Chapter B:

Key concepts

Consultation draft, October 2019

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.

Accredited data recipient

B.2 A person is an 'accredited data recipient' if the person:

- is an accredited person
- has collected CDR data from a data holder under the consumer data 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. [1]

B.3 A person will only be an 'accredited data recipient' in relation to the CDR data that it has collected under the consumer data rules.

B.4 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.5 Once an accredited person has collected CDR data, they will be an accredited data recipient in relation to that CDR data.

B.6 As such, a person may be both an accredited data recipient and an accredited person at any point in time, in relation to different consumers.[2]

B.7 Where a privacy safeguard applies to 'accredited data recipients', the privacy safeguard only applies in relation to CDR data collected by accredited persons under the consumer data rules.

Accredited person

B.8 An 'accredited person' is a person who has been granted accreditation by the Data Recipient Accreditor.[3]

B.9 The Data Recipient Accreditor is the Australian Competition and Consumer Commission (ACCC).[4]

B.10 To be granted an accreditation, the person must satisfy the accreditation criteria in Part 5 of the Consumer Data Rules.

---

[1] 56AK. Rather, the person must hold that CDR data as a result of seeking to collect the CDR data from a data holder under the Consumer Data Rules.

[2] The person would be an accredited person in relation to a consumer that it is seeking consent to collect and use CDR data from and an accredited data recipient in relation to consumers for which it has already collected CDR data.

[3] 56CA (1).

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

CDR data

B.11 'CDR data' is information that is:

- within a class of information specified in the designation instrument for each sector,[5] or
- derived from the above information ('derived CDR data').[6]

Derived CDR data

B.12 'Derived CDR data' is data that has been wholly or partly derived from CDR data, or data derived from previously derived data.[7] This means data derived from 'derived CDR data' is also 'derived CDR data'.

B.13 'Derived' takes its ordinary meaning. This is because 'derived' is not defined in the *Competition and Consumer Act 2010* (Cth) (Competition and Consumer Act) or the *Privacy Act 1988* (Cth) (the Privacy Act).

CDR participant

B.14 A 'CDR participant' is a data holder or an accredited data recipient.[8]

CDR receipt

B.15 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.[9]

B.16 CDR receipts must be given in accordance with Consumer Data Rule 4.18.

CDR regime

B.17 The 'CDR regime' was enacted by the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth) to insert a new Part IVD into the Competition and Consumer Act.

---

[5] The designation instrument specifies classes of data for each sector. 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.

[6] 56AI(1). 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 for the banking sector (available here) as well as the explanation of 'voluntary consumer data' in this Chapter.

[7] 56AI(2).

[8] 56AL(1).

[9] Consumer Data Rule 4.18(1).

B.18 The CDR regime includes the Consumer Data Rules, privacy safeguards, data standards, designation instruments, and any regulations made in respect of the provisions inserted into the Competition and Consumer Act by these amendments.

Collect

B.19 'Collects' is defined in section 4(1) of the Competition and Consumer Act, which 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 Competition and Consumer Act).

B.20 'Record' is defined in the Privacy Act to include a document or an electronic or other device, but does not include:[10]

- anything kept in a library, art gallery or museum for the purposes of reference, study or exhibition
- Commonwealth records as defined by subsection 3(1) of the *Archives Act 1983* that are in the open access period for the purposes of that Act
- certain records in the care of the National Archives of Australia
- documents placed by or on behalf of a person (other than an agency) in the memorial collection within the meaning of the *Australian War Memorial Act 1980*, or
- letters or other articles in the course of transmission by post. [11]

Consent

B.21 Consent must meet the requirements set out in the Consumer Data Rules.

B.22 Consent is the only basis on which an accredited person may collect and use CDR data.

B.23 Consent also underpins how an accredited person or accredited data recipient may collect and use CDR data in the CDR regime.[12]

B.24 For further information, including the requirements by which an accredited person must seek consent from a consumer, see Chapter C (Consent).

[10] The Privacy Act definition of 'record' also excludes a generally available publication, but as stated in B.19 generally available publications are included in the CDR definition of 'collects'. See Privacy Act, s 6.

[11] Privacy Act, s 6

[12] 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 Consumer Data 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 (Consumer Data Rule 7.5(1)(a)). For further information, see Chapter 6 (Privacy Safeguard 6).

Consumer, CDR consumer or 'eligible' CDR consumer

B.25 The 'CDR consumer' is the person who is able to:

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

B.26 A 'CDR consumer' is an identifiable or reasonably identifiable person to whom CDR data relates because of the supply of a good or service either to the person or to an associate of the person.[13]

B.27 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 or family member.[14]

B.28 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.[15]

B.29 Section 4B(1) of the Competition and Consumer Act does not apply for the purposes of determining whether a person is a CDR consumer.[16] This section explains when a person is taken to have acquired particular goods or services as a consumer, outside of the CDR regime.

B.30 The Privacy Safeguard guidelines use the term 'consumer' to refer to 'CDR consumer'.

Reasonably identifiable

B.31 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.32 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 B.47-B.50 for a discussion on the meaning of 'held'), and
- whether it is practicable to use that information to identify the person.

B.33 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

[13] 56AI(3)(a). 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.

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

[15] 56AI(3).

[16] 56AI(4).

person as a CDR consumer – the entity would need to handle CDR data which relates to the CDR consumer in accordance with the privacy safeguards.

B.34 See B.113-B.116 for a discussion on the meaning of 'reasonably'.

Relates to

B.35 For a person to be a CDR consumer, CDR data must 'relate to' that person.

B.36 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.[17] The relevant context in the CDR regime is the Competition and Consumer Act and the Privacy Act.

B.37 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 consumer data rules.[18]

B.38 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.39 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.42-B.46 below).

B.40 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.[19]

B.41 By using the broad phrase 'relates to', the CDR regime captures meta-data.[20]

Associate

B.42 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.43 In this context, 'associate' has the same meaning as in the *Income Tax Assessment Act 1936* (Cth) (the ITA Act).[21] Section 318 of the ITA Act defines 'associates' with respect to natural persons, companies, trustees and partnerships.[22]

B.44 For natural persons, an associate is:

- a relative
- a partner

---

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

[18] s 56AI(3)(a).

[19] Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2018, [1.108].

[20] 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 2018, [1.106].

[21] 56AI(3).

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

- 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.45 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.46 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 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.47 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.[23]

B.48 A person 'holds' data if they have possession or effective control of a medium that contains the CDR data. As 'held' is not defined in the Competition and Consumer Act, it takes its ordinary meaning, consistent with the OAIC's APP Guidelines.

B.49 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.

B.50 For example, a person 'holds' data where the person:

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

Eligible CDR consumer

B.51 While 'CDR consumer' is defined in the Competition and Consumer Act, only 'eligible' CDR consumers may make consumer data requests under the Consumer Data Rules.

B.52 A consumer for the banking sector is 'eligible' if they have an account with the data holder that is open and set up in such a way that it can be accessed online.[24]

B.53 A consumer for the banking sector who is an individual must be 18 years or older.

B.54 A person may be an eligible consumer if they are a body corporate, body politic or individual.

[23] 56AI(3).

[24] Consumer Data Rules, Schedule 3, clause 2.1.

Consumer dashboard

B.55 Each accredited person and each data holder must provide a 'consumer dashboard' for CDR consumers.

B.56 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.57 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.

Consumer data request

B.58 A 'consumer data request' is either:

- a request made directly by a CDR consumer to a data holder[25] or
- 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.[26]

B.59 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.[27]

B.60 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.[28]

B.61 Refer to Chapter C: Consent for further information.

Direct request service

B.62 A data holder's 'direct request service' is an online service allowing eligible CDR consumers to make consumer data requests directly to the data holder in a timely and efficient manner.[29]

[25] Consumer Data Rule 3.3(1).

[26] Consumer Data Rule 4.4(1).

[27] Consumer Data Rule 3.3(1).

[28] Consumer Data Rule 4.4(1).

[29] Consumer Data Rule 1.13(2)

B.63 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.64 This service must conform with the data standards.

Accredited person request service

B.65 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.[30]

B.66 It also allows accredited persons to receive requested data in machine-readable form.

B.67 This service must conform with the data standards.

Valid consumer data request

B.68 A consumer data request is 'valid' if it is made directly by an eligible CDR consumer.[31]

Valid request

B.69 A 'valid' request is defined in the Consumer Data Rules in Part 3 (Consumer data requests made by eligible CDR consumers) and Part 4 (Consumer data requests made by accredited persons).

B.70 Under Part 3, 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).[32]

B.71 Under Part 4, 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.[33]

B.72 An 'eligible' consumer for the banking sector is discussed above at the CDR Consumer key concept.

Consumer data rules

B.73 The ACCC has the power to make rules,[34] with the consent of the Minister,[35] to determine how the CDR functions in each sector. Consumer data rules may be made on all aspects of

[30] Consumer Data Rule 1.13(3).

[31] Consumer Data Rule 3.3(3).

[32] Consumer Data Rule 4.3.

[33] Consumer Data Rule 3.3(3).

[34] 56BA(1)

[35] 56BR

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.

B.74 On 2 September 2019, the ACCC published a lock down version of the Consumer Data Rules and accompanying Explanatory Statement, available at CDR Rules (banking).

B.75 This lock down version of the Consumer Data Rules cover the foundational rules required to implement the CDR in the banking sector.

B.76 Initially, the Consumer Data Rules will apply only to certain products that are offered by certain data holders in the banking sector. It is intended that the rules will progressively apply to a broader range of data holders and products over time.

Current

Current consent

B.77 Consent to collect and use particular CDR data is 'current' if it has not expired under Consumer Data Rule 4.14.[36]

B.78 Consumer Data 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
- another Consumer Data Rule provides that consent expires or
- the accredited person's accreditation is revoked or surrendered.

Current authorisation

B.79 Authorisation to disclose particular CDR data to an accredited person is 'current' if it has not expired under Consumer Data Rule 4.26.

B.80 Consumer Data Rule 4.26 provides that authorisation expires if:

- it is withdrawn
- the CDR 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 Consumer Data Rule provides that authorisation expires, or

[36] Consumer Data Rule 1.7(1) (Definitions).

- the accreditation of the accredited person to whom the data holder is authorised to disclose is revoked or surrendered.

Consumer Experience Guidelines

B.81 The 'Consumer Experience Guidelines' (or CX Guidelines) are data standards made by the Data Standards Body and the Data Standards Chair.

B.82 The Consumer Experience Guidelines set out guidelines for best practice design patterns to be used by entities seeking consent from consumers under the CDR.

B.83 The Consumer Experience Guidelines 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.84 The Consumer Experience Guidelines contain supporting examples illustrating how the Consumer Experience Guidelines can be implemented.

B.85 The Consumer Experience Guidelines are available on CSIRO's Data61 Consumer Data Standards website, www.consumerdatastandards.org.au.

Data holder

B.86 A person is a data holder of CDR data if the person holds 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:[37]

- The person is specified or belongs to a class of persons specified in a designation instrument and the CDR data or other CDR data from which the CDR data was directly or indirectly derived was not disclosed to the person under the Consumer Data Rules.[38]
- The CDR data or other CDR data from which the CDR data was directly or indirectly derived was not disclosed to the person under the Consumer Data Rules and the person is an accredited data recipient of other CDR data.[39]
- The CDR data or other CDR data from which the CDR data was directly or indirectly derived was disclosed to the person under the Consumer Data Rules, the person is an accredited person and the conditions specified in the Consumer Data Rules are met.

[37] 56AJ(1) and Consumer Data Rules 1.7(1) and 1.7(3).

[38] 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 Consumer Data Rule 4.8(2).

[39] 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.

Earliest holding day

B.87 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.[40]

B.88 Under the designation instrument for the banking sector, the earliest holding day is 1 January 2017.[41]

Data minimisation principle

B.89 The data minimisation principle limits the scope and amount of CDR data an accredited person may collect and use.

B.90 An accredited person collects and uses CDR data in compliance with the data minimisation principle if:[42]

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

   in order to provide the goods or services requested by the CDR 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.

B.91 The test is one of purpose and proportionality. An accredited person may only seek to collect or use CDR data for the purpose of providing the requested goods or services, and the CDR data sought or used must be reasonably needed (i.e. proportional) for that purpose.

B.92 It is not sufficient that the data is used or sought for the purpose of providing the requested goods or services. CDR data may be used or sought for the purpose of providing the requested goods or services, at the same time as being disproportionate to that purpose. For example, the amount of data sought or the number of data holders it is sought from may not be proportionate for that purpose.

Data standards

B.93 A 'data standard' is a standard made in writing and published on the internet[43] by the Data Standards Chair of the Data Standards Body as appointed by the Treasurer.

B.94 Data standards are about:

- the format and description of CDR data
- the disclosure of CDR data

[40] 56AJ(1)(b).

[41] 5(3).

[42] Consumer Data Rule 1.8.

[43] 56FC.

- the collection, use, accuracy, storage, security and deletion of CDR data
- de-identifying CDR data, or
- other matters prescribed by regulations.[44]

B.95 The current data standards are available on CSIRO's Data61 Consumer Data Standards website, consumerdatastandards.org.au/.

Designated gateway

B.96 A 'designated gateway' is a person is specified in a legislative instrument made under s 56AC(2) of the Competition and Consumer Act.[45]

B.97 There are currently no designated gateways in the CDR regime.

Designation Instrument

B.98 A 'designation instrument' is a legislative instrument made by the Minister under section 56AC(2) of the Competition and Consumer Act.[46]

B.99 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.100 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.101 'Disclosure' is not defined in the Competition and Consumer Act or the Privacy Act.

B.102 Under the CDR regime 'disclose' takes its ordinary, broad meaning as it does under the Privacy Act.[47]

B.103 An entity discloses CDR data when it makes the data accessible or visible to others outside the entity and releases the subsequent handling of the data from its effective control. 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.[48]

B.104 'Disclosure' is a separate concept from:

- 'Unauthorised access' which is addressed in Privacy Safeguard 12. An entity is not taken to have disclosed CDR data where a third party intentionally exploits the entity's

[44] 56FA(1).

[45] 56AL.

[46] 56AM(1).

[47] See OAIC, Australian Privacy Principles Guidelines (22 July 2019), Chapter B: Key Concepts [B.63 – B.69].

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

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.139-B.140 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.105 'Eligible' CDR consumers are discussed above at paragraphs B.51-B.54.

Outsourced service provider

B.106 The Consumer Data Rules provide that an 'outsourced service provider' is a person to whom an accredited person discloses CDR data under a 'CDR outsourcing arrangement'.[49]

B.107 A third-party service provider will not be an 'outsourced service provider' if data is not 'disclosed' to them.

CDR outsourcing arrangement

B.108 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: [50]

- the recipient will provide, to the discloser, goods or services using CDR data
- the recipient must take the steps in Schedule 2 of the Consumer Data Rules to protect CDR data disclosed to it by the outsourcer as if it were an accredited data recipient
- the recipient must not use or disclose any such CDR data other than in accordance with the contract
- the recipient 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
- the recipient 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 outsourcer
  - 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.

B.109 A CDR outsourcing arrangement requires the recipient to provide goods or services using CDR data. This means that, if an accredited person has an arrangement with a third party

[49] Consumer Data Rule 1.7(1) (Definitions) and 1.10.

[50] Consumer Data Rule 1.7(1) (Definitions) and 1.10.

service provider in respect of collected CDR data but the third party does not use the CDR data to provide goods or services, the third party will not fall under the definition of 'outsourced service provider' and cannot be disclosed CDR data under the Consumer Data Rules.

Purpose

B.110 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.[51]

B.111 The purpose of an act is the reason or object for which it is done.

B.112 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.[52] 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.113 'Reasonable' and 'reasonably' are used in the privacy safeguards and Consumer Data 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.[53]

B.114 '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.115 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.[54] What is reasonable can be influenced by current standards and practices.

B.116 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',[55] and 'involves an evaluation of the known facts, circumstances and considerations which may bear rationally upon the issue in question'.[56] There may be a conflicting range of objective circumstances to be considered, and the factors in support of a conclusion should outweigh those against.

---

[51] 4F(1)(b).

[52] 4F.

[53] 56AI(3)(c).

[54] 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).

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

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

Reasonable steps

B.117 The 'reasonable steps' test is an objective test and is to be applied in the same manner as 'reasonable' and 'reasonably'.

B.118 An entity must be able to justify that reasonable steps were taken.

Redundant data

B.119 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 Consumer Data Rules or for a purpose for which the entity may use or disclose it under Division 5 of the Competition and Consumer Act.
- the entity is not required to retain the data by or under an Australian law or court/tribunal order and the data does not relate to any current or anticipated legal or dispute resolution proceedings to which the entity is a party.[57]

Required consumer data

B.120 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 Consumer Data Rule 3.4(3), or
- an accredited person in response to a consumer data request under Consumer Data Rule 4.6(4).

B.121 'Required consumer data' for the banking sector is defined in paragraph 3.2 of Schedule 3 to the Consumer Data Rules.[58]

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

Australian law

B.122 'Australian law' has the meaning given to it in the Privacy Act. It means:

- 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

[57] 56EO(2).

[58] 3.2(3) of Schedule 3 of the Consumer Data Rule sets out what CDR data will be neither required consumer data nor voluntary consumer data.

- a rule of common law or equity.[59]

Court/tribunal order

B.123 '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.[60]

B.124 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.125 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.126 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.127 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.128 A person that 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.129 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.130 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[61] 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.131 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.[62]

---

[59] Privacy Act, s 6(1).

[60] Privacy Act, s 6(1).

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

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

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

Required

B.132 A data holder is 'required' to disclose CDR data under the Consumer Data Rules:

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

B.133 An accredited data recipient is never 'required' to disclose CDR data under the Consumer Data Rules.

Authorised

B.134 A data holder may be 'authorised' to disclose CDR data to an accredited person by a CDR consumer.[63] Such an authorisation must be in accordance with Division 4.4 of the Consumer Data Rules.

B.135 A data holder is also authorised to disclose voluntary product data in response to a product data request under Consumer Data Rule 2.4(2), however the privacy safeguards do not apply to required product data.

B.136 An accredited data recipient is 'authorised' to disclose CDR data under the Consumer Data Rules:

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

Required product data

B.137 In the banking sector, 'required product data' means CDR data for which there are no CDR consumers, and which is:[64]

- within a class of information specified in the banking sector designation instrument

[63] Consumer Data Rule 4.5.

[64] 3.1(1) of Schedule 3 to the Consumer Data Rules

- 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.138 The privacy safeguards do not apply to required product data.[65]

Use

B.139 'Use' is not defined in the Competition and Consumer Act. 'Use' is a separate concept from disclosure, which is discussed at paragraphs B.101-B.104 above.

B.140 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.141 'Voluntary consumer data' is CDR data a data holder may disclose to a CDR consumer under Consumer Data Rule 3.4(2) or to an accredited person under Consumer Data Rule 4.6(2).

B.142 For the banking sector, 'voluntary consumer data' is CDR data that is not required consumer data and for which there is a CDR consumer.[66]

B.143 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,[67] but may nonetheless be CDR data (as it is data derived from a specified class of information in the relevant designation instrument).

[65] 56EB(1).

[66] 3.2(2) of Schedule 3 of the Consumer Data Rules. 3.2(3) of Schedule 3 of the Consumer Data Rule sets out what CDR data will be neither required consumer data nor voluntary consumer data.

[67] Section 10 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.

Voluntary product data

B.144 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.[68]

B.145 The privacy safeguards do not apply to voluntary product data.[69]

[68] 3.1(2) of Schedule 3 to the Consumer Data Rules

[69] 56EB(1).