Chapter B:

Key concepts

Version 4.0, November 2022

OAIC

Contents

About this Chapter

B.1 This Chapter outlines some key words and phrases that are used in the privacy safeguards and consumer data rules (CDR Rules).

B.2 The example below outlines a key information flow in the CDR system and demonstrates the operation of several key concepts in the CDR system. While it outlines a key information flow, it does not account for all CDR arrangements and sector specific nuances.

B.3 Further information regarding the underlined terms can be found within this Chapter under the corresponding heading.

Key concepts in the CDR system explained

Accredited persons

Meadow Cost Comparison wants to receive CDR data to provide product comparison services to consumers under the CDR system, so it applies to the ACCC (the Data Recipient Accreditor)[1] to become accredited at the unrestricted level. (It is also possible to be accredited at the 'sponsored' level). The ACCC is satisfied that Meadow Cost Comparison meets the accreditation criteria under the CDR Rules and grants unrestricted accreditation. Meadow Cost Comparison is therefore an **accredited person** and is allowed to receive CDR data under the CDR system.

CDR data

Carly is a customer of Sunny Bank but is interested in what alternative credit card rates other banks could provide. Carly has an existing credit card, and provides Meadow Cost Comparison with a valid request (with her consent) to collect her account numbers, balances and features from Sunny Bank and use that information for the purposes of comparing credit card rates. Account numbers, balances, and features fall into a class of information set out in the designation instrument for the banking sector,[2] and are therefore **CDR data**.

[1] See paragraph B.7.

[2] Competition and Consumer Act, subsection 56AI(1). The Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 sets out the classes of information in the banking sector that are subject to the CDR system, the persons who hold this information and will be required or authorised to transfer the information under the regime, and the earliest date that the information must have begun to be held to be subject to the CDR system.

Data holders

Sunny Bank is a **data holder**. This is because:

- Carly's CDR data is within a class of information specified in the designation instrument for the banking sector
- Carly's CDR data is held by Sunny Bank on or after the earliest holding day[3]
- Sunny Bank is not a designated gateway for the data, and
- Sunny Bank is an authorised deposit-taking institution (one of the categories specified in paragraph 56AJ(1)(d) of the Competition and Consumer Act).[4]

CDR consumers

Carly is a **CDR consumer for CDR data** because:

- the CDR data relates to Carly because it is about her credit card
- the CDR data is held by a data holder (Sunny Bank), being one of the entity types listed in paragraph 56AI(3)(b),[5] and
- Carly is identifiable or reasonably identifiable from the CDR data.[6]

[3] For the banking sector, 1 January 2017 is the 'earliest holding day' specified in the designation instrument: Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, subsection 5(3). See paragraph B.159 for further information.

[4] Sunny Bank is an authorised-deposit taking institution, which has been specified as a relevant class of persons in the designation instrument for the banking sector (the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019).

[5] See paragraph B.154 for further information.

[6] Competition and Consumer Act, subsection 56AI(3).

Accredited data recipients

Meadow Cost Comparison, as an unrestricted accredited person makes a consumer data request on Carly's behalf by asking Sunny Bank to disclose Carly's CDR data.[7] Sunny Bank asks Carly to authorise the disclosure of her CDR data to Meadow Cost Comparison.

Upon receiving authorisation from Carly to do so, Sunny Bank discloses Carly's CDR data to Meadow Cost Comparison.

Following receipt of Carly's data from Sunny Bank, Meadow Cost Comparison is now an **accredited data recipient** of CDR data. This is because Meadow Cost Comparison:

- is an accredited person
- has been disclosed CDR data from a data holder (Sunny Bank) under the CDR Rules
- holds that CDR data, and
- does not hold that CDR data as a data holder or designated gateway.[8]

Consumer dashboards

Given that Meadow Cost Comparison has made a consumer data request on Carly's behalf, Meadow Cost Comparison provides Carly with a **consumer dashboard**.[9] A consumer dashboard is an online service that allows Carly to manage and view details about her consent.

Upon receiving the consumer data request from Meadow Cost Comparison, Sunny Bank also provides Carly with a consumer dashboard that will allow Carly to manage and view details about her authorisation.[10]

Accredited data recipient

B.4 A person is an 'accredited data recipient' of a consumer's CDR data if the person:

- is an accredited person (see paragraphs B.7 to B.11 below)
- was disclosed CDR data from a CDR participant under the CDR Rules[11]

[7] Only entities with unrestricted accreditation can collect CDR data directly from a data holder. In this example, we have specified that Meadow Cost Comparison holds unrestricted accreditation which allows it to make a consumer data request directly to Sunny Bank for collection of Carly's CDR data.

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

[9] CDR Rules. rule 1.14.

[10] CDR Rules, rule 1.15.

[11] If an accredited person is disclosed CDR data otherwise than in accordance with the CDR Rules (for instance, outside the CDR system), they will not become an 'accredited data recipient' for that CDR data.

- holds that CDR data (or has another person hold that CDR data on their behalf), and
- does not hold that CDR data as a data holder or designated gateway.[12]

B.5 Accredited persons should be aware that where they are seeking consent from a consumer to collect, use or disclose CDR data, and the CDR data is yet to be collected, they are not yet an accredited data recipient of the CDR data.

B.6 For an illustration of how and when an accredited person becomes an accredited data recipient of CDR data, see the example under paragraph B.3.

Accredited person

B.7 An 'accredited person' is a person who has been granted accreditation by the Data Recipient Accreditor.[13] The Data Recipient Accreditor is the Australian Competition and Consumer Commission (ACCC).[14]

B.8 An example of an accredited person could be a bank, a fintech, a retailer such as an electricity retailer or financial comparison service or another business that wishes to provide a good or service using CDR data. This is demonstrated by the example under paragraph B.3.

B.9 To be granted an accreditation, the person must satisfy the relevant accreditation criteria in Part 5 of the CDR Rules.

B.10 A data holder may be accredited under the CDR system, and therefore be both a data holder and an accredited person.

B.11 There are 2 levels of accreditation:

- unrestricted accreditation, and
- sponsored accreditation.[15]

Unrestricted accreditation

B.12 Entities with unrestricted accreditation can undertake the full range of functions permitted for accredited persons under the CDR Rules.

B.13 A person with unrestricted accreditation is able to sponsor other accredited persons in the CDR system under sponsorship arrangements, and/or enter into CDR representative arrangements with unaccredited entities.[16] See paragraphs B.49 to B.53 and B.240 to B.249 for more information.

In this situation, the *Privacy Act 1988* and the APPs would apply (to the extent the CDR data is personal information, and where the accredited person is an APP entity). Note: Small business operators accredited under the CDR system are APP entities in relation to information that is personal information but is not CDR data. See s 6E(1D) of the Privacy Act.

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

[13] Competition and Consumer Act, subsection 56CA(1).

[14] The ACCC has been appointed as the Data Recipient Accreditor by the Minister under section 56CG of the Competition and Consumer Act.

[15] CDR Rules, rule 5.1A.

[16] CDR Rules, rules 1.10D and 1.10AA.

Sponsored accreditation

B.14 A person with 'sponsored accreditation' has or intends to have a sponsorship arrangement with an unrestricted accredited person who is willing to act as their sponsor in the CDR system. There are certain restrictions on participation in the CDR system for those entities with sponsored accreditation (see 'Affiliate' below).

B.15 A person accredited to the sponsored level and in a sponsorship arrangement will be known as an 'affiliate' of its sponsor.

Affiliate

B.16 An 'affiliate' is a person with sponsored accreditation who has entered into a written contract (a 'sponsorship arrangement'), with another person with unrestricted accreditation (the 'sponsor') that meets certain requirements as set out in paragraphs B.247 to B.249.[17]

B.17 The sponsored accreditation model allows a person who is accredited to the 'sponsored' level (rather than the unrestricted level) to provide goods or services directly to a consumer.

B.18 An affiliate may collect CDR data from an accredited data recipient (via a consumer data request made under rule 4.7A) or request that their sponsor collect CDR data from a CDR participant on their behalf. They cannot collect data directly from a data holder.[18]

B.19 An affiliate cannot engage an outsourced service provider to collect CDR data from a CDR participant on their behalf[19] and they cannot have a CDR representative.[20]

B.20 As a sponsor and their affiliate are both accredited persons, each entity will be liable in their own right for their handling of CDR data. In addition, where a sponsor collects a consumer's CDR data at the affiliate's request, that data is taken also to have been collected by the affiliate.[21] This ensures that limitations on uses and disclosures apply to affiliates.

B.21 The CDR Rules contain some specific obligations for affiliates, particularly in relation to consent, notification, dashboards and CDR policy content. For more information, see Chapter C (paragraphs C.15, C.30 – C.31, C.64, C.72, C.76, C.103, diagram after C.118), Chapter 1 (paragraph 1.54), Chapter 3 (paragraphs 3.26 – 3.27, 3.36 – 3.38, diagram after 3.42), Chapter 5 (paragraph 5.3, 5.10, 5.25, 5.38 – 5.40), Chapter 6 (paragraphs 6.24, 6.73), Chapter 10 (paragraph 10.53), Chapter 11 (paragraph 11.31) and the OAIC's separate guidance for affiliates.[22]

B.22 An affiliate may have more than one sponsor at any time.

---

[17] CDR Rules, rule 1.10D. The Note under this Rule states that 'A person does not need to have sponsored accreditation to enter into a sponsorship arrangement as an affiliate, but will need it to make consumer data requests to the sponsor for information held by the sponsor as an accredited data recipient.'

[18] CDR Rules, subrule 5.1B(3).

[19] CDR Rules, subrule 5.1B(4).

[20] CDR Rules, subrule 5.1B(5).

[21] CDR Rules, subrule 7.6(3).

[22] For more information on the privacy obligations of affiliates, see: https://www.oaic.gov.au/consumer-data-right/guidance-and-advice/sponsored-accreditation-model-privacy-obligations-of-affiliates.

Assurance report

B.23 An assurance report for a person with unrestricted accreditation means a report made in accordance with ASAE 3150 or an approved standard, report or framework.

B.24 An assurance report for a person with sponsored accreditation is an assessment of its capacity to comply with Schedule 2 (Steps for privacy safeguard 12 – security of CDR data held by accredited data recipients) of the CDR Rules that is made in accordance with any approved requirements.[23]

B.25 This report does not include information that must be provided in an attestation statement.

B.26 Assurance reports are discussed in Chapter 12 (Security of CDR data and destruction or de-identification of redundant data).

Attestation statement

B.27 An attestation statement for a person with unrestricted accreditation means the responsible party's statement on controls and system description, made in accordance with ASAE 3150.

B.28 An attestation statement for a person with sponsored accreditation is a statement about its compliance with Schedule 2 of the CDR Rules that is made in accordance with any approved requirements. [24]

B.29 Attestation statements are discussed in Chapter 12 of the privacy safeguard guidelines which relate to the security of CDR data.

Australian Privacy Principles, APPs

B.30 The Australian Privacy Principles (APPs) are set out in Schedule 1 of the *Privacy Act 1988* (Cth). There are 13 APPs and they set out standards, rights and obligations in relation to a regulated entity's handling, holding, accessing and correcting of personal information.

B.31 For information about which APPs apply to CDR entities in the CDR context, see Chapter A.

Authorise, Authorisation

B.32 An authorisation is sought from or provided by a CDR consumer. It must meet the requirements set out in the CDR Rules, and be sought in accordance with the data standards.[25]

B.33 Data holders must ask the consumer to authorise the disclosure of their CDR data to an accredited person before disclosing CDR data to the relevant accredited person.[26]

---

[23] See CDR Rules, subclause 2.1(1) of Schedule 1. For example, the Rules list the CDR Accreditation Guidelines.

[24] See CDR Rules, subclause 2.1(1) of Schedule 1.

[25] CDR Rules, rule 4.5. See Division 4.4 of the CDR Rules for the requirements for asking a consumer to give or amend an authorisation.

[26] For SR (shared responsibility) data covered by a SR data request, the obligation to ask for authorisation applies to the primary data holder as if it were the data holder for the SR data: CDR Rules, subrule 1.23(3).

B.34 For requests that relate to joint accounts, in some cases, the data holder might need to seek an authorisation (known as an 'approval') from the other joint account holder/s.[27] Joint accounts are discussed further at paragraph B.184.

B.35 For further information, see the Guide to privacy for data holders. See also the example under paragraph B.3 to understand at which point a data holder must seek authorisation from the consumer to disclose CDR data.

CDR data

B.36 'CDR data' is information that is:

- within a class of information specified in the designation instrument for each sector;[28] or
- derived from the above information ('derived CDR data').[29]

Derived CDR data

B.37 'Derived CDR data' is data that has been wholly or partly derived from CDR data, or data derived from previously derived data ('indirectly derived' data).[30] This means data derived from 'derived CDR data' is also 'derived CDR data'.

B.38 'Derived' takes its ordinary meaning. This is because 'derived' is not defined in the Competition and Consumer Act or the Privacy Act.

SR or shared responsibility data

B.39 CDR data for which there is a CDR consumer may be specified as SR (shared responsibility) data where it is held by one data holder (the secondary data holder), but it would be more practical for consumer data requests for the data to be directed to a different data holder (the primary data holder).[31]

B.40 Under current arrangements, only the energy sector has SR data (and by extension, primary and secondary data holders). For further information on data holders, see paragraphs B.154 to B.155. The meaning of SR data for the energy sector is set out in the Schedule 4 to the CDR Rules. In the energy sector, the Australian Energy Market Operator Limited (AEMO) is the secondary data holder,[32] and SR data means AEMO data in relation to a CDR consumer.[33] AEMO data is NMI (national metering identifier) standing data, metering data and DER (distributed energy resource) register data that relates to a relevant arrangement with the

---

[27] Depending on which 'disclosure option' (i.e. pre-approval or co-approval option) applies to the joint account: CDR Rules, rule 4A.5. Joint account holders can manage 'disclosure options through the disclosure option management service: CDR Rules, rule 4A.6. See Subdivision 4A.3.2 of the CDR Rules, which sets out how consumer data requests to data holders that relate to joint accounts are handled in the CDR system.

[28] Competition and Consumer Act, subsection 56AI(1). For further information on designation instruments, see paragraphs B.171 to B.173.

[29] Competition and Consumer Act, subsection 56AI(1). For information on 'materially enhanced information' as derived CDR data, see paragraph B.264.

[30] Competition and Consumer Act, subsection 56AI(2).

[31] Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 5.

[32] See CDR Rules, clause 4.3 of Schedule 4.

[33] See CDR Rules, clause 4.3 of Schedule 4. See definition of AEMO data at CDR Rules, clause 1.2 of Schedule 4.

retailer.[34] The primary data holder for this data is the energy retailer, who has a direct relationship with the consumer.[35] The outcome of this is that consumer data requests involving AEMO data are to be directed to the retailer, rather than to AEMO.[36]

B.41 For further guidance on primary and secondary data holders, see paragraphs B.156 to B.158.

CDR insight

B.42 A 'CDR insight' is an insight based on a consumer's CDR data, which is subject to an insight disclosure consent.[37]

B.43 CDR insights are CDR data.[38] The CDR insights model is intended to allow accredited data recipients[39] to disclose CDR data outside the CDR system to either confirm, deny, or provide simple information to a person selected by the CDR consumer, where this is for a limited, permitted purpose. 'Insight disclosure consent' is defined at B.85.

CDR participant

B.44 A 'CDR participant' is a data holder, or an accredited data recipient, of CDR data.[40]

CDR policy

B.45 A 'CDR policy' is a document that provides information to consumers about how a CDR entity manages CDR data and how CDR consumers can make an inquiry or a complaint. The policy must be developed and maintained by entities in accordance with Privacy Safeguard 1 and CDR Rule 7.2.

B.46 The CDR policy must be a separate document to any of the entity's privacy policies. For further information on the suggested process for developing a CDR policy and the minimum requirements for what must be included, see Chapter 1 (Privacy Safeguard 1) and the Guide to developing a CDR policy.

[34] See CDR Rules, clause 1.2 of Schedule 4. The CDR Rules define NMI standing data, metering data and DER register data with reference to the definitions in the National Electricity Rules: see CDR Rules, clauses 1.2 and 1.3 of Schedule 4.

[35] See CDR Rules, clause 4.3 of Schedule 4 and Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 20.

[36] CDR Rules, subrules 1.22(2) and 1.23(2).

[37] CDR Rules, rule 1.7.

[38] See CDR Rules, rules 1.7 and 1.10A(3).

[39] CDR representatives can also disclose CDR insights with the consumer's consent.

[40] Competition and Consumer Act, subsection 56AL(1).

CDR receipt

B.47 A 'CDR receipt' is a notice given by an accredited person[41] to a CDR consumer who has provided, amended or withdrawn a consent.[42]

B.48 CDR receipts must be given in accordance with CDR Rule 4.18.

CDR principal

B.49 A CDR principal is a person with unrestricted accreditation who has entered a written contract (a 'CDR representative arrangement'), with an unaccredited person (a 'CDR representative'). The written contract must meet the requirements in the CDR Rules (as discussed under 'CDR representative arrangement' below).[43]

B.50 Under a CDR representative arrangement, a CDR principal collects CDR data on behalf of their CDR representative (in accordance with a consumer's collection consent), and discloses that data to the CDR representative so they may provide goods or services to consumers using that data.

B.51 While the CDR representative has the consumer-facing relationship, the CDR principal retains obligations in relation to the consumer for a range of matters, including providing the dashboard and notifications. Some of these obligations may be delegated to the CDR representative.

B.52 The CDR principal is liable for the actions of their CDR representative, including breaches of the privacy safeguards.[44] In addition, a CDR principal must ensure that the CDR representative complies with the requirements of the written contract,[45] and the CDR principal is liable if the CDR representative breaches any of the CDR representative arrangement provisions which are required by CDR Rule 1.10AA(2).[46]

B.53 The CDR Rules contain some specific obligations for CDR principals, particularly in relation to the written contract, consent, notification, dashboards and the CDR principal's CDR policy. For more information, see Chapter C (paragraphs C.9 – C.11, C.15, C.27 – C.29, C.59, C.73, C.84, C.86, C.92, C.97, C.99, C.109, diagram after C.118), Chapter 1 (paragraphs 1.8, 1.11, 1.20, 1.44, 1.54, 1.60), Chapter 2 (paragraph 2.6), Chapter 3 (paragraphs 3.16 – 3.17, 3.23 – 3.24, diagram after 3.42), Chapter 4 (paragraph 4.9), Chapter 5 (paragraphs 5.10, 5.15), Chapter 6 (paragraphs 6.8, 6.24, 6.78 – 6.79), Chapter 7 (paragraphs 7.9, 7.20, 7.41 – 7.42), Chapter 8 (paragraph 8.8), Chapter 9 (paragraph 9.7), Chapter 10 (paragraph 10.8), Chapter 11

[41] Where the accredited person who is required to give a CDR receipt is a CDR principal, the receipt may be given through the CDR representative – CDR Rules, paragraph 4.3C(1)(l).

[42] CDR Rules, subrule 4.18(1).

[43] CDR Rules, subrule 1.10AA(2). These requirements are discussed in paragraphs B.58, B.60 - B.65.

[44] See CDR Rules, rules 4.3C(2) (Giving and amending consents), 7.3(2) (Rules relating to PS2 – anonymity and pseudonymity), 7.3A (Rule relating to PS4 – destruction of unsolicited data), 7.6(4) (Use or disclosure of CDR data), 7.8A (Rules relating to PSs 8 and 9), 7.9(5) (Rule relating to PS10 – notifying of the disclosure of CDR data), 7.10A (Rule relating to PS 11 – quality of data), 7.11(2) (Rule relating to PS 12 – security of CDR data), 7.12(3) (Rule relating to PS 12 – de-identification of redundant data) and 7.16 (Rule relating to PS 13 – correction of data).

[45] CDR Rules, subrule 1.16A(1).

[46] CDR Rules, subrule 1.16A(2) and (3).

(paragraphs 11.11, 11.31), Chapter 12 (paragraphs 12.10, 12.40, 12.42, 12.56 – 12.57, 12.121 – 12.123), Chapter 13 (paragraph 13.12), and the OAIC's separate guidance for CDR principals.[47]

CDR representative

B.54 A CDR representative is an unaccredited person who has entered a written contract (a 'CDR representative arrangement') with a CDR principal that meets the requirements in the CDR Rules (as discussed under 'CDR representative arrangement' below).[48] The CDR principal must be accredited at the unrestricted level.

B.55 A CDR representative collects CDR data from their CDR principal, and uses that CDR data to provide goods or services directly to the consumer.

B.56 A CDR representative may collect CDR data only from their CDR principal. They are not permitted under the CDR Rules to collect CDR data from data holders or other accredited data recipients.

B.57 As an unaccredited entity, a CDR representative is not bound by the privacy safeguards, but must comply with the terms of the CDR representative arrangement with the CDR principal.[49] As outlined in paragraph B.52 above, the CDR principal is liable for the actions of their CDR representative. A CDR representative's contractual obligations apply in addition to other privacy obligations they have under the Privacy Act if they are an APP entity. While they are not directly bound by the privacy safeguards, the following paragraphs are of particular relevance to CDR representatives: Chapter C (paragraphs C.9 – C.11, C.15, C.27 – C.29, C.51, C.59, C.64, C.73, C.84, C.86, C.92, C.97, C.99, C.109, diagram after C.118), Chapter 1 (paragraphs 1.8, 1.11, 1.60), Chapter 2 (paragraph 2.6), Chapter 3 (paragraphs 3.16 – 3.17, 3.23 – 3.24, 3.28, diagram after 3.42), Chapter 4 (paragraph 4.9), Chapter 5 (paragraphs 5.10, 5.15), Chapter 6 (paragraphs 6.8, 6.24, 6.78 – 6.79), Chapter 7 (paragraph 7.9), Chapter 8 (paragraph 8.8), Chapter 9 (paragraph 9.7), Chapter 10 (paragraph 10.8), Chapter 11 (paragraph 11.11), Chapter 12 (paragraph 12.10), Chapter 13 (paragraphs 13.12).

B.58 A CDR representative may have one CDR principal only, and must not engage a person as the provider in a CDR outsourcing arrangement.

CDR representative arrangement

B.59 A CDR representative arrangement is a written contract between a CDR representative (an unaccredited person) and their CDR principal that meets the minimum requirements listed in CDR Rule 1.10AA(2).

B.60 Under the arrangement:

- the CDR principal will make consumer data requests on behalf of the CDR representative (where the consumer has given the representative a collection and use consent), and disclose the relevant CDR data to the CDR representative

[47] See https://www.oaic.gov.au/consumer-data-right/guidance-and-advice/CDR-representative-model-Privacy-obligations-of-CDR-principals.

[48] CDR Rules, subrule 1.10AA(2). These requirements are discussed in paragraphs B.58, B.60 - B.65.

[49] For more information on the privacy obligations of CDR representatives, see: https://www.oaic.gov.au/consumer-data-right/guidance-and-advice/cdr-representative-model-privacy-obligations-of-cdr-representatives.

- the CDR representative will use the CDR data to provide the relevant goods or services to the CDR consumer
- the CDR representative may disclose the CDR data in accordance with a disclosure consent given by the consumer.[50]

B.61 A CDR representative must not seek consent from a consumer, or collect, use, disclose or otherwise handle CDR data unless they have a 'CDR representative arrangement' in place with their CDR principal, and their details have been entered onto the Register of Accredited Persons.

B.62 The purpose of a CDR representative arrangement is to regulate the CDR representative's handling of 'service data', being CDR data that was collected by the CDR principal on the CDR representative's behalf (and subsequently disclosed by the CDR principal to the CDR representative), and any information directly or indirectly derived from such CDR data.

B.63 Under a CDR representative arrangement, a CDR representative is required to comply with the following privacy safeguards in relation to service data as if they were the CDR principal:

- Privacy Safeguard 2 (giving the CDR consumer the option of using a pseudonym, or not identifying themselves)
- Privacy Safeguard 4 (destroying unsolicited CDR data)
- Privacy Safeguard 11 (ensuring the quality of CDR data)
- Privacy Safeguard 12 (security of CDR data and destruction or de-identification of redundant CDR data), and
- Privacy Safeguard 13 (correction of CDR data).[51]

B.64 Under a CDR representative arrangement, a CDR representative is required to comply with the following privacy safeguards as if they were an accredited data recipient:

- Privacy Safeguard 8 (overseas disclosure of CDR data)
- Privacy Safeguard 9 (adoption or disclosure of government-related identifiers).[52]

B.65 In addition, CDR representatives have further obligations under a CDR representative arrangement, including requirements to:

- adopt and comply with the principal's CDR policy in relation to service data[53]
- take the steps in Schedule 2 to the CDR Rules to protect the service data as if it were the CDR principal[54]
- not use or disclose the service data other than in accordance with the CDR representative arrangement with the principal[55]

---

[50] See Chapter C (Consent — The basis for collecting and using CDR data) for more information about obtaining consent from a CDR consumer under a CDR representative arrangement.

[51] CDR Rules, paragraph 1.10AA(2)(d)(i).

[52] CDR Rules, subrule 1.10AA(2)(f).

[53] CDR Rules, paragraph 1.10AA(2)(e). See Chapter 1 (Privacy Safeguard 1 – Open and transparent management of CDR data) of these guidelines for more information on CDR policies.

[54] CDR Rules, paragraph 1.10AA(2)(d)(ii).

[55] CDR Rules, paragraph 1.10AA(2)(d)(iii).

- when directed by the principal, delete any service data that it holds in accordance with the CDR data deletion process, and provide to the principal records of any deletion that are required to be made under the CDR data deletion process.[56]

CDR system

B.66 The 'CDR system' was enacted by the *Treasury Laws Amendment (Consumer Data Right) Act 2019* to insert a new Part IVD into the Competition and Consumer Act.

B.67 The CDR system includes the CDR Rules, privacy safeguards, data standards, designation instruments, and any regulations made in respect of the provisions in the Competition and Consumer Act.

Collect

B.68 'Collect' is not defined in the Competition and Consumer Act or the Privacy Act.

B.69 Under the CDR system 'collect' has its ordinary, broad meaning (as it does under the Privacy Act). The concept of 'collection' applies broadly, and includes gathering, acquiring or obtaining CDR data by any means including from individuals and other entities.

B.70 Subsection 4(1) of the Competition and Consumer Act, provides that a person 'collects' information only if the person collects the information for inclusion in:

- a record (within the meaning of the Privacy Act), or
- a generally available publication (within the meaning of the Privacy Act).[57]

Consent

B.71 Consent is the:

- only basis on which an accredited person may collect CDR data,[58] and
- primary basis on which an accredited data recipient of particular CDR data, or a CDR representative, may use and disclose CDR data.[59]

B.72 Consent means a collection consent, a use consent or a disclosure consent (including a consent that has been amended by a consumer under the CDR Rules).[60] The CDR system sets out specific categories of consents that may be sought from a CDR consumer. These are set out in CDR Rule 1.10A and outlined below in paragraphs B.75 to B.89.

---

[56] CDR Rules, paragraph 1.10AA(2)(d)(iv).

[57] 'Record' is defined in subsection 6(1) of the Privacy Act to include a document or an electronic or other device, with certain exclusions. 'Generally available publication' is defined in subsection 6(1) of the Privacy Act to include certain publications that are, or will be, generally available to members of the public whether or not published in print, electronically or any other form and whether or not available on the payment of a fee.

[58] See Chapter 3 (Privacy Safeguard 3) for information on seeking to collect of CDR data.

[59] See Chapter 6 (Privacy Safeguard 6), Chapter 7 (Privacy Safeguard 7), Chapter 8 (Privacy Safeguard 8) and Chapter 9 (Privacy Safeguard 9) for information regarding use or disclosure of CDR data.

[60] CDR Rules, rule 1.7.

B.73 Consent must meet the requirements set out in the CDR Rules.[61]

B.74 For further information, including the requirements which must be complied with when asking a CDR consumer to give or amend a consent, see Chapter C (Consent).

Collection consent

B.75 A collection consent is a consent given by a CDR consumer for an accredited person to collect particular CDR data from a data holder or accredited data recipient of that CDR data.[62]

Use consent

B.76 A use consent is a consent given by a CDR consumer for an accredited data recipient of particular CDR data to use that CDR data in a particular way, for example to provide goods or services requested by the consumer.[63]

B.77 Where CDR data is collected under a CDR representative arrangement,[64] a use consent is consent given by a CDR consumer for the CDR principal who collected their CDR data to disclose that data to the CDR representative, and for the CDR representative to use it to provide goods or services requested by the CDR consumer.[65]

B.78 Types of use consents include a direct marketing consent for an accredited data recipient to use CDR data for the purposes of direct marketing, and a de-identification consent (as outlined in paragraph B.80 to B.82 and B.88 to B.89 below).[66]

AP disclosure consent

B.79 An AP disclosure consent is a consent given by a consumer for an accredited data recipient of particular CDR data, or a CDR representative, to disclose that CDR data to an accredited person in response to a consumer data request.[67]

---

[61] The requirements that an accredited person must comply with when asking for consent are contained in Division 4.3 of the CDR Rules. The specific requirements differ depending on which type of consent is being sought.

[62] CDR Rules, paragraphs 1.10A(1)(a) and 1.10A(2)(a). 'Collection consent' also includes consent given by a consumer to a CDR representative for a CDR principal to collect CDR data from a data holder or accredited data recipient and disclose it to the CDR representative – CDR Rules, subrule 1.10A(4).

[63] CDR Rules, paragraphs 1.10A(1)(b) and 1.10A(2)(b).

[64] See CDR Rules, rule 1.10AA.

[65] CDR Rules, paragraph 4.3A(2)(b).

[66] CDR Rules, rule 1.7 defines a consent as 'a collection consent, a use consent or a disclosure consent; or such a consent as amended in accordance with these rules'.

[67] CDR Rules, paragraphs 1.10A(1)(c)(i) and 1.10A(2)(e). Disclosures under an AP disclosure consent have been permitted since 1 July 2021. See CDR Rules, paragraph 1.10AA(2)(a) in relation to CDR representatives.

Direct marketing consent

B.80 A direct marketing consent is a consent given by a CDR consumer for an accredited data recipient of particular CDR data, or a CDR representative, to use or disclose CDR data for the purposes of direct marketing.[68]

B.81 A direct marketing consent for an accredited data recipient or CDR representative to use CDR data for the purposes of direct marketing is a form of 'use consent'.

B.82 A direct marketing consent for an accredited data recipient or CDR representative to disclose CDR data to an accredited person for the purposes of direct marketing is a form of 'disclosure consent'.[69]

TA disclosure consent

B.83 A TA disclosure consent is a consent given by a CDR consumer for an accredited data recipient of particular CDR data, or CDR representative, to disclose that CDR data to a trusted adviser[70] of the consumer.[71]

B.84 A TA disclosure consent is a form of 'disclosure consent'.

Insight disclosure consent

B.85 An insight disclosure consent is a consent given by a CDR consumer for an accredited data recipient or CDR representative to disclose their CDR data to a specified person for one or more of the following purposes:

- verifying the consumer's identity
- verifying the consumer's account balance, or
- verifying the details of credits to, or debits from, the consumer's accounts.[72]

B.86 Where the CDR data relates to more than one transaction, an insight disclosure consent does not authorise the accredited data recipient or CDR representative to disclose the amount or date in relation to any individual transaction.[73]

B.87 An insight disclosure consent is a form of 'disclosure consent'.

---

[68] CDR Rules, paragraphs 1.10A(1)(d) and 1.10A(2)(c). See CDR Rules, paragraph 1.10AA(2)(a) in relation to CDR representatives.

[69] CDR Rules, paragraph 1.10A(1)(c)(ii). A 'disclosure consent' includes an AP disclosure consent, as well as a consent for an accredited data recipient to disclose CDR data to an accredited person for the purposes of direct marketing.

[70] See B.253 for more information on trusted advisers.

[71] CDR Rules, paragraphs 1.10A(1)(c)(iii) and 1.10A(2)(f). CDR Rules, subrule 7.5A(2) prohibits disclosure of CDR data to a trusted adviser under a TA disclosure consent until the earlier of 1 February 2022, or the day that a relevant consumer experience data standard is made under paragraph 8.11(1)(c)(iv). See CDR Rules, paragraph 1.10AA(2)(a) in relation to CDR representatives.

[72] CDR Rules, paragraphs 1.10A(1)(c)(iv), 1.10A(2)(g) and 1.10A(3)(a)(i)-(iii). Disclosure of a CDR insight under an insight disclosure consent has been permitted since 1 February 2022. See CDR Rules, paragraphs 1.10AA(2)(a) in relation to CDR representatives.

[73] CDR Rules, paragraph 1.10A(3)(b).

De-identification consent

B.88 A de-identification consent is a consent given by a CDR consumer for an accredited data recipient of particular CDR data, or a CDR representative, to de-identify some or all of that CDR data in accordance with the CDR data de-identification process[74] and:

- use the de-identified data for 'general research' (see paragraph B.181), and/or
- disclose (including by selling) the de-identified data.[75]

B.89 A de-identification consent is a form of 'use consent'.

Consumer, CDR consumer or 'eligible' CDR consumer

B.90 The 'CDR consumer' is the person who has the right to:

- access the CDR data held by a data holder, and
- direct that the CDR data be disclosed to an accredited person.[76]

B.91 A person is a 'CDR consumer' for CDR data if each of the following four conditions are met:[77]

- the CDR data 'relates to'[78] the person because of the supply of a good or service to the person or an associate[79] of the person[80]
- the CDR data is held by another person who is:
  - a data holder of the CDR data
  - an accredited data recipient of the CDR data, or
  - holding[81] the data on behalf of a data holder or accredited data recipient of the CDR data[82]
- the person is identifiable, or reasonably identifiable,[83] from the CDR data or other information held by the other person (the data holder, accredited data recipient, or person holding data on their behalf),[84] and

[74] See CDR Rules, rule 1.17 and Chapter 12 (Privacy Safeguard 12) for further information on the CDR data de-identification process. See CDR Rules, paragraph 1.10AA(2)(a) in relation to CDR representatives.

[75] CDR Rules, paragraphs 1.10A(1)(e) and 1.10A(2)(d).

[76] Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraph 1.100.

[77] Competition and Consumer Act, subsection 56AI(3).

[78] See paragraphs B.99 to B.105 for the meaning of 'relates to'.

[79] See paragraphs B.106 to B.111 for the meaning of 'associate'.

[80] Competition and Consumer Act, paragraph 56AI(3)(a). Note that paragraph 56AI(3)(a)(ii) allows for regulations to be made to prescribe circumstances in which CDR data may relate to a person.

[81] See paragraphs B.182 to B.183 for the meaning of 'holds'.

[82] Competition and Consumer Act, subsection 56AI(3)(b).

[83] See paragraphs B.95 to B.98 for the meaning of 'reasonably identifiable'.

[84] Competition and Consumer Act, paragraph 56AI(3)(c).

- none of the conditions (if any) prescribed by the regulations apply to the person in relation to the CDR data.[85]

B.92 A CDR consumer can be an individual or a business enterprise.[86]

B.93 Section 4B of the Competition and Consumer Act does not apply for the purposes of determining whether a person is a 'CDR consumer'.[87] This section explains when a person is taken to have acquired particular goods or services as a consumer, outside of the CDR system.

B.94 These guidelines use the term 'consumer' and 'CDR consumer' interchangeably.

Reasonably identifiable

B.95 As outlined in paragraph B.91, for a person to be a 'CDR consumer' that person must be identifiable, or 'reasonably identifiable', from the CDR data or other information held by the relevant entity (i.e. the data holder, accredited data recipient, or person holding data on their behalf).[88]

B.96 For the purpose of determining whether a person is a 'CDR consumer' for CDR data, 'reasonably identifiable' is an objective test that has practical regard to the relevant context. This can include consideration of:

- the nature and amount of information
- other information held by the entity (see paragraphs B.182 to B.183 for a discussion on the meaning of 'held'), and
- whether it is practicable to use that information to identify the person.

B.97 Where it is unclear whether a person is 'reasonably identifiable', an entity should err on the side of caution and act as though the person is 'reasonably identifiable' from the CDR data or other information held by the entity. In practice, this generally means treating the person as a 'CDR consumer' – the entity would need to handle CDR data which relates to the consumer in accordance with the privacy safeguards.

B.98 See B.204 to B.207 for a discussion on the meaning of 'reasonably'.

Relates to

B.99 As outlined in paragraph B.91, for a person to be a 'CDR consumer' the CDR data must 'relate to' that person.[89]

B.100 In this context, the concept of 'relates to' is broad. It applies where there is some 'association' between the CDR data and the person which is 'relevant' or 'appropriate'

[85] At the time of publication, there are no conditions prescribed by the regulations.

[86] Competition and Consumer Act, subsection 56AI(3); Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraphs 1.100 and 1.101. See also section 2C of the *Acts Interpretation Act 1901* (Cth), which provides that in any Act (including the references to 'person' in subsection 56AI(3) of the Competition and Consumer Act), expressions used to denote persons generally include a body politic or corporate as well as an individual.

[87] Competition and Consumer Act, subsection 56AI(4).

[88] Competition and Consumer Act, paragraph 56AI(3)(c).

[89] Competition and Consumer Act, paragraph 56AI(3)(a).

depending on the statutory context.[90] The relevant context in the CDR system is the Competition and Consumer Act and the Privacy Act.

B.101 The Competition and Consumer Act states that the CDR data must 'relate to' the person because of the supply of a good or service to them or an associate of theirs, or because of circumstances of a kind prescribed by the CDR Rules.[91]

B.102 CDR data will not 'relate to' a person unless the data itself is somehow relevant or appropriate for that person to use as a consumer under the CDR system.

B.103 An association between a person and certain CDR data will not be relevant or appropriate merely because, for instance, a sibling or other relative of the person has been supplied goods or services which the data concerns (see the discussion of 'associate' at B.106 to B.111 below).

B.104 Where information is primarily about a good or service but reveals information about a person's use of that good or service, it 'relates to' the person.[92]

B.105 By using the broad phrase 'relates to', the CDR system captures meta-data.[93]

Associate

B.106 As outlined in paragraph B.91, for a person to be a CDR consumer the CDR data must relate to that person because of the supply of a good or service to the person or one or more of that person's 'associates'.[94]

B.107 This means a person can be a 'CDR consumer' for CDR data relevant to goods or services used by one of their associates, such as a partner, family member or related body corporate.[95]

B.108 In this context, 'associate' has the same meaning as in the *Income Tax Assessment Act 1936* (ITA Act).[96] Section 318 of the ITA Act defines 'associates' with respect to natural persons, companies, trustees and partnerships.[97]

B.109 For natural persons, an associate includes:

- a relative
- a partner
- a trustee of a trust under which the person or another associate benefits, or

[90] *PMT Partners Pty Ltd (in liq) v Australian National Parks and Wildlife Service* (1995) 184 CLR 301, 331 (Toohey and Gummow JJ).

[91] Competition and Consumer Act, paragraph 56AI(3)(a).

[92] Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, section 1.108.

[93] This includes meta-data of the type found not to be 'about' an individual for the purpose of the Privacy Act in *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFA 4: Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, section 1.106.

[94] Competition and Consumer Act, paragraph 56AI(3)(a).

[95] Examples of this include where CDR data relates to a joint account or where a CDR consumer purchases goods or services used by a household.

[96] Competition and Consumer Act, subsection 56AI(3).

[97] For the purposes of the CDR system, associates of partnerships are not directly relevant, as a partnership is not a 'person'.

- certain companies able to be sufficiently influenced by the person or their associates.

B.110 The ITA Act offers further guidance on when a person is an 'associate' of a natural person, trustee of a trust or a company.

B.111 The ITA Act does not define 'associate' with respect to a government entity. This means that a government entity that is not a company cannot be a CDR consumer if the CDR data relates to the entity because of the supply of a good or service to one or more of the entity's 'associates', because the entity does not have any 'associates' as defined in the ITA Act.

Eligible CDR consumer

B.112 While 'CDR consumer' is defined in the Competition and Consumer Act, only 'eligible' CDR consumers may make consumer data requests to access or transfer their CDR data under the CDR Rules.

B.113 A consumer is 'eligible' if, at that time all of the following are met:[98]

- for any consumer – the consumer is an account holder or a secondary user[99] for an account with the data holder that is open
- for a consumer that is an individual – the consumer is 18 years or older
- for a consumer that is a partner in a partnership for which there is partnership account[100] with the data holder – the partnership account is open,[101] and
- the additional criteria in the relevant sector schedule to the CDR Rules are met.[102]

B.114 Schedule 3 to the CDR Rules provides that banking consumers are only 'eligible' if the consumer is able to access their banking account online, or where relevant, if the partnership account is set up in such a way that it can be accessed online (together, 'online consumers').[103]

B.115 Schedule 4 to the CDR Rules provides that energy consumers are only 'eligible' if the consumer is a customer of the retailer in relation to an eligible arrangement, the account relates to the arrangement, and certain consumption requirements are met.[104] Unlike the

---

[98] CDR Rules, rule 1.10B.

[99] A person is a 'secondary user' for an account with a data holder if the person is an individual who is 18 years or older, 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: rule 1.7. 'Account privileges' is defined in the relevant sector schedule to the CDR Rules: see clause 2.2 of Schedule 3 and clause 2.2 of Schedule 4. For the banking sector, clause 2.2 of Schedule 4 for the energy sector. For the staged application of the CDR Rules in relation to secondary users, see the relevant sector schedule to the CDR Rules. For general information on the staged application of CDR Rules, see paragraphs B.250 to B.252.

[100] A 'partnership account' means an account with a data holder that is held by or on behalf of the partnership or the partners in a partnership: CDR Rules, rule 1.7.

[101] For the staged application of the CDR Rules in relation to partnerships, see the relevant sector schedule to the CDR Rules. For general information on the staged application of CDR Rules, see paragraphs B.250 to B.252.

[102] For the banking sector, see CDR Rules, clause 2.1 to Schedule 3. For the energy sector, see CDR Rules, clause 2.1 of Schedule 4.

[103] See CDR Rules, clause 2.1 to Schedule 3.

[104] See CDR Rules, subclause 2.1(1) of Schedule 4. An arrangement will be an 'eligible arrangement' if it relates to one or more connection points or child connection points for which there is a financially responsible market participant in the National Electricity Market: CDR Rules, subclause 2.1(2) of Schedule 4.

banking sector, energy sector consumers will be eligible even if they do not have online access to their account with their energy retailer ('offline consumers'). These Guidelines provide advice with respect to how particular rules should be applied in the context of both online and offline consumers.

B.116 For SR data, if a CDR consumer is eligible to make or initiate a consumer data request to a primary data holder, the CDR consumer is not eligible to make or initiate a consumer data request for that data to the secondary data holder.[105] For further information on primary data holders, see paragraph B.157. For further information on SR data, see paragraphs B.39 to B.40.

B.117 For guidance regarding 'consumers' and 'CDR consumers', see paragraphs B.90 to B.94.

Consumer dashboard, or dashboard

B.118 Each accredited person and each data holder must offer (and in most circumstances must provide) a 'consumer dashboard' for CDR consumers.[106]

B.119 Where a CDR principal makes a consumer data request at the request of a CDR representative, it may arrange for a CDR representative to provide the consumer dashboard on its behalf.[107]

B.120 An accredited person's consumer dashboard is an online service that can be used by CDR consumers to manage consumer data requests and associated consents they have given to the accredited person or CDR representative (for example, to withdraw such consents). The service must also provide the CDR consumer with certain details of each consent. Each dashboard is visible only to the accredited person (or CDR representative where the CDR representative provides the dashboard) and the relevant CDR consumer.

B.121 The requirements for an accredited person's consumer dashboard are set out in CDR Rule 1.14.[108] For more information, see Chapter C (Consent).

B.122 A data holder's consumer dashboard is an online service that can be used by each CDR consumer to manage authorisations to disclose CDR data in response to consumer data requests (for example, to withdraw such authorisations). The service must also notify the CDR consumer of information related to CDR data disclosed pursuant to an authorisation.

B.123 A data holder must provide a consumer dashboard to a CDR consumer in the circumstances specified in the relevant sector schedule to the CDR Rules.[109] In the banking sector, a data holder must provide a consumer dashboard whenever it receives a consumer data request from an accredited person. In the energy sector, an offline consumer may choose not to have

[105] CDR Rules, rule 1.19.

[106] Energy consumers may be eligible CDR consumers even if they do not have an online account with their retailer: see paragraph B.115. For eligible energy consumers without an online account, the retailer must offer the CDR consumer a dashboard and provide it if the CDR consumer accepts: CDR Rules, clause 2.3 of Schedule 4. For other CDR consumers, each accredited person and data holder must provide a consumer dashboard: CDR Rules, rules 1.14 and 1.15.

[107] CDR Rules, subrule 1.14(5).

[108] Additional requirements for updating dashboards in relation to collections and disclosures are set out in CDR Rules, rules 7.4 and 7.9.

[109] For the banking sector, see CDR Rules, clause 2.3 of Schedule 3. For the energy sector, see CDR Rules, clause 2.3 of Schedule 4.

a consumer dashboard provided by their energy retailer.[110] The requirements for a data holder's consumer dashboard are set out in CDR Rule 1.15.[111] For more information, see the Guide to privacy for data holders.

B.124 If a consumer data request relates to a joint account where either the co-approval or pre-approval option applies, the data holder must provide each relevant account holder with a consumer dashboard.[112] Where this is the case, the dashboards must have the functionality set out in CDR Rule 4A.13, which includes:

- allowing relevant account holders to manage approvals in relation to authorisations
- allowing for the withdrawal of approvals.

B.125 These guidelines use the term 'dashboard' and 'consumer dashboard' interchangeably.

Consumer data request

B.126 A 'consumer data request' is a request made by an accredited person to a data holder,[113] accredited data recipient[114] or CDR representative[115] on behalf of a CDR consumer, in response to the consumer's valid request for the accredited person to seek to collect the consumer's CDR data.[116]

B.127 A request from an accredited person to a data holder must be made through the data holder's accredited person request service and must relate only to data the person has consent from the CDR consumer to collect and use.[117]

B.128 A request from an accredited person to a data holder or accredited data recipient must comply with the data minimisation principle.[118]

---

[110] Energy retailers must offer offline CDR consumers a dashboard and provide it if the CDR consumer accepts: CDR Rules, clause 2.3 of Schedule 4. For further information on offline consumers in the energy sector, see paragraph B.115.

[111] If the request is a SR data request, the primary data holder must comply with CDR Rule 1.15 and provide a consumer dashboard as if it were the data holder for that data: CDR Rules, rule 1.21.

[112] CDR Rule, rules 4A.13. Where a co-approval option or pre-approval option applies to a joint account and consumer data request, the data holder must provide each account holder with a consumer dashboard. This includes the requirements set out in CDR Rules, rules 1.15 and 4A.13.

[113] CDR Rules, rule 4.4.

[114] CDR Rules, rule 4.7A.

[115] CDR Rules, rule 4.3B.

[116] The CDR Rules also make provision for consumer data requests to be made directly by a CDR consumer to a data holder: CDR Rules, Part 3. A request directly from a CDR consumer must be made using a data holder's 'direct request service': CDR Rules, subrule 3.3(1). A data holder's 'direct request service' is an online service, that must comply with the data standards, that allows eligible CDR consumers to make consumer data requests under Part 3 of the CDR Rules directly to the data holder in a timely and efficient manner and allows consumers to receive the requested data in human-readable form: CDR Rules, subrule 1.13(2). However:

- for the banking sector, there is currently no compliance date for a data holder's obligations under Part 3 of the CDR Rules: CDR Rules, clause 6.6 of Schedule 3.
- for the energy sector, Part 3 of the CDR Rules does not apply in relation to energy sector data: CDR Rules, clause 8.5 of Schedule 4.

[117] CDR Rules, subrule 4.4(3). There are no equivalent requirements under CDR Rule 4.7A for how an accredited person makes a consumer data request to an accredited data recipient.

[118] CDR Rules, subrules 4.4(1) and 4.7A(1).

B.129 Refer to Chapter 3 (Privacy Safeguard 3) and Chapter C (Consent) for further information.

SR data request

B.130 A SR data request (or shared responsibility data request) is a consumer data request for a CDR consumer's CDR data where that data is or includes SR data.[119] Like other consumer data requests, SR data requests will be made by an accredited person on a consumer's behalf.[120] SR data requests must be made to the primary data holder for the CDR data.[121]

B.131 For further information on primary and secondary data holders, see paragraphs B.157 to B.158. For further information on SR data, see paragraphs B.39 to B.40.

Accredited person request service

B.132 A data holder's 'accredited person request service' is an online service allowing accredited persons to make consumer data requests to the data holder on behalf of eligible CDR consumers.[122]

B.133 It also allows accredited persons to receive requested data in machine-readable form.

B.134 This service must conform with the data standards.

B.135 If an accredited person proposes to make a SR data request on behalf of a CDR consumer, the accredited person must make the request using the primary data holder's direct request service.[123]

Valid request

B.136 A 'valid' request is defined in the CDR Rules in Part 4 (Consumer data requests made by accredited persons).[124]

B.137 Under Part 4 of the CDR Rules, a request is 'valid' if:

- the CDR consumer has requested the accredited person to provide goods or services to themselves or another person and the accredited person needs to collect the CDR data and use it in order to provide those goods or services
- the accredited person has asked the CDR consumer to give their consent for the person to collect their CDR data from a CDR participant and use that CDR data in order to provide those goods or services, and

---

[119] CDR Rules, rule 1.7.

[120] The CDR Rules also make provision for SR data request to be made directly by a CDR consumer to a primary data holder using the primary data holder's 'direct request service': CDR Rules, subrule 1.22(2). Currently, the energy sector is the only CDR sector with SR data. Part 3 of the CDR Rules (Consumer data requests made by eligible CDR consumers) does not apply to energy sector data: CDR Rules, clause 8.5 of Schedule 4. This means that currently, no CDR consumers will be able to directly make an SR data request.

[121] CDR Rules, subrules 1.22(2) and 1.23(2).

[122] CDR Rules, subrule 1.13(3).

[123] CDR Rules, subrule 1.23(2).

[124] It is also defined in Part 3 (Consumer data requests made by eligible CDR consumers). However, for the banking sector, there is currently no compliance date for a data holder's obligations under Part 3 of the CDR Rules: CDR Rules, clause 6.6 of Schedule 3. For the energy sector, Part 3 of the CDR Rules does not apply in relation to energy sector data: CDR Rules, clause 8.5 of Schedule 4.

- the CDR consumer has given a collection consent and a use consent in response to the accredited person's request (and that consent has not been withdrawn).[125]

B.138 Refer to Chapter 3 (Privacy Safeguard 3) for further information regarding valid requests, and Chapter C (Consent) for information regarding collection and use consents.

Competition and Consumer Regulations

B.139 The 'Competition and Consumer Regulations' refer to the *Competition and Consumer Regulations 2010*.

B.140 The Governor-General may make regulations prescribing matters required or permitted by the Competition and Consumer Act to be prescribed, or necessary or convenient to be prescribed for carrying out or giving effect to that Act.[126] This includes regulations that exempt a person or class of persons from CDR provisions in relation to particular CDR data or one or more classes of CDR data.[127] It also includes regulations that modify the operation of CDR obligations for a person or class of persons.[128]

B.141 Currently, the Competition and Consumer Regulations exempt AEMO from certain privacy safeguard obligations, modify how the privacy safeguards apply to retailers in the energy sector, and modify certain provisions for parts of the banking sector.[129]

CDR Rules

B.142 The consumer data rules (CDR Rules) refer to the Competition and Consumer (Consumer Data Right) Rules 2020.

B.143 The Minister has the power to make rules to determine how the CDR system functions in each sector.[130] CDR Rules may be made on aspects of the CDR system (as provided in Part IVD of the Competition and Consumer Act) including the privacy safeguards,[131] accreditation of data recipients and the disclosure, collection, use, accuracy, storage, security or deletion of CDR data for which there are one or more CDR consumers.[132]

[125] CDR Rules, rule 4.3.

[126] Competition and Consumer Act, subsection 172(1).

[127] Competition and Consumer Act, paragraphs 56GE(2)(a)-(b). See also Explanatory Statement, Competition and Consumer Amendment (Consumer Data Right) Regulations 2021, page 1.

[128] Competition and Consumer Act, paragraph 56GE(2)(c). See also Explanatory Statement, Competition and Consumer Amendment (Consumer Data Right) Regulations 2021, page 1.

[129] Competition and Consumer Regulations, Part 2BA.

[130] Competition and Consumer Act, subsection 56BA(1).

[131] Competition and Consumer Act, Part IVD, Division V.

[132] Competition and Consumer Act, section 56BB.

Current

Current consent

B.144 A consent is 'current' if it has not expired under CDR Rule 4.14.[133]

B.145 CDR Rule 4.14 provides that a consent expires when one of the following occurs:

- if it is withdrawn, in accordance with CDR Rule 4.13(1)(a) or (b)
- at the end of the period the CDR consumer consented to, in accordance with CDR Rule 4.11
- 12 months have passed after consent was given or last amended
- for a collection consent:
  - when the accredited person is notified by the data holder of the withdrawal of authorisation[134]
  - when the accredited person with a collection consent to collect CDR data from a particular accredited data recipient is notified by the accredited data recipient of the expiry of the AP disclosure consent to disclose that CDR data[135]
- for an AP disclosure consent to disclose CDR data to a particular accredited person, when the accredited data recipient is notified by the accredited person of the expiry of the collection consent to collect that CDR data[136]
- if the accredited person's accreditation is revoked or surrendered, when this revocation or surrender takes effect[137]
- upon an accredited person becoming a data holder of particular CDR data (in this situation, each of the accredited person's consents that relate to the CDR data would expire),[138] or
- if another CDR Rule provides that consent expires.

B.146 For further information on when a consent expires, see Chapter C (Consent).

Current authorisation

B.147 Authorisation to disclose particular CDR data to an accredited person is 'current' if it has not expired under CDR Rule 4.26.[139]

B.148 CDR Rule 4.26 provides that authorisation expires when one of the following occurs:

- if it is withdrawn

[133] CDR Rules, subrule 1.7(1) (Definitions).

[134] CDR Rules, subrule 4.14(1A).

[135] CDR Rules, subrule 4.14(1B).

[136] Ibid.

[137] CDR Rules, subrule 4.14(2).

[138] CDR Rules, subrule 4.14(1C).

[139] CDR Rules, rule 1.7.

- if the CDR consumer ceases to be eligible
- when the data holder is notified by the accredited person of the withdrawal of consent to collect the CDR data
- if the authorisation was for disclosure of CDR data over a specified period, at the end of that period or the period as last amended
- if the authorisation was for disclosure of CDR data on a single occasion, once the disclosure has occurred
- once 12 months have passed after authorisation was given
- if the accreditation of the accredited person to whom the data holder is authorised to disclose is revoked or surrendered, when the data holder is notified of that revocation or surrender, or
- if another CDR Rule provides that authorisation expires.[140]

B.149 For further information on when an authorisation expires, see the Guide to privacy for data holders.

Consumer Experience Guidelines

B.150 The Consumer Experience Guidelines set out guidelines for best practice design patterns to be used by entities seeking consent and/or authorisation from consumers under the CDR system.

B.151 The Consumer Experience Guidelines are made by the Data Standards Body and cover matters including:

- the process and decision points for a CDR consumer when consenting to share their data
- what (and how) information should be presented to CDR consumers to support informed decision making, and
- language that should be used (where appropriate) to ensure a consistent experience for CDR consumers across the broader CDR ecosystem.

B.152 The Consumer Experience Guidelines contain examples illustrating how a range of key CDR Rules can be implemented.

B.153 The Consumer Experience Guidelines are available on the Data Standards Body website, consumerdatastandards.gov.au.

Data holder

B.154 A person is a data holder of CDR data if: [141]

[140] See CDR Rules, subclause 7.2(3) of Schedule 3 and subclause 9.2(3) of Schedule 4.

[141] Competition and Consumer Act, section 56AJ.

- the CDR data falls within a class of information specified in the designation instrument for the relevant sector[142]
- the CDR data is held by (or on behalf of) the person on or after the earliest holding day[143]
- the CDR data began to be held by (or on behalf of) the person before that earliest holding day, is of continuing use and relevance (e.g. a current account number),[144] and is not about the provision of a product or service by (or on behalf of) the person before the earliest holding day[145] (e.g. a transaction on an account)[146]
- the person is not a designated gateway for the CDR data, and
- any of the three cases below apply:
  - **First case – person is also specified in the designation instrument:** the person is specified or belongs to a class of persons specified in a designation instrument and neither the CDR data, nor any other CDR data from which the CDR data was directly or indirectly derived, was disclosed to the person under the CDR Rules.[147]
  - **Second case – reciprocity arising from the person being disclosed other CDR data under the CDR Rules:** neither the CDR data, nor any other CDR data from which the CDR data was directly or indirectly derived, was disclosed to the person under the CDR Rules, and the person is an accredited data recipient of other CDR data.[148]
  - **Third case – conditions in the CDR Rules are met:** the CDR data or any other CDR data from which the CDR data was directly or indirectly derived was disclosed to the person under the CDR Rules, the person is an accredited person and the conditions specified in the CDR Rules are met.[149]

B.155 For further information on the privacy obligations for data holder, see the Guide to privacy for data holders.

Primary and secondary data holders

B.156 In the current CDR system, only the energy sector has 'primary' and 'secondary' data holders. For the energy sector, 'primary data holder' and 'secondary data holder' are defined

---

[142] For further information on designation instruments, which state the persons who are data holders in each sector, see paragraphs B.171 to B.173. See also Competition and Consumer Act, paragraph 56AC(2)(a).

[143] Being the earliest holding date specified in the designation instrument for the relevant sector. The earliest holding day for each CDR sector is set out in the table at paragraph B.159.

[144] Explanatory Memorandum, Treasury Laws Amendment (2020 Measures No. 6) Bill 2020, [2.35].

[145] For a product or service that the person began providing before the earliest holding day and continued providing after that day, the person will:

- not be the data holder of CDR data about the person's provision of the product or service before that day, but
- be the data holder of CDR data about the person's provision of the product or service on or after the earliest holding day (provided all the other criteria in s 56AJ of the Competition and Consumer Act, as discussed at paragraphs B.154 are met by the entity): see Competition and Consumer Act, Note 2 to section 56AJ.

[146] Explanatory Memorandum, Treasury Laws Amendment (2020 Measures No. 6) Bill 2020, [2.35].

[147] For example, the person is an accredited data recipient of that CDR data or is an outsourced service provider to whom the CDR data was disclosed under CDR Rules, rule 1.10.

[148] Competition and Consumer Act, subsection 56AJ(3). This means that the person is an accredited person who is an accredited data recipient in respect of data other than the CDR data in question.

[149] The conditions for each sector are outlined in the sector specific schedule to the CDR Rules. For the banking sector, see CDR Rules, clause 7.2 of Schedule 3. For the energy sector, see CDR Rules, clause 9.2 of Schedule 4.

in Schedule 4 to the CDR Rules.[150] Primary and secondary data holders share responsibility for responding to requests for CDR data that is or includes SR data (SR data requests).[151] Data holders will only be 'primary' or 'secondary' data holders for SR data.

B.157 For the energy sector, the primary data holder is the retailer that has a direct relationship with the CDR consumer.[152] Under the energy sector designation instrument, the retailer is not a specified data holder for the SR data identified in Schedule 4 to the CDR Rules.[153] Despite this, from the point of view of the CDR consumer, the primary data holder is treated as if it were the data holder for the consumer's SR data. This means a consumer or accredited person will make the SR data request to the primary data holder. The primary data holder will then seek the consumer's authorisation to disclose SR data, will offer (and in most circumstances provide) the consumer dashboard, and will disclose (or refuse to disclose) the requested SR data.[154]

B.158 For the energy sector, the secondary data holder is AEMO. The primary data holder must request relevant SR data from AEMO as secondary data holder where it needs this information to respond to the SR data request.[155] The secondary data holder is then authorised to disclose the CDR data directly to the primary data holder that has received the relevant consumer data request.[156] If the secondary data holder chooses not to disclose the requested SR data, it must notify the primary data holder of its refusal.[157] While AEMO is a data holder, in some cases it is treated differently to primary data holders in the energy sector. Certain chapters in these guidelines therefore specify that references to data holders do not include AEMO.[158]

Earliest holding day

B.159 A designation instrument must specify the 'earliest holding day' for a particular sector. This is the earliest day applicable to the sector for holding the designated information.[159] The earliest holding day for each designated CDR sector is outlined in the table below.

---

[150] CDR Rules, rule 1.7. See also CDR Rules, clause 4.3 of Schedule 4.

[151] For further information on SR data, see paragraphs B.39 to B.40.

[152] CDR Rules, subclause 4.3(b) of Schedule 4 and Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 3–6.

[153] See Consumer Data Right (Energy Sector) Designation 2020, subsections 8(2) and 12(2); CDR Rules, clauses 4.3 and 1.2 of Schedule 4.

[154] See CDR Rules, subrules 1.22(2), 1.23(2), 1.21 and 1.22(6). See also Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, pages 3–4.

[155] CDR Rules, subrule 1.22(5). The primary data holder will request this information when it has received a SR data request that includes information held by the secondary data holder, the consumer has authorised the disclosure of that data, and the primary data holder has not refused the SR data request under CDR Rules, rule 4.7: See CDR Rules, subrule 1.23(9) and Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 4. The secondary data holder is required to have an online service to receive and respond to requests from primary data holders for CDR data it holds: CDR Rules, subrule 1.20(2).

[156] See Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 3.

[157] CDR Rules, subrule 1.22(5).

[158] See Chapter 1 (Privacy Safeguard 1), Chapter 10 (Privacy Safeguard 10), Chapter 11 (Privacy Safeguard 11) and Chapter 13 (Privacy Safeguard 13).

[159] Competition and Consumer Act, paragraph 56AC(2)(c). Notwithstanding the earliest holding day, a person may be a data holder of CDR data that it held (or was held on its behalf) before the earliest holding day if the data is of continuing

CDR sector	Earliest holding day
Banking sector	1 January 2017[160]
Energy sector	1 July 2018[161]
Telecommunications sector	1 January 2022[162]

Data minimisation principle

B.160 The data minimisation principle limits the scope and amount of CDR data an accredited person may collect and use.

B.161 An accredited person collects and uses CDR data in compliance with the data minimisation principle if:[163]

- when making a consumer data request on behalf of a CDR consumer, the person does not seek to collect:
  - more CDR data than is reasonably needed, or
  - CDR data that relates to a longer time period than is reasonably needed

  in order to provide the goods or services requested by the CDR consumer, and
- the person does not use the collected data or derived data beyond what is reasonably needed in order to provide the requested goods or services or to fulfill any other purpose consented to by the CDR consumer.

Data standards

B.162 A 'data standard' is a standard made by the Data Standards Chair of the Data Standards Body under section 56FA of the Competition and Consumer Act.

B.163 Data standards are about:

- the format and description of CDR data
- the disclosure of CDR data
- the collection, use, accuracy, storage, security and deletion of CDR data
- de-identifying CDR data, or

use and relevance, and is not about the provision of a product or service by (or on behalf of) the person before the earliest holding day: Competition and Consumer Act, paragraph 56AJ(1)(ba).

[160] Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, subsection 5(3).

[161] Consumer Data Right (Energy Sector) Designation 2020, subsection 6(3).

[162] Consumer Data Right (Telecommunications Sector) Designation 2022, subsection 5(3). Note that, as at the date of publication of this document, there are no rules allowing for the sharing of designated telecommunications data pursuant to the CDR. For further information see paragraphs B.171 to B.173.

[163] CDR Rules, rule 1.8.

- other matters prescribed by regulations.[164]

B.164 The current data standards are available on Consumer Data Standards website, consumerdatastandards.gov.au and include the following:

- API Standards
- Shared Responsibility Standards
- Information Security Standards
- Register Standards, and
- Consumer Experience Standards.

Consumer Experience Standards

B.165 The 'Consumer Experience Standards' are data standards[165] regarding:

- the obtaining of authorisations and consents and withdrawal of authorisations and consents
- the collection and use of CDR data, including requirements to be met by CDR participants in relation to seeking consent from CDR consumers.
- the authentication of CDR consumers, and
- the types of CDR data and descriptions of those types to be used by CDR participants in making and responding to requests ('Data Language Standards').

B.166 The Consumer Experience Standards are available on Consumer Data Standards website, consumerdatastandards.gov.au.

Data Language Standards

B.167 The 'Data Language Standards' are data standards[166] regarding the types of CDR data and descriptions of those types to be used by CDR participants in making and responding to requests.

B.168 The Data Language Standards form part of the Consumer Experience Standards and are available on the Consumer Data Standards website, consumerdatastandards.gov.au.

Designated gateway

B.169 A 'designated gateway' is a person specified as a gateway in a legislative instrument made under subsection 56AC(2) of the Competition and Consumer Act, to whom CDR data is (or is to be) disclosed under the CDR Rules because of the reasons in paragraph 56AL(2)(c) of the Competition and Consumer Act.[167]

[164] Competition and Consumer Act, section 56FA and CDR Rules, rule 8.11.

[165] Competition and Consumer Act, section 56FA and CDR Rules, rule 8.11.

[166] Competition and Consumer Act, section 56FA and CDR Rules, rule 8.11.

[167] See section 56AL of the Competition and Consumer Act for the definition of 'designated gateway'.

B.170 There are currently no designated gateways in the banking sector or energy sector.[168] 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.[169]

Designation instrument

B.171 A 'designation instrument' is a legislative instrument made by the Minister under subsection 56AC(2) of the Competition and Consumer Act.

B.172 A designation instrument designates a sector of the Australian economy for the purposes of the CDR system by specifying classes of information that can be shared under the CDR, among other things. A designation instrument has the effect of enlivening the ability to make rules allowing for the sharing of designated data pursuant to the CDR.[170]

B.173 Existing CDR designation instruments are listed in the table below. The designation instrument for each CDR sector is also available on the Federal Register of Legislation.

CDR sector	Designation Instrument
Banking sector	Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019
Energy sector	Consumer Data Right (Energy Sector) Designation 2020
Telecommunications sector	Consumer Data Right (Telecommunications Sector) Designation 2022[171]

Disclosure

B.174 'Disclosure' is not defined in the Competition and Consumer Act or the Privacy Act.

B.175 Under the CDR system 'disclose' takes its ordinary, broad meaning.

B.176 An entity discloses CDR data when it makes the data accessible or visible to others outside the entity.[172] This interpretation focuses on the act done by the disclosing party, and not on

[168] 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.

[169] For further information on the effect of designation instruments, see paragraph B.172.

[170] See Competition and Consumer Act, Division 2 of Part IVD.

[171] At the date of publication of these guidelines, there are no rules allowing for the sharing of designated telecommunications data under the CDR system.

[172] Information will be 'disclosed' under the CDR system regardless of whether an entity retains effective control over the data.

the actions or knowledge of the recipient. Disclosure, in the context of the CDR system, can occur even where the data is already held by the recipient.[173]

B.177 For example, an entity discloses CDR data when it transfers a copy of the data in machine-readable form to another entity.

B.178 Where an accredited data recipient engages a third party to perform services on its behalf, the provision of CDR data to that third party will in most circumstances be a disclosure (see paragraphs B.258 to B.261 for the limited circumstances where it will be a 'use').

B.179 'Disclosure' is a separate concept from:

- 'Unauthorised access' which is addressed in Chapter 12 (Privacy Safeguard 12). An entity is not taken to have disclosed CDR data where a third party intentionally exploits the entity's security measures and gains unauthorised access to the information. Examples include unauthorised access following a cyber-attack or a theft, including where the third party then makes that data available to others outside the entity.
- 'Use' which is discussed in paragraphs B.258 to B.261 below. 'Use' encompasses information handling and management activities occurring within an entity's effective control, for example, when staff of an entity access, read, exchange or make decisions based on CDR data the entity holds.

Eligible

B.180 'Eligible' CDR consumers are discussed at paragraphs B.112 to B.117.

General research

B.181 'General research' is defined in CDR Rule 1.7 to mean research undertaken by an accredited data recipient with CDR data de-identified in accordance with the CDR Rules that does not relate to the provision of goods or services to any particular CDR consumer. An example is product or business development.[174]

Holds

B.182 Subsection 4(1) of the Competition and Consumer Act provides that a person 'holds' information if they have possession or control of a record (within the meaning of the Privacy Act)[175] that contains the information.[176] This definition is comparable to the definition of 'holds' in the Privacy Act.[177]

B.183 The term 'holds' extends beyond physical possession of a record to include a record that a CDR entity has the right or power to deal with. Whether a CDR entity 'holds' a particular item

[173] For a similar approach to interpreting 'disclosure', see *Pratt Consolidated Holdings Pty Ltd v Commissioner of Taxation* [2011] AATA 907, [112]–[119].

[174] Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020,* [21].

[175] 'Record' is defined in subsection 6(1) of the Privacy Act.

[176] Competition and Consumer Act, subsection 4(1).

[177] Privacy Act, subsection 6(1).

of CDR data may therefore depend on the particular data collection, management and storage arrangements it has adopted. For example, a CDR entity 'holds' CDR data where:

- it physically possesses a record containing the CDR data and can access that data physically or by use of an electronic device (such as decryption software), or
- it has the right or power to deal with the CDR data, even if it does not physically possess or own the medium on which the CDR data is stored. For example, the entity has outsourced the storage of CDR data to a third party but it retains the right to deal with it, including to access and amend that data.

Joint account

B.184 A joint account is an account with a data holder for which there are 2 or more account holders. Each account holder must be:

- an individual
- so far as the data holder is aware, acting in their own capacity and not on behalf of another person, and
- an 'eligible CDR consumer'.[178]

A 'partnership account' is not a joint account.[179]

B.185 For the purposes of the CDR system, one of three disclosure options applies to a joint account:[180]

- **pre-approval option**: joint account data may be disclosed in response to a valid CDR consumer data request on the authorisation of the requester, without the approval of the relevant account holders. This option applies to a joint account by default.[181]
- **co-approval option**: joint account data may be disclosed in response to a valid CDR consumer data request only after the requester has authorised the disclosure, and each of the relevant joint account holders has approved the disclosure
- **non-disclosure option**: means that joint account data may not be disclosed even in response to a valid CDR consumer data request.

B.186 A data holder must provide the pre-approval and non-disclosure options, but may choose whether to make the co-approval option available.[182]

B.187 Part 4A of the CDR Rules sets out the rules that apply to CDR consumer data requests for the disclosure of CDR data that relates to a joint account.[183]

---

[178] See paragraphs B.112 to B.117 for further information about 'an eligible CDR consumer'.

[179] CDR Rules, subrule 1.7(1) (Definitions).

[180] CDR Rules, rule 4A.5.

[181] CDR Rules, subrule 4A.5(5).

[182] CDR Rules, subrules 4A.5(2) and (3).

[183] For more information, see 'Authorisation' in Chapter C (Consent), and the OAIC's Guide to privacy for data holders.

Outsourced service provider

B.188 The CDR Rules provide that an 'outsourced service provider' is a person who, under a CDR outsourcing arrangement with a principal:

- collects CDR data from a CDR participant on behalf of the principal , and/or
- provides goods or services to the principal using CDR data that it has collected on behalf of the principal or that has been disclosed to it by the principal.[184]

B.189 An outsourced service provider must not disclose any service data[185] to another person, other than under a further outsourcing arrangement.[186] This means an outsourced service provider may further outsource its functions under the arrangement to another person, where they have a CDR outsourcing arrangement in place with that person. In this case, their original CDR outsourcing arrangement with their principal will require them to ensure that the other person complies with the requirements of the further CDR outsourcing arrangement.[187]

B.190 For the meaning of 'collects', refer to B.68 to B.70 above.

B.191 For the meaning of 'discloses', refer to B.174 to B.179 above.

CDR outsourcing arrangement

B.192 A CDR outsourcing arrangement is a written contract between a principal and an outsourced service provider (the 'provider'). Under this arrangement a provider will collect CDR data on behalf of the principal and/or provide goods or services to the principal using the service data that it has collected or that has been disclosed to it by the principal. [188]

B.193 CDR data collected by, or disclosed to, an outsourced service provider under a CDR outsourcing arrangement, including any data directly or indirectly derived from such CDR data, is known as 'service data'.[189]

B.194 The CDR outsourcing arrangement must require the provider to:

- take the steps in Schedule 2 to the CDR Rules to protect service data, as if it were an accredited data recipient
- not use or disclose service data other than in accordance with the CDR outsourcing arrangement
- not disclose service data to another person otherwise than under a further CDR outsourcing arrangement, and if it does so, to ensure that the other person complies with the requirements of the CDR outsourcing arrangement, and
- if directed by the principal under the CDR outsourcing arrangement:
  - provide access to any service data that it holds

[184] CDR Rules, rules 1.7(1) and 1.10.

[185] See paragraph B.193 in relation to 'service data'.

[186] CDR Rules, paragraph 1.10(2)(b)(v).

[187] CDR Rules, paragraph 1.10(2)(b)(vi).

[188] CDR Rules, rule 1.10.

[189] CDR Rules, subrule 1.10(4). 'Service data' is also discussed from paragraph B.236.

- return any CDR data that the principal disclosed to it
- delete (in accordance with the CDR data deletion process) any service data disclosed to it by the principal
- provide to the principal records of any deletion that are required to be made under the CDR data deletion process, and
- direct any other person to which it has disclosed CDR data to take corresponding steps.[190]

B.195 An affiliate cannot engage an outsourced service provider to collect data on their behalf, but may engage a provider to provide goods or services using CDR data disclosed to it by the affiliate.[191]

B.196 A CDR representative must not engage an outsourced service provider.[192]

B.197 For information on the meaning of 'service data' in relation to a CDR outsourcing arrangement, see B.236 below.

Principal under a CDR outsourcing arrangement

B.198 A principal under a CDR outsourcing arrangement is a party to such an arrangement with an outsourced service provider under which the provider:

- collects CDR data from a CDR participant on behalf of the principal, and/or
- provides goods or services to the principal using CDR data that it has collected on behalf of the principal or that has been disclosed to it by the principal.[193]

B.199 If a principal is an accredited person, it must ensure that the provider complies with the provider's requirements under the CDR outsourcing arrangement.[194]

B.200 A principal is liable for the collection, use and disclosure of CDR data by their outsourced service provider (and its subcontractors), regardless of whether that collection, use or disclosure is in accordance with the CDR outsourcing arrangement.[195]

Purpose

B.201 A person is deemed to engage in conduct for a particular 'purpose' if they engage in the conduct for purposes which include that purpose, and where that purpose is a substantial purpose.[196]

B.202 The purpose of an act is the reason or object for which it is done.

---

[190] CDR Rules, paragraph 1.10(2)(b).

[191] CDR Rules. subrule 5.1B(4).

[192] CDR Rules, paragraph 1.10AA(2)(c).

[193] CDR Rules, rule 1.10.

[194] CDR Rules, subrule 1.16(1).

[195] CDR Rules, rule 7.6.

[196] Competition and Consumer Act, paragraph 4F(1)(b).

B.203 There may be multiple purposes. If one of those purposes is a substantial purpose, a person is deemed to engage in conduct for that particular purpose.[197] This means that:

- all substantial purposes for which a person holds CDR data are deemed to be a 'purpose' for which the person holds the data, and
- if one purpose for a use of CDR data is direct marketing, and that purpose is a substantial purpose, the use is deemed to be for the purpose of direct marketing for the purposes of Privacy Safeguard 6.

Reasonable, Reasonably

B.204 'Reasonable' and 'reasonably' are used in the privacy safeguards and CDR Rules to qualify a test or obligation. For example, for CDR data to have a 'CDR consumer', at least one person must be identifiable or 'reasonably' identifiable from the CDR data or other information held by the relevant entity.[198]

B.205 'Reasonable' and 'reasonably' are not defined in the Competition and Consumer Act or the Privacy Act. The terms bear their ordinary meaning, as being based upon or according to reason and capable of sound explanation.

B.206 What is reasonable is a question of fact in each individual case. It is an objective test that has regard to how a reasonable person, who is properly informed, would be expected to act in the circumstances. What is reasonable can be influenced by current standards and practices.[199]

B.207 An entity must be able to justify its conduct as 'reasonable'. The High Court has observed that whether there are 'reasonable grounds' to support a course of action 'requires the existence of facts which are sufficient to [persuade] a reasonable person',[200] and 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'.[201] There may be a conflicting range of objective circumstances to be considered, and the factors in support of a conclusion should outweigh those against.

Reasonable steps

B.208 References to 'reasonable steps' are used in the privacy safeguards and CDR Rules. Examples include:

- Privacy Safeguard 11, which includes a requirement for data holders and accredited data recipients to take reasonable steps to ensure the quality of disclosed CDR data.[202]

---

[197] Competition and Consumer Act, section 4F.

[198] Competition and Consumer Act, paragraph 56AI(3)(c).

[199] For example, *Jones v Bartlett* [2000] HCA 56, [57]–[58] (Gleeson CJ); *Bankstown Foundry Pty Ltd v Braistina* [1986] HCA 20, [12] (Mason, Wilson and Dawson JJ).

[200] *George v Rockett* (1990) 170 CLR 104, 112.

[201] *McKinnon v Secretary, Department of Treasury* (2006) 228 CLR 423, 430 (Gleeson CJ & Kirby J).

[202] See Chapter 11 (Privacy Safeguard 11) for information about the obligations under Privacy Safeguard 11 (section 56EN of the Competition and Consumer Act).

- CDR Rule 1.10C, where a person is taken to be a trusted adviser if the accredited data recipient has taken reasonable steps to confirm that the person was, and remains, a member of a specified class.[203]

B.209 The 'reasonable steps' test is an objective test and is to be applied in the same manner as 'reasonable' and 'reasonably'.

B.210 An entity must be able to justify that reasonable steps were taken.

Redundant data

B.211 CDR data is 'redundant data' if the data is collected by an accredited data recipient under the CDR system and the entity no longer needs any of the data for a purpose permitted under the CDR Rules or for a purpose for which the entity may use or disclose it under Division 5, Part IVD of the Competition and Consumer Act.[204]

B.212 For further information on redundant data, including how to meet the obligation under Privacy Safeguard 12 to delete or de-identify redundant data, see Chapter 12 (Privacy Safeguard 12).

Required consumer data

B.213 CDR data is 'required consumer data' if it is required to be disclosed by a data holder to:

- a CDR consumer in response to a valid consumer data request under CDR Rule 3.4(3), or
- an accredited person in response to a consumer data request under CDR Rule 4.6(4).

B.214 'Required consumer data' for each CDR sector is defined in the relevant sector schedule to the CDR Rules.[205]

Required or authorised by an Australian law or by a court/tribunal order

B.215 A number of the privacy safeguards and CDR Rules provide an exception if a CDR entity is 'required or authorised by or under an Australian law or a court/tribunal order' to act differently. For example, Privacy Safeguard 6 which prohibits the use or disclosure of CDR data by an accredited data recipient unless, for example, the use or disclosure is required or authorised by or under another Australian law or a court/tribunal order.[206]

---

[203] See Chapter 6 (Privacy Safeguard 6) for information about disclosures by accredited data recipients to trusted advisers.

[204] Competition and Consumer Act, subsection 56EO(2). Note that this section also applies to designated gateways. For information on designated gateways, see paragraphs B.169 to B.170.

[205] For the banking sector, see CDR Rules, clause 3.2 of Schedule 3. For the energy sector, see CDR Rules, clause 3.2 of Schedule 4.

[206] And the accredited data recipient makes a written note of the use or disclosure. Competition and Consumer Act, paragraph 56EI(1)(c). See Chapter 6 (Privacy Safeguard 6) for further information.

Australian law

B.216 'Australian law' has the meaning given to it in the Privacy Act.[207] It means:

- an Act of the Commonwealth, or of a State or Territory
- regulations or any other instrument made under such an Act
- any other law in force in the Jervis Bay Territory or an external Territory, or
- a rule of common law or equity.[208]

Court/tribunal order

B.217 'Court/tribunal order' has the meaning given to it in the Privacy Act. It means an order, direction or other instrument made by a court, a tribunal, a judge, a magistrate, a person acting as a judge or magistrate, a judge or magistrate acting in a personal capacity, or a member or an officer of a tribunal.[209]

B.218 The definition applies to orders and the like issued by Commonwealth, State and Territory courts, tribunals and members, and officers. The definition includes an order, direction or other instrument that is of an interim or interlocutory nature.

B.219 The reference to a judge or a magistrate acting in a personal capacity means that the definition applies to an order or direction issued by a judge or magistrate who has been appointed by government to an office or inquiry that involves the exercise of administrative or executive functions, including functions that are quasi-judicial in nature. An example is a judge who is appointed by Government to conduct a royal commission.

Required

B.220 A person who is 'required' by an Australian law or a court/tribunal order to handle data in a particular way has a legal obligation to do so and cannot choose to act differently.

B.221 The obligation will usually be indicated by words such as 'must' or 'shall' and may be accompanied by a sanction for non-compliance.

Authorised

B.222 A person who is 'authorised' under an Australian law or a court/tribunal order has discretion as to whether they will handle data in a particular way. The person is permitted to take the action but is not required to do so. The authorisation may be indicated by a word such as 'may' but may also be implied rather than expressed in the law or order.

B.223 A person may be impliedly authorised by law or order to handle data in a particular way where a law or order requires or authorises a function or activity, and this directly entails the data handling practice.

---

[207] Competition and Consumer Act, subsection 4(1).

[208] Privacy Act, subsection 6(1).

[209] Privacy Act, subsection 6(1).

B.224 For example, a statute that requires a person to bring information to the attention of a government authority where they know or believe a serious offence has been committed[210] may implicitly authorise a person to use CDR data to confirm whether or not the offence has been committed, and then may require the person to disclose the data to the authority.

B.225 An act or practice is not 'authorised' solely because there is no law or court/tribunal order prohibiting it. The purpose of the privacy safeguards is to protect the privacy of consumers by imposing obligations on persons in their handling of CDR data. A law will not authorise an exception to those protections unless it does so by clear and direct language.[211]

Required or authorised to use or disclose CDR data under the CDR Rules

B.226 For data holders, certain regulatory provisions refer to situations where the data holder is or was 'required or authorised' to disclose the CDR data under the CDR Rules. For example, the requirement in Privacy Safeguard 13 to respond to a correction request applies where the data holder was 'earlier required or authorised under the CDR Rules' to disclose the CDR data.[212]

B.227 For accredited data recipients, certain regulatory provisions refer to situations where the accredited data recipient is 'required or authorised' under the CDR Rules to use or disclose CDR data. For example, Privacy Safeguard 6 provides that an accredited data recipient must not use or disclose CDR data unless, for example, the use or disclosure is required or authorised under the CDR Rules.[213]

Required

B.228 A data holder is 'required' to disclose required consumer data[214] under the CDR Rules:

- in response to a valid consumer data request under CDR Rules subrule 3.4(3), subject to rule 3.5, and
- in response to a consumer data request from an accredited person on behalf of a CDR consumer under subrule 4.6(4) of the CDR Rules, subject to rules 4.6A and 4.7, where the data holder has a current authorisation to disclose the data from the CDR consumer.

B.229 A primary data holder will be 'required' to disclose any SR data covered by a SR data request under the CDR Rules as if the primary data holder were the data holder for that data.[215]

B.230 An accredited data recipient is never 'required' to use or disclose CDR data under the CDR Rules.

---

[210] For example, subsection 316(1) of the *Crimes Act 1900* (NSW).

[211] See *Coco v The Queen* (1994) 179 CLR 427.

[212] Competition and Consumer Act, paragraph 56EP(1)(c). See Chapter 13 (Privacy Safeguard 13) for further information.

[213] Competition and Consumer Act, paragraph 56EI(1)(b). See Chapter 6 (Privacy Safeguard 6) for further information.

[214] See paragraphs B.213 to B.214 for further information about 'required consumer data'.

[215] CDR Rules, subrules 1.22(6) and 1.23(7).

Authorised

B.231 A data holder may be 'authorised' to disclose a consumer's CDR data to an accredited person by the relevant CDR consumer.[216] Such an authorisation must be in accordance with Division 4.4 of the CDR Rules.

B.232 A secondary data holder will be 'authorised' to disclose the SR data that it holds to the primary data holder when requested.[217]

B.233 An accredited data recipient is 'authorised' to use or disclose CDR data under the CDR Rules in the circumstances outlined in CDR Rule 7.5. For information on the permitted uses or disclosures that do not relate to direct marketing, see Chapter 6 (Privacy Safeguard 6). For information on the permitted uses or disclosures that relate to direct marketing, see Chapter 7 (Privacy Safeguard 7).

Required product data

B.234 The privacy safeguards do not apply to required product data.[218]

B.235 'Required product data' for each CDR sector is defined in the relevant sector schedule to the CDR Rules.[219]

Service data

B.236 'Service data' in relation to a CDR outsourcing arrangement refers to CDR data collected by or disclosed to an outsourced service provider under a CDR outsourcing arrangement, including any data directly or indirectly derived from such CDR data.[220]

B.237 For guidance regarding 'outsourced service providers' and 'CDR outsourcing arrangements', see B.188 to B.189.

B.238 'Service data' in relation to a CDR representative arrangement refers to CDR data disclosed to a CDR representative by its CDR principal for the purposes of the CDR representative arrangement, including any data directly or indirectly derived from such CDR data.[221]

B.239 For guidance regarding 'CDR representatives', 'CDR principals' and 'CDR Representative arrangements', see B.49 to B.65.

---

[216] CDR Rules, rule 4.5.

[217] Explanatory Statement, Competition and Consumer (Consumer Data Right) Amendment Rules (No. 2) 2021, page 4.

[218] Competition and Consumer Act, subsection 56EB(1).

[219] For the banking sector, see CDR Rules, clause 3.1 of Schedule 3. For the energy sector, see CDR Rules, clause 3.1 of Schedule 4.

[220] CDR Rules, subrule 1.10(4).

[221] CDR Rules, subrule 1.10AA(3).

Sponsor

B.240 A sponsor is a person with unrestricted accreditation who has entered into a written contract ('a sponsorship arrangement') with another person (known as the 'affiliate') that meets certain requirements.[222]

B.241 The role of the sponsor is to disclose CDR data to their affiliate so that the affiliate may use that data to provide goods or services directly to a CDR consumer. The sponsor may also collect CDR data on behalf of their affiliate, and use or disclose CDR data at the request of their affiliate.

B.242 As a sponsor and their affiliate are both accredited persons, each entity will be liable in their own right for their handling of CDR data. For example, where a sponsor makes a consumer data request, or uses or discloses CDR data at their affiliate's request, the sponsor remains liable for their own conduct and must ensure they comply with the relevant privacy obligations.

B.243 The CDR Rules do contain some specific obligations for sponsors, particularly in relation to disclosure, notification and CDR policy. For more information, see Chapter C (paragraphs C.15, C.30, C.72, C.103, diagram after C.118), Chapter 1 (paragraph 1.54), Chapter 3 (paragraphs 3.26 – 3.27, diagram after 3.42), Chapter 5 (paragraph 5.3, 5.10, 5.25, 5.38 – 5.40), Chapter 6 (paragraphs 6.24, 6.73), Chapter 10 (paragraph 10.53), Chapter 11 (paragraph 11.31), Chapter 12 (paragraphs 12.21, 12.72 – 12.75), and the OAIC's separate guidance for sponsors.[223]

B.244 The CDR Rules also impose some additional obligations on sponsors in relation to accreditation and the sponsorship arrangement.[224] For example, a sponsor has obligations relating to an affiliate's information security capabilities and related compliance matters.[225] A sponsor must also notify the Data Recipient Accreditor as soon as practicable after becoming a sponsor of an affiliate, or when a sponsorship arrangement is suspended, expires or is terminated.[226]

B.245 A sponsor may enter into multiple sponsorship arrangements.

Sponsorship Arrangement

B.246 A 'sponsorship arrangement' is a written contract between a 'sponsor' and an 'affiliate' which meets the minimum requirements in CDR Rule 1.10D(1).

B.247 The sponsorship arrangement must provide for the sponsor to disclose CDR data that it holds as an accredited data recipient to their affiliate, in response to a consumer data request from the affiliate.

---

[222] CDR Rules, rule 1.10D.

[223] See https://www.oaic.gov.au/consumer-data-right/guidance-and-advice/sponsored-accreditation-model-privacy-obligations-of-sponsors.

[224] Sponsors should also refer to the 'sponsored accreditation' section of the ACCC's CDR Accreditation Guidelines: https://www.cdr.gov.au/sites/default/files/2022-02/CDR-Accreditation-guidelines-version-3-published-16-February-2022.pdf.

[225] CDR Rules, clause 2.2 of Schedule 1.

[226] CDR Rules, subrule 5.14(2).

B.248 The arrangement must also require the affiliate to provide the sponsor with appropriate information and access to their operations as needed for the sponsor to fulfil their obligations as a sponsor (see paragraph B.244).

B.249 The arrangement may also provide for the sponsor to make consumer data requests, or to use or disclose CDR data, at their affiliate's request.

Staged application

B.250 The relevant sector schedule to the CDR Rules may provide for the 'staged application' of CDR Rules in that sector. Staged application means that the CDR Rules will apply to a broader range of data holders or a broader range of CDR data within that sector over time. The result of staged application is that data holders may be required to comply with particular CDR data sharing obligations from different dates.

B.251 Part 6 of Schedule 3 to the CDR Rules provides for staged application of the CDR Rules in the banking sector. Under Part 6, the CDR Rules apply to a progressively broader range of banking sector data holders and a progressively broader range of banking products.[227] The staged application of consumer data sharing obligations for certain banking sector data holders and banking products commenced on 1 July 2020.[228]

B.252 Part 8 of Schedule 4 to the CDR Rules provides for staged application of the CDR Rules in the energy sector. Under Part 8, the CDR Rules apply to a progressively broader range of energy sector data holders.[229] The staged application of consumer data sharing obligations for certain energy sector data holders commences on 15 November 2022.[230]

Trusted adviser

B.253 'Trusted advisers' are defined in the CDR Rules.[231] Consumers can nominate certain people to be their 'trusted adviser' and provide consent for an accredited data recipient to share data with that adviser, in order to receive advice or a service.[232]

B.254 A trusted adviser must belong to one of the following specified classes:

- qualified accountants within the meaning of the *Corporations Act 2001*[233]

[227] For further detail regarding the staged application of the CDR Rules in the banking sector, see Part 6 of Schedule 3 to the CDR Rules. For general information about the rollout of the CDR, see the CDR website: https://www.cdr.gov.au/rollout.

[228] See CDR Rules, clause 6.6 of Schedule 3.

[229] For further detail regarding the staged application of the CDR Rules in the energy sector, see Part 8 of Schedule 4 to the CDR Rules. For general information about the rollout of the CDR, see the CDR website: https://www.cdr.gov.au/rollout.

[230] See CDR Rules, clause 8.6 of Schedule 4.

[231] See CDR Rules, subrule 1.10C(2).

[232] CDR representatives can also disclose data to a trusted adviser with a consumer's consent.

[233] Section 88B of the *Corporations Act 2001* states that ASIC may declare in writing persons who are qualified accountants for the purposes of that Act. ASIC's qualified accountant declaration instrument can be accessed here: https://asic.gov.au/regulatory-resources/financial-services/financial-product-disclosure/certificates-issued-by-a-qualified-accountant/.

- people admitted to the legal profession that hold a current practising certificate
- registered tax agents, BAS agents and tax (financial) advisers within the meaning of the *Tax Agent Services Act 2009*
- financial counselling agencies within the meaning of the ASIC Corporations (Financial Counselling Agencies) Instrument 2017/792
- financial advisers that are relevant providers under the *Corporations Act 2001*, other than provisional and limited-service time-share advisers, and
- mortgage brokers within the meaning of the *National Consumer Credit Protection Act 2009*.

B.255 A person is taken to be a member of a trusted adviser class for the purposes of rule 1.10C of the CDR Rules if the accredited data recipient has taken reasonable steps to confirm that the person was, and remains, a member of the class.

B.256 Trusted advisers are not CDR participants and are therefore not subject to the privacy safeguards or other obligations that apply under the CDR system. They should, however, be aware of their professional obligations that relate to their handling of a consumer's data, and privacy obligations under the Privacy Act if they are an APP entity.

B.257 An accredited data recipient must not make any of the following a condition for the supply of the goods or services:

- the consumer nominating a trusted adviser
- the consumer nominating a particular person as a trusted adviser, or
- the consumer giving consent to disclosure of data to a trusted adviser.[234]

Use

B.258 'Use' is not defined in the Competition and Consumer Act or the Privacy Act. 'Use' is a separate concept from disclosure, which is discussed at paragraphs B.174– B.179

B.259 Generally, an entity 'uses' CDR data when it handles and manages that data within its effective control. Examples include the entity:

- accessing and reading the data
- searching records for the data
- making a decision based on the data
- passing the data from one part of the entity to another
- de-identifying data, and
- deriving data from the data.

B.260 In limited circumstances, providing CDR data to a third party (such as a cloud service provider) for limited purposes may be a use of data, rather than a disclosure (see paragraphs B.174– B.179). However, such a provision of data will constitute a 'use' only if the data remains encrypted at all times, and the third party does not hold or have access to the

[234] CDR Rules, subrule 1.10C(4).

decryption keys (on the basis that the third party would be technically unable to view or access the data at all times, and there would therefore be no disclosure).

B.261 Whether the provision of CDR data constitutes a use or a disclosure needs to be considered carefully on a case-by-case basis, and depends on the specific technical arrangements in place with the third party. If the third party could access or view unencrypted data, for example, to maintain or provide its service, then the provision of data to that third party would constitute a disclosure, and a CDR outsourcing arrangement would be required (see paragraphs B.192 to B.197).

Voluntary consumer data

B.262 'Voluntary consumer data' is CDR data a data holder may disclose to a CDR consumer under CDR Rule 3.4(2) or to an accredited person under subrule 4.6(2) of the CDR Rules.

B.263 'Voluntary consumer data' for each CDR sector is defined in the relevant sector schedule to the CDR Rules.[235]

B.264 An example of voluntary consumer data is 'materially enhanced information', which is excluded from certain specified classes of information in the designation instruments for the banking and energy sectors,[236] but may nonetheless be CDR data (as it is data derived from a specified class of information in the relevant designation instrument).[237]

Voluntary product data

B.265 The privacy safeguards do not apply to voluntary product data.[238]

B.266 'Voluntary product data' for each CDR sector is defined in the relevant sector schedule to the CDR Rules.[239]

B.267 An example of voluntary product data in the banking sector is information about the availability or performance of a particular savings account product, where that information is not publicly available.[240]

---

[235] For the banking sector, see CDR Rules, clause 3.2 of Schedule 3. For the energy sector, see CDR Rules, clause 3.2 of Schedule 4.

[236] See section 10 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 and section 11 of the Consumer Data Right (Energy Sector) Designation 2020. See also section 7 of the Consumer Data Right (Telecommunications Sector) Designation 2022, 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. For further information on designation instruments, see paragraphs B.171 to B.173.

[237] Competition and Consumer Act, subsection 56AI(1).

[238] Competition and Consumer Act, subsection 56EB(1).

[239] For the banking sector, see CDR Rules, clause 3.1 of Schedule 3. For the energy sector, see CDR Rules, clause 3.1 of Schedule 4.

[240] See CDR Rules, clause 3.1(1)-(2) of Schedule 3.