that the notification is as simple and easy to understand as possible. To do this, entities should consider a range of factors when formulating a notification, such as:

- the audience
- the language used (including the level of detail), and
- the presentation of the information (e.g. layout, format and any visual aids used). For more complex notifications, entities could consider providing a condensed summary of key matters in the notification and linking to a more comprehensive summary or, where it may assist the consumer, a full log of disclosure.

What CDR data was disclosed

10.42 Data holders and accredited data recipients must notify the consumer of what CDR data was disclosed.

10.43 In doing so, the entity should ensure the CDR data is described in a manner that allows the consumer to easily understand what CDR data was disclosed.

10.44 Data holders and accredited data recipients must use the Data Language Standards when describing what CDR data was disclosed.[38] This will aid consumer comprehension by ensuring consistency between how CDR data was described in the authorisation/consent-seeking processes and how CDR data is described in the consumer dashboard.

When the CDR data was disclosed

10.45 Data holders and accredited data recipients must notify the consumer of when the CDR data was disclosed.[39]

'One-off' disclosure[40]

10.46 The entity should include the date on which the CDR data was disclosed.

[38] The Data Language Standards (https://consumerdatastandardsaustralia.github.io/standards/#data-language-standards-common) provide descriptions of the types of data to be used by data holders and accredited data recipients when making and responding to requests. Adherence to the Data Language Standards is mandatory and will help ensure there is a consistent interpretation and description of the consumer data that will be shared in the CDR system. See section 56FA of the Competition and Consumer Act and rule 8.11 in the CDR Rules.

[39] CDR Rules, paragraph 7.9(1)(b). Note this requirement refers to dates of disclosure, not the date that authorisation was provided or expired.

[40] For data holders, this is where the accredited person made a consumer data request on behalf of the consumer for a collection of CDR data on a single occasion. For accredited data recipients, this is where the consumer's disclosure consent applies for the disclosure of CDR data on a single occasion.

Ongoing disclosure[41]

10.47 The entity should, at a minimum, include the date range in which CDR data will be disclosed, with the starting date being the date on which the CDR data was first disclosed, and the end date being the date on which the entity will make its final disclosure. This end date might not necessarily be the same as the date that the authorisation (in the case of a data holder) or disclosure consent (in the case of an accredited data recipient) expires.

10.48 Where the entity is unsure of the end date they may put the date the authorisation or disclosure consent expires, but must update the end date as soon as practicable after it becomes known.[42]

10.49 If disclosure of particular CDR data stops (for example, because authorisation for that data is withdrawn), but disclosure later recommences under an amended authorisation, then the disclosure is not continuous and 2 separate date ranges should be included.

To whom the CDR data was disclosed

10.50 In a notification to the consumer of the disclosure of CDR data to an accredited person, the entity must indicate the accredited person to whom the CDR data was disclosed.

10.51 The accredited person must be identified in accordance with any entry on the Register of Accredited Persons specified as being for that purpose.[43]

Example

Bank Belle, a data holder, receives a consumer data request on 1 July 2022 from Watson and Co, an accredited person, to disclose Zoe's transaction details.

Bank Belle asks Zoe on 1 July 2022 to authorise the disclosure of her transaction details to Watson and Co for the sharing period specified in the consumer data request (i.e. 1 July 2022 to 1 January 2023).

Upon receiving Zoe's authorisation, Bank Belle discloses Zoe's transaction details to Watson and Co on 1 July 2022.

Bank Belle updates Zoe's consumer dashboard on 1 July 2022 to include the following notification statement:

We shared your transaction details with Watson and Co on 01.07.22. We'll continue to share your transaction details with Watson and Co until 01.01.23.

[41] For data holders, this is where the accredited person made a consumer data request on behalf of the consumer for collection of CDR data over a specified period of time. For accredited data recipients, this is where the consumer's disclosure consent applies for the disclosure of CDR data over a specified period of time.

[42] CDR Rules, rules 4.19 and 4.27 require data holders and accredited data recipients (respectively) to update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

[43] CDR Rules, paragraphs 7.9(1)(c) and (2)(c).

The above statement is an example of how Bank Belle, a data holder, could notify Zoe of the disclosure of her CDR data in accordance with subrule 7.9(1) in the CDR Rules.

10.52 In a notification to the consumer of a disclosure of CDR data to a trusted adviser, the accredited data recipient must indicate the trusted adviser to whom the CDR data was disclosed.[44]

10.53 In a notification to the consumer of the disclosure of a CDR insight, the accredited data recipient must indicate to whom the data was disclosed.[45]

10.54 In a notification to the consumer of a disclosure of CDR data to a specified person in accordance with a business consumer disclosure consent, the accredited data recipient must indicate to whom the CDR data was disclosed.[46]

Other notification requirements under the CDR Rules

For data holders

10.55 In addition to the Privacy Safeguard 10 notification requirements in relation to disclosure, there are other notification requirements that must be complied with by a data holder:

- general obligation to update the consumer dashboard (CDR Rules, rule 4.27)
- notification requirements where authorisations are withdrawn or otherwise expire (CDR Rules, rules 4.26A and 4.28).

For accredited data recipients

10.56 In addition to the Privacy Safeguard 10 notification requirements in relation to disclosure, there are other notification requirements relating to consent and collection that must be complied with by an accredited data recipient:[47,48]

- providing CDR receipts to the consumer (CDR Rules, rule 4.18)
- notification requirements where certain consents expire or are amended (CDR Rules, rules 4.18AA, 4.18A, 4.18B and 4.18C)
- general obligation to update the consumer dashboard (CDR Rules, rule 4.19)

---

[44] CDR Rules, subrule 7.9(3).

[45] CDR Rules, subrule 7.9(4).

[46] CDR Rules, subrule 7.9(3A).

[47] For an accredited data recipient who collected CDR data on behalf of a principal in a CDR outsourcing arrangement, note the effect of subrule 1.7(5) in the CDR Rules which provides that, in the CDR Rules, 'unless the contrary intention appears, a reference to an accredited person making a consumer data request, collecting CDR data, obtaining consents, providing a consumer dashboard, or using or disclosing CDR data does not include a reference to an accredited person doing those things on behalf of a principal in its capacity as the provider in an OSP arrangement, in accordance with the arrangement'.

For information on 'CDR outsourcing arrangements', see Chapter B (Key concepts).

[48] Under a sponsorship arrangement, where both an affiliate and their sponsor are required to give one of the notices in CDR Rules 4.18 – 4.20, the Rules provide that the sponsor and affiliate may choose which of them will give the notice: CDR Rules, rule 4.20A.

- ongoing notification requirements for consents to collect and use (CDR Rules, rule 4.20), and
- notifying the consumer of the collection of their CDR data under Privacy Safeguard 5 (CDR Rules, rule 7.4).

10.57 For further information regarding the notification requirements for consent, see Chapter C (Consent). For further information regarding the notification requirement for collection, see Chapter 5 (Privacy Safeguard 5).

Disclosure to a designated gateway

10.58 Privacy Safeguard 10 applies where a data holder or accredited data recipient discloses CDR data to a designated gateway as required or authorised under the CDR Rules.[49]

10.59 There are currently no CDR Rules made for this circumstance.

Note: *There are currently no designated gateways in the banking sector or energy sector.*[50] *See Chapter B (Key concepts) for the meaning of designated gateway.*

Interaction with other Privacy Safeguards

10.60 Data holders and accredited data recipients must comply with Privacy Safeguard 1 by taking reasonable steps to implement practices, procedures and systems that will ensure they comply with the CDR system, including Privacy Safeguard 10. See Chapter 1 (Privacy Safeguard 1).

10.61 Privacy Safeguard 11 mandates the steps which data holders and accredited data recipients must take to advise a consumer where they have disclosed CDR data that was incorrect. See Chapter 11 (Privacy Safeguard 11).

[49] CDR Rules may be made in relation to the notification requirements for that disclosure.

[50] For the banking sector, see the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. For the energy sector, the energy designation specifies AEMO as a gateway for certain information: subsection 6(4) of the Consumer Data Right (Energy Sector) Designation 2020. However, at the time of publication, AEMO is not a designated gateway for any CDR data because under current CDR Rules, no CDR data is (or is to be) disclosed to AEMO because of the reasons in subsection 56AL(2)(c) of the Competition and Consumer Act.

There are also no designated gateways in the telecommunications sector, although unlike the banking and energy sectors at the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications data under the CDR system: Consumer Data Right (Telecommunications Sector) Designation 2022.