Chapter B:

Key concepts

Version 1.0, February 2020

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 regime and demonstrates the operation of several key concepts in the CDR regime.

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

Key concepts in the CDR regime explained

Accredited persons

Meadow Bank wants to receive CDR data to provide products or services to consumers under the CDR regime, so it applies to the ACCC (the Data Recipient Accreditor)[1] to become accredited. The ACCC is satisfied that Meadow Bank meets the accreditation criteria under the CDR Rules and grants accreditation. Meadow Bank is therefore an **accredited person** and is allowed to receive CDR data under the CDR regime.

CDR data

Carly is a customer of Sunny Bank, but is interested in what alternative credit card rates Meadow Bank could provide. Carly has an existing credit card, and provides Meadow Bank with a valid request (with her consent) to collect her account numbers, balances and features from Sunny Bank 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**.

Data holders

Sunny Bank is a **data holder**. This is because Sunny Bank holds Carly's CDR data, is not a designated gateway for the data, began to hold CDR data after 1 January 2017[3] and is an authorised deposit-taking institution (one of the categories specified in s 56AJ(1)(d) of the Competition and Consumer Act).[4]

---

[1] See paragraph B.11.

[2] Section 56AI(1) of the Competition and Consumer Act. The designation instrument for the banking sector sets out the classes of information that are subject to the CDR regime, 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 regime.

[3] 1 January 2017 is the 'earliest holding day' specified in the designation instrument for the banking sector: s 5(3) of the designation instrument. See paragraphs B.91 to B.92 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.

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 s 56AI(3)(b),[5] and
- Carly is identifiable or reasonably identifiable from the CDR data.[6]

Accredited data recipients

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

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

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

- 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.[7]

Consumer dashboards

Given that Meadow Bank has made a consumer data request on Carly's behalf, Meadow Bank provides Carly with a **consumer dashboard**.[8] 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 Bank, Sunny Bank also provides Carly with a consumer dashboard that will allow Carly to manage and view details about her authorisation.[9]

---

[5] See paragraph B.35 for further information.

[6] Section 56AI(3) of the Competition and Consumer Act.

[7] Section 56AK of the Competition and Consumer Act.

[8] CDR Rule 1.14(1)(a).

[9] CDR Rule 1.15(1)(a).

Accredited data recipient

B.4 A person is an 'accredited data recipient' if the person:

- is an accredited person (see paragraphs B.9-B.12 below)
- was disclosed CDR data from a data holder under the CDR Rules
- 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.[10]

B.5 A person will only be an 'accredited data recipient' in relation to the CDR data that it has been disclosed under the CDR Rules.[11]

B.6 Where an accredited person seeks consent from a consumer to collect and use CDR data, and subsequently seeks to collect CDR data, they do so as an accredited person because they are yet to collect the CDR data.

B.7 Once an accredited person has been disclosed CDR data under the CDR Rules, they will be both an accredited data recipient and an accredited person. For an illustration of how and when an accredited person becomes an accredited data recipient for CDR data, see the example under paragraph B.3.

B.8 A data holder may be accredited, and therefore be both a data holder and an accredited data recipient.

Accredited person

B.9 An 'accredited person' is a person who has been granted accreditation by the Data Recipient Accreditor.[12]

B.10 In the banking sector for example, an accredited person could be a bank or a fintech that wishes to provide a good or service using CDR data. This is demonstrated by the example under paragraph B.3.

B.11 The Data Recipient Accreditor is the Australian Competition and Consumer Commission (ACCC).[13]

B.12 To be granted an accreditation, the person must satisfy the accreditation criteria in Part 5 of the CDR Rules.

---

[10] Section 56AK of the Competition and Consumer Act. Rather, the person must hold that CDR data as a result of seeking to collect the CDR data from a data holder under the CDR Rules.

[11] If an accredited person is disclosed CDR data otherwise than in accordance with the CDR Rules (for instance, in breach of Privacy Safeguard 3), they will not become an 'accredited data recipient' for that CDR data.

In this situation, the *Privacy Act 1988* and the Australian Privacy Principles would apply (to the extent the CDR data is personal information, and where the accredited person is not a 'small business operator' under the *Privacy Act 1988* (see section 6E(1D) of the Privacy Act).

[12] Section 56CA(1) of the Competition and Consumer Act.

[13] The ACCC has been appointed as the Data Recipient Accreditor by the Treasurer under s 56CG of the Competition and Consumer Act.

Authorise, Authorisation

B.13 An authorisation must meet the requirements set out in the CDR Rules, and be sought in accordance with the data standards.[14]

B.14 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.

B.15 For the banking sector, for requests that relate to joint accounts, in some cases, the data holder might need to seek an authorisation from the other joint account holder.[15]

B.16 For further information, see Chapter C (Consent). 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.17 'CDR data' is information that is:

- within a class of information specified in the designation instrument for each sector,[16] or
- derived from the above information ('derived CDR data').[17]

Derived CDR data

B.18 'Derived CDR data' is data that has been wholly or partly derived from CDR data, or data derived from previously derived data.[18] This means data derived from 'derived CDR data' is also 'derived CDR data'.

B.19 'Derived' takes its ordinary meaning. This is because 'derived' is not defined in the Competition and Consumer Act or the *Privacy Act 1988* (the Privacy Act).

CDR participant

B.20 A 'CDR participant' is a data holder, or an accredited data recipient, of CDR data.[19]

---

[14] CDR Rule 4.5(2). See Division 4.4 of the CDR Rules.

[15] See clause 4.5 of Schedule 3 to the CDR Rules.

[16] Section 56AI(1) of the Competition and Consumer Act. The designation instrument for the banking sector sets out the classes of information that are subject to the CDR regime, 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 regime. The designation instrument for the banking sector is available here.

[17] Section 56AI(1) of the Competition and Consumer Act. The designation instrument for the banking sector (available here) excludes 'materially enhanced information' from the class of information about the use of a product. However, 'materially enhanced information' is nonetheless CDR data (as it is data derived from a specified class of information in the relevant designation instrument). For further information, see the Explanatory Statement to the Designation Instrument (available here) as well as the explanation of 'voluntary consumer data' in this Chapter.

[18] Section 56AI(2) of the Competition and Consumer Act.

[19] Section 56AL(1) of the Competition and Consumer Act.

CDR receipt

B.21 A 'CDR receipt' is a notice given by an accredited person to a CDR consumer who has consented to the accredited person collecting and using their CDR data, or given to a consumer who has withdrawn such a consent.[20]

B.22 CDR receipts must be given in accordance with CDR Rule 4.18.

CDR regime

B.23 The 'CDR regime' 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.24 The CDR regime 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.25 'Collect' is not defined in the Competition and Consumer Act or the Privacy Act.

B.26 Under the CDR regime '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.27 Section 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).[21]

Consent

B.28 Consent must meet the requirements set out in the CDR Rules.

B.29 Consent is the primary basis on which an accredited person may collect and use CDR data.[22]

[20] CDR Rule 4.18(1).

[21] 'Record' is defined in s 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 s 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.

[22] While consent is the only basis on which an accredited person may collect CDR data, consent is a primary basis on which an accredited person may use CDR data. See Chapter 6 (Privacy Safeguard 6) for further information regarding use of CDR data.

B.30 Consent also underpins how an accredited person or accredited data recipient may collect and use CDR data in the CDR regime.[23]

B.31 For further information, including the requirements by which an accredited person must seek consent from a consumer, see Chapter C (Consent).

Consumer, CDR consumer or 'eligible' CDR consumer

B.32 The 'CDR consumer' is the person who is able to:

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

B.33 A CDR consumer is an identifiable or reasonably identifiable person to whom the CDR data relates, because of the supply of a good or service either to the person or an associate of the person. [24] A consumer can be an individual, another person such as a company, or a business enterprise.[25]

B.34 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.[26]

B.35 The CDR data that relates to the 'CDR consumer' must be held by:

- a data holder of the CDR data
- an accredited data recipient of the CDR data, or
- an entity that holds the data on behalf of a data holder or accredited data recipient of the CDR data.[27]

B.36 Section 4B(1) of the Competition and Consumer Act does not apply for the purposes of determining whether a person is a 'CDR consumer'.[28] This section explains when a person is taken to have acquired particular goods or services as a consumer, outside of the CDR regime.

B.37 These guidelines use the term 'consumer' to refer to 'CDR consumer'.

---

[23] For example, an accredited person may only use or disclose CDR data in accordance with a current consent from the consumer unless an exception applies. One way in which an accredited person is authorised to use or disclose CDR data under the CDR Rules is to provide goods or services requested by the consumer. This must be done in compliance with the data minimisation principle and in accordance with a current consent from the consumer (CDR Rule 7.5(1)(a)). For further information, see Chapter 6 (Privacy Safeguard 6).

[24] Section 56AI(3)(a) of the Competition and Consumer Act. Note that s 56AI(3)(a)(ii) allows for regulations to be made to prescribe circumstances in which CDR data may relate to a person.

[25] Section 56AI(4) of the Competition and Consumer Act; Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Bill 2019*, paragraph 1.100.

[26] In the banking sector, a key example of this is where CDR data relates to a joint account.

[27] Section 56AI(3) of the Competition and Consumer Act.

[28] Section 56AI(4) of the Competition and Consumer Act.

Reasonably identifiable

B.38 For a person to be a 'CDR consumer', the person must be identifiable, or 'reasonably identifiable', from the CDR data or other information held by the entity.

B.39 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.54- B.56 or a discussion on the meaning of 'held') and
- whether it is practicable to use that information to identify the person.

B.40 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.41 See B.119-B.122 for a discussion on the meaning of 'reasonably'.

Relates to

B.42 For a person to be a 'CDR consumer', CDR data must 'relate to' that person.

B.43 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' depending on the statutory context.[29] The relevant context in the CDR regime is the Competition and Consumer Act and the Privacy Act.

B.44 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.[30]

B.45 CDR data will not 'relate to' a person unless the data itself is somehow relevant or appropriate for that person's use as a consumer under the CDR regime.

B.46 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.49-B.53 below).

B.47 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.[31]

---

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

[30] Section 56AI(3)(a) of the Competition and Consumer Act.

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

B.48 By using the broad phrase 'relates to', the CDR regime captures meta-data.[32]

Associate

B.49 For a person to be a CDR consumer, 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'.

B.50 In this context, 'associate' has the same meaning as in the *Income Tax Assessment Act 1936* (ITA Act).[33] Section 318 of the ITA Act defines 'associates' with respect to natural persons, companies, trustees and partnerships.[34]

B.51 For natural persons, an associate is:

- a relative
- a partner
- a trustee of a trust under which the person or another associate benefits, or
- certain companies able to be sufficiently influenced by the person or their associates.

B.52 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.53 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.

Held

B.54 CDR data that relates to a CDR consumer must be 'held' by:

- a data holder of the CDR data
- an accredited data recipient of the CDR data, or
- an entity that holds the data on behalf of a data holder or accredited data recipient of the CDR data.[35]

B.55 Section 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)[36] that contains the information.[37] This definition is comparable to the definition of 'holds' in the Privacy Act.[38]

---

[32] 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.

[33] Section 56AI(3) of the Competition and Consumer Act.

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

[35] Section 56AI(3) of the Competition and Consumer Act.

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

[37] Section 4(1) of the Competition and Consumer Act.

[38] Section 6(1) of the Privacy Act.

B.56 If a person has a right or power to deal with particular data, the person has effective control of the data and therefore 'holds' the data.

Eligible CDR consumer

B.57 While 'CDR consumer' is defined in the Competition and Consumer Act, only 'eligible' CDR consumers may make consumer data requests under the CDR Rules.

B.58 A consumer for the banking sector is 'eligible' if, at that time:

- for any consumer – the consumer has an account with the data holder that is open and set up in such a way that it can be accessed online
- for a consumer that is an individual – the consumer is 18 years or older, and
- for any consumer with a debit card, personal credit, business credit or charge card account – where the account is in the name of a single person (the 'account holder') but multiple individuals are authorised to make transactions, the consumer is the account holder.[39]

B.59 For guidance regarding 'consumers' and 'CDR consumers', see paragraphs B.32 – B.37.

Consumer dashboard, or dashboard

B.60 Each accredited person and each data holder must provide a 'consumer dashboard' for CDR consumers.

B.61 An accredited person's consumer dashboard is an online service that can be used by CDR consumers. Each dashboard is visible only to the accredited person and the relevant CDR consumer.

- CDR consumers can use their dashboard to manage consumer data requests and associated consents for the accredited person to collect and use CDR data.
- The service must also notify the consumer of information related to CDR data collected pursuant to a consent.

B.62 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. The service must also notify the consumer of information related to CDR data disclosed pursuant to an authorisation.

B.63 These guidelines use the term 'dashboard' and 'consumer dashboard' interchangeably.

Consumer data request

B.64 A 'consumer data request' is either:

- a request made directly by a CDR consumer to a data holder[40], or

[39] Clause 2.1 of Schedule 3 to the CDR Rules.

[40] CDR Rule 3.3(1).

- a request made by an accredited person to a data holder, 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.[41]

B.65 A request directly from a CDR consumer must be made using the data holder's direct request service and may be for some or all of the consumer's CDR data.[42]

B.66 A request from an accredited person must be made through the data holder's accredited person request service and must relate only to data the person has consent from the consumer to collect and use. A request from an accredited person must comply with the data minimisation principle.[43]

B.67 Refer to Chapter C (Consent) for further information.

Direct request service

B.68 A data holder's 'direct request service' is an online service that allows eligible CDR consumers to make consumer data requests directly to the data holder in a timely and efficient manner.[44]

B.69 It also allows CDR consumers to receive the requested data in human-readable form and sets out any fees for disclosure of voluntary consumer data.

B.70 This service must conform with the data standards.

Accredited person request service

B.71 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.[45]

B.72 It also allows accredited persons to receive requested data in machine-readable form.

B.73 This service must conform with the data standards.

Valid consumer data request

B.74 A consumer data request is 'valid' if it is made directly by an eligible CDR consumer.[46]

Valid request

B.75 A 'valid' request is defined in the CDR Rules in Part 3 (Consumer data requests made by eligible CDR consumers) and Part 4 (Consumer data requests made by accredited persons).

[41] CDR Rule 4.4(1).

[42] CDR Rule 3.3(1).

[43] CDR Rule 4.4(1).

[44] CDR Rule 1.13(2).

[45] CDR Rule 1.13(3).

[46] CDR Rule 3.3(3).

B.76 Under Part 3, a consumer data request made by a CDR consumer directly to a data holder is 'valid' if it is made by a CDR consumer who is eligible to make the request.[47]

B.77 An 'eligible' consumer for the banking sector is discussed above at paragraphs B.57 to B.59.

B.78 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 the CDR data to provide those goods or services
- the accredited person has asked the consumer to give their consent for the person to collect and use the CDR data in order to provide those goods or services and
- the CDR consumer has given consent in response to the accredited person's request (and that consent has not been withdrawn).[48]

B.79 Refer to Chapter 3 (Privacy Safeguard 3) for further information regarding valid requests.

CDR Rules

B.80 The consumer data rules (CDR Rules) refer to the *Competition and Consumer (Consumer Data Right) Rules 2020*.

B.81 The ACCC has the power to make rules,[49] with the consent of the Minister,[50] to determine how the CDR functions in each sector. CDR Rules may be made on all aspects of the CDR regime (as provided in Part IVD the Competition and Consumer Commission Act) including the privacy safeguards, accreditation of an entity, the Data Standards Body and the format of CDR data and the data standards.

Current

Current consent

B.82 Consent to collect and use particular CDR data is 'current' if it has not expired under CDR Rule 4.14.[51]

B.83 CDR Rule 4.14 provides that consent expires if:

- it is withdrawn
- the accredited person is notified by the data holder of the withdrawal of authorisation
- the period of consent has ended
- 12 months has passed after consent was given

[47] CDR Rule 3.3(3).

[48] CDR Rule 4.3.

[49] Section 56BA(1) of the Competition and Consumer Act.

[50] Section 56BR of the Competition and Consumer Act.

[51] CDR Rule 1.7(1) (Definitions).

- another CDR Rule provides that consent expires, or
- the accredited person's accreditation is revoked or surrendered.

Current authorisation

B.84 Authorisation to disclose particular CDR data to an accredited person is 'current' if it has not expired under CDR Rule 4.26.

B.85 CDR Rule 4.26 provides that authorisation expires if:

- it is withdrawn
- the consumer ceases to be eligible
- the data holder is notified by the accredited person of the withdrawal of consent to collect the CDR data
- the period of authorisation has ended
- authorisation was for a single occasion and the disclosure has occurred
- 12 months has passed after authorisation was given
- another CDR Rule provides that authorisation expires, or
- the accreditation of the accredited person to whom the data holder is authorised to disclose is revoked or surrendered.

Consumer Experience Guidelines

B.86 The Consumer Experience Guidelines set out guidelines for best practice design patterns to be used by entities seeking consent from consumers under the CDR regime.

B.87 The Consumer Experience Guidelines are made by the Data Standards Body and cover:

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

B.88 The Consumer Experience Guidelines contain supporting examples illustrating how a range of key CDR Rules can be implemented.

B.89 The Consumer Experience Guidelines are available on the Data Standards Body website, www.consumerdatastandards.org.au.

Data holder

B.90 A person is a data holder of CDR data if the person holds the CDR data, is not a designated gateway for the data, began to hold the data after the earliest holding day, and any of the three cases below apply:[52]

- 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.[53]
- 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.[54]
- 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.[55]

Earliest holding day

B.91 A designation instrument must specify the 'earliest holding day' for a particular sector. This is the day on which data held by an entity may be CDR data.[56]

B.92 Under the designation instrument for the banking sector, the earliest holding day is 1 January 2017.[57]

Data minimisation principle

B.93 The data minimisation principle limits the scope and amount of CDR data an accredited person may collect and use.

B.94 An accredited person collects and uses CDR data in compliance with the data minimisation principle if:[58]

a. when making a consumer data request on behalf of a consumer, the person does not seek to collect:

   i. more CDR data than is reasonably needed, or

[52] Section 56AJ(1) of the Competition and Consumer Act and CDR Rules 1.7(1) and 1.7(3).

[53] 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 Rule 4.8(2).

[54] Section 56AJ(3) of the Competition and Consumer Act. 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. Although under the designation instrument only authorised deposit-taking institutions (ADIs) are designated as persons who hold the specified classes of information for the purposes of s 56AC(2)(b), a non-ADI accredited person may become a data holder in respect of certain CDR data if this circumstance applies.

[55] The conditions for the banking sector are contained in clause 7.2 of Schedule 3 to the CDR Rules.

[56] Section 56AJ(1)(b) of the Competition and Consumer Act.

[57] Section 5(3) of the designation instrument.

[58] CDR Rule 1.8.

ii. CDR data that relates to a longer time period than is reasonably needed

in order to provide the goods or services requested by the consumer, and

b. 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.

Data standards

B.95 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.96 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
- other matters prescribed by regulations.[59]

B.97 The current data standards are available on CSIRO's Data61 Consumer Data Standards website, consumerdatastandards.org.au and include the following:

- API Standards
- Information Security Standards, and
- Consumer Experience Standards.

Consumer Experience Standards

B.98 The 'Consumer Experience Standards' are data standards[60] 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.99 The Consumer Experience Standards are available on CSIRO's Data61 Consumer Data Standards website, www.consumerdatastandards.org.au.

[59] Section 56FA(1) of the Competition and Consumer Act.

[60] Section 56FA(3) of the Competition and Consumer Act and CDR Rule 8.11.

Data Language Standards

B.100 The 'Data Language Standards' are data standards[61] regarding the types of CDR data and descriptions of those types to be used by CDR participants in making and responding to requests.

B.101 The Data Language Standards form part of the Consumer Experience Standards and are available on CSIRO's Data61 Consumer Data Standards website, www.consumerdatastandards.org.au.

Designated gateway

B.102 A 'designated gateway' is a person is specified in a legislative instrument made under s 56AC(2) of the Competition and Consumer Act.[62]

B.103 There are currently no designated gateways in the CDR regime.

Designation instrument

B.104 A 'designation instrument' is a legislative instrument made by the Minister under section 56AC(2) of the Competition and Consumer Act.[63]

B.105 A designation instrument designates a sector of the Australian economy for the purposes of the CDR regime by specifying classes of information that can be transferred under the CDR, among other things.

B.106 These guidelines use 'designation instrument' to refer to the designation instrument for the banking sector (the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019), dated 4 September 2019.

Disclosure

B.107 'Disclosure' is not defined in the Competition and Consumer Act or the Privacy Act.

B.108 Under the CDR regime 'disclose' takes its ordinary, broad meaning.

B.109 An entity discloses CDR data when it makes the data accessible or visible to others outside the entity.[64] This interpretation focuses on the act done by the disclosing party, and not on the actions or knowledge of the recipient. Disclosure, in the context of the CDR regime, can occur even where the data is already held by the recipient.[65]

---

[61] Section 56FA(3) of the Competition and Consumer Act and CDR Rule 8.11.

[62] Section 56AL of the Competition and Consumer Act.

[63] Section 56AM(1) of the Competition and Consumer Act.

[64] Information will be 'disclosed' under the CDR regime regardless of whether an entity retains effective control over the data. This is different to the situation under the Privacy Act, where in some limited circumstances the provision of information from an entity to a contractor to provide services on behalf of the entity may be a use, rather than a disclosure. See paragraph B.144 in Chapter B: Key concepts of the APP Guidelines.

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

B.110 For example, an entity discloses CDR data when it transfers a copy of the data in machine-readable form to another entity.

B.111 '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.145–B.146 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.112 'Eligible' CDR consumers are discussed at paragraphs B.57–B.59.

Outsourced service provider

B.113 The CDR Rules provide that an 'outsourced service provider' is a person to whom an accredited person discloses CDR data under a 'CDR outsourcing arrangement'.[66]

B.114 Any provision of CDR data by an accredited data recipient to an outsourced service provider will be a disclosure.[67]

CDR outsourcing arrangement

B.115 A person discloses CDR data to another person under a 'CDR outsourcing arrangement' if it does so under a written contract between the discloser and the recipient under which the recipient: [68]

- will provide, to the discloser, goods or services using CDR data
- must take the steps in Schedule 2 to the CDR Rules to protect CDR data disclosed to it by the discloser, and any CDR data that it directly or indirectly derives from the CDR data, as if it were an accredited data recipient
- must not use or disclose any such CDR data other than in accordance with the contract

[66] CDR Rules 1.7(1) (Definitions) and 1.10.

[67] Whether an accredited data recipient retains effective control over the data does not affect whether data is 'disclosed'. This is different to the situation under the Privacy Act, where in some limited circumstances the provision of information from an entity to a contractor to provide services on behalf of the entity may be a use, rather than a disclosure. See paragraph B.144 in Chapter B: Key concepts of the APP Guidelines.

See paragraph B.144 in Chapter B: Key concepts of the APP Guidelines.

[68] CDR Rules 1.7(1) (Definitions) and 1.10.

- must not disclose such CDR data to another person otherwise than under a CDR outsourcing arrangement, and if it does so, it must ensure that the other person complies with the requirements of the CDR outsourcing arrangement, and
- must, if directed by the discloser:
  - delete (in accordance with the CDR data deletion process) or return to the discloser any CDR data disclosed to it by the discloser
  - provide to the discloser 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.

Purpose

B.116 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.[69]

B.117 The purpose of an act is the reason or object for which it is done.

B.118 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.[70] 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.119 'Reasonable' and 'reasonably' are used in the privacy safeguards and CDR Rules to qualify a test or obligation. An example is that a 'CDR consumer' is a person who is identifiable or 'reasonably' identifiable from certain CDR data or related information.[71]

B.120 '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.121 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.[72]

---

[69] Section 4F(1)(b) of the Competition and Consumer Act.

[70] Section 4F of the Competition and Consumer Act.

[71] Section 56AI(3)(c) of the Competition and Consumer Act.

[72] 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).

B.122 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',[73] and 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'.[74] 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.123 The 'reasonable steps' test is an objective test and is to be applied in the same manner as 'reasonable' and 'reasonably'.

B.124 An entity must be able to justify that reasonable steps were taken.

Redundant data

B.125 CDR data is 'redundant data' if the data is collected by an accredited data recipient under the CDR regime 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.[75]

Required consumer data

B.126 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.127 'Required consumer data' for the banking sector is defined in clause 3.2 of Schedule 3 to the CDR Rules.[76]

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

Australian law

B.128 'Australian law' has the meaning given to it in the Privacy Act. It means:

---

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

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

[75] Section 56EO(2) of the Competition and Consumer Act. Note that this section also applies to designated gateways, however there are currently no designated gateways in the CDR regime.

[76] Clause 3.2(3) of Schedule 3 to the CDR Rules sets out what CDR data will be neither required consumer data nor voluntary consumer data.

- an Act of the Commonwealth, or of a State or Territory
- regulations or any other instrument made under such an Act
- a Norfolk Island enactment, or
- a rule of common law or equity.[77]

Court/tribunal order

B.129 '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.[78]

B.130 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.131 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.132 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.133 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.134 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.135 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.

B.136 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[79] 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.

---

[77] Section 6(1) of the Privacy Act.

[78] Section 6(1) of the Privacy Act.

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

B.137 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.[80]

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

Required

B.138 A data holder is 'required' to disclose CDR data under the CDR Rules:

- in response to a valid consumer data request under CDR Rule 3.4(3), subject to CDR Rule 3.5
- in response to a consumer data request from an accredited person on behalf of a CDR consumer under CDR Rule 4.6(4), subject to CDR Rule 4.7, where the data holder has a current authorisation to disclose the data from the CDR consumer, and
- in response to a product data request under CDR Rule 2.3(1), subject to CDR Rule 2.5, where a data holder is required to disclose required product data under CDR Rule 2.4(3) (however the privacy safeguards do not apply to required product data).

B.139 An accredited data recipient is never 'required' to disclose CDR data under the CDR Rules.[81]

Authorised

B.140 A data holder may be 'authorised' to disclose CDR data to an accredited person by a CDR consumer.[82] Such an authorisation must be in accordance with Division 4.4 of the CDR Rules.

B.141 A data holder is also authorised to disclose voluntary product data in response to a product data request under CDR Rule 2.4(2), however the privacy safeguards do not apply to required product data.

B.142 An accredited data recipient is 'authorised' to disclose CDR data under the CDR Rules:

- to the CDR consumer under CDR Rule 7.5(1)(c)
- to an outsourced service provider under CDR Rule 7.5(1)(d), and
- to a third party if the CDR data is de-identified, under CDR Rule 7.5(1)(e).

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

[81] In their capacity as an accredited data recipient.

[82] CDR Rule 4.5.

Required product data

B.143 In the banking sector, 'required product data' means CDR data for which there are no CDR consumers, and which is:[83]

- within a class of information specified in the banking sector designation instrument
- about the eligibility criteria, terms and conditions, price, availability or performance of a product
- publicly available, in the case where the CDR data is about availability or performance
- product specific data about a product, and
- held in a digital form.

B.144 The privacy safeguards do not apply to required product data.[84]

Use

B.145 '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.107–B.111 above.

B.146 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.

Voluntary consumer data

B.147 '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 CDR Rule 4.6(2).

B.148 For the banking sector, 'voluntary consumer data' is CDR data for which there is a CDR consumer that is:

- not required consumer data, and
- not specified in the CDR Rules as being neither required consumer data nor voluntary consumer data.[85]

---

[83] Clause 3.1(1) of Schedule 3 to the CDR Rules.

[84] Section 56EB(1) of the Competition and Consumer Act and s 6(1) of the Privacy Act.

[85] Clause 3.2(2) of Schedule 3 to the CDR Rules. Clause 3.2(3) of Schedule 3 to the CDR Rule sets out what CDR data will be neither required consumer data nor voluntary consumer data.

B.149 An example of voluntary consumer data is 'materially enhanced information', which is excluded from a specified class of information under section 10 of the designation instrument for the banking sector,[86] but may nonetheless be CDR data (as it is data derived from a specified class of information in the relevant designation instrument).

Voluntary product data

B.150 In the banking sector, 'voluntary product data' means CDR data for which there are no CDR consumers:

- that is within a class of information specified in the banking sector designation instrument
- that is product specific data about a product, and
- that is not required product data.[87]

B.151 The privacy safeguards do not apply to voluntary product data.[88]

[86] Section 10 of the designation instrument carves out information about the use of a product from being specified under section 7 where that information has been materially enhanced. Section 10(3) sets out, for the avoidance of doubt, information which is *not* materially enhanced information.

[87] Clause 3.1(2) of Schedule 3 to the CDR Rules.

[88] Section 56EB(1) of the Competition and Consumer Act.