Chapter B:

Key concepts

Version 3.0 June 2021

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 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**.

cont

[1] See paragraph B.9.

[2] Section 56AI(1) of the Competition and Consumer Act. The Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 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.

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

cont

[3] For the banking sector, 1 January 2017 is the 'earliest holding day' specified in the designation instrument: s 5(3) of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019. See paragraphs B.103 to B.104 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.43 for further information.

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

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]

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[10]
- holds that CDR data (or has another person hold that CDR data on their behalf), and

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

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

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

[10] 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.

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 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.

- does not hold that CDR data as a data holder or designated gateway.[11]

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.[12]

B.8 In the banking sector, an example of an accredited person could be a bank, a FinTech or other business that wishes to provide a good or service using CDR data from the banking sector. This is demonstrated by the example under paragraph B.3.

B.9 The Data Recipient Accreditor is the Australian Competition and Consumer Commission (ACCC).[13]

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

B.11 A data holder may be accredited under the CDR system, and therefore be both a data holder and an accredited person.

Authorise, Authorisation

B.12 An authorisation must meet the requirements set out in the CDR Rules, and be sought in accordance with the data standards.[14]

B.13 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.14 For the banking sector, 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.[15]

B.15 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.

---

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

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

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

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

[15] Depending on which 'disclosure option' (i.e. pre-approval or co-approval option) has been selected by the joint account holders through the joint account management service: cl 4.5 and 4.6 of Schedule 3 to the CDR Rules. See subdivision 4.3.2 of Schedule 3 to the CDR Rules, which sets out how consumer data requests to data holders that relate to joint accounts are handled in the CDR regime.

CDR data

B.16 '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.17 '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.18 '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.19 A 'CDR participant' is a data holder, or an accredited data recipient, of CDR data.[19]

CDR policy

B.20 A 'CDR policy' is a document that provides information to consumers about how CDR data is managed and how they 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.21 The CDR policy must be a separate document to an entity's privacy policy. 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.

[16] Section 56AI(1) of the Competition and Consumer Act. The Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 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 Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 (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.22 A 'CDR receipt' is a notice given by an accredited person to a CDR consumer who has provided, amended or withdrawn a consent.[20]

B.23 CDR receipts must be given in accordance with CDR Rule 4.18.

CDR regime

B.24 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.25 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.26 'Collect' is not defined in the Competition and Consumer Act or the Privacy Act.

B.27 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.28 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.29 Consent is the:

- only basis on which an accredited person may collect CDR data,[22] and
- primary basis on which an accredited data recipient of particular CDR data may use and disclose CDR data.[23]

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

[23] 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.

B.30 The CDR regime sets out specific categories of consents that an accredited person may seek from a consumer. These are set out in CDR Rule 1.10A and outlined below in paragraphs B.33-B.41.

B.31 Consent must meet the requirements set out in the CDR Rules.[24]

B.32 For further information, including the requirements which an accredited person must comply with when asking a consumer to give or amend a consent, see Chapter C (Consent).

Collection consent

B.33 A collection consent is a consent given by a consumer for an accredited person to collect particular CDR data from a data holder or accredited data recipient of that CDR data.[25]

Use consent

B.34 A use consent is a consent given by a 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.[26]

B.35 A use consent includes 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.40 below).

AP disclosure consent

B.36 An AP disclosure consent is a consent given by a consumer for an accredited data recipient of particular CDR data to disclose that CDR data to an accredited person in response to a consumer data request.[27]

Direct marketing consent

B.37 A direct marketing consent is a consent given by a consumer for an accredited data recipient of particular CDR data to use or disclose CDR data for the purposes of direct marketing.[28]

B.38 A direct marketing consent for an accredited data recipient to use CDR data for the purposes of direct marketing is a form of 'use consent'.

---

[24] 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.

[25] CDR Rules 1.10A(1)(a) and 1.10A(2)(a).

[26] CDR Rules 1.10A(1)(b) and 1.10A(2)(b).

[27] CDR Rules 1.10(1)(c)(i) and 1.10A(2)(e). CDR Rule 7.5A prohibits an accredited person from disclosing CDR data to another accredited person under an AP disclosure consent until the earlier of 1 July 2021 or the making of a relevant consumer experience data standard. In practice, there is limited utility in seeking an AP disclosure consent until disclosures under AP disclosure consents are authorised in the CDR regime.

[28] CDR Rules 1.10A(1)(d) and 1.10A(2)(c).

B.39 A direct marketing consent for an accredited data recipient to disclose CDR data to an accredited person for the purposes of direct marketing is a form of 'disclosure consent'.[29]

De-identification consent

B.40 A de-identification consent is a consent given by a consumer for an accredited data recipient of particular CDR data to de-identify some or all of that CDR data in accordance with the CDR data de-identification process[30] and:

- use the de-identified data for 'general research' (see paragraph B.126), and/or
- disclose (including by selling) the de-identified data.[31]

B.41 A de-identification consent is a form of 'use consent'.

Consumer, CDR consumer or 'eligible' CDR consumer

B.42 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 them or to an accredited person.[32]

B.43 A person is a 'CDR consumer' for CDR data if each of the following four conditions are met:[33]

- the CDR data 'relates to'[34] the person because of the supply of a good or service to the person or an associate[35] of the person[36]
- 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[37] the data on behalf of a data holder or accredited data recipient of the CDR data[38]

[29] CDR Rule 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.

[30] See CDR Rule 1.17 and Chapter 12 (Privacy Safeguard 12) for further information on the CDR data de-identification process.

[31] CDR Rules 1.10A(1)(e) and 1.10A(2)(d).

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

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

[34] See paragraphs B.51 to B.57 for the meaning of 'relates to'.

[35] See paragraphs B.58 to B.63 for the meaning of 'associate'.

[36] 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.

[37] See paragraphs B.127 to B.128 for the meaning of 'holds'.

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

- the person is identifiable, or reasonably identifiable,[39] 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),[40] and
- none of the conditions (if any) prescribed by the regulations apply to the person in relation to the CDR data.

B.44 A CDR consumer can be an individual or a business enterprise.[41]

B.45 Section 4B(1) of the Competition and Consumer Act does not apply for the purposes of determining whether a person is a 'CDR consumer'.[42] This section explains when a person is taken to have acquired particular goods or services as a consumer, outside of the CDR regime.

B.46 These guidelines use the term 'consumer' to refer to 'CDR consumer'.

Reasonably identifiable

B.47 As outlined in paragraph B.43, 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).[43]

B.48 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.127 to B.128 for a discussion on the meaning of 'held'), and
- whether it is practicable to use that information to identify the person.

B.49 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.50 See B.138 to B.141 for a discussion on the meaning of 'reasonably'.

---

[39] See paragraphs B.47 to B.50 for the meaning of 'reasonably identifiable'.

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

[41] Section 56AI(3) of the Competition and Consumer Act; Explanatory Memorandum, Treasury Laws Amendment (Consumer Data Right) Bill 2019, paragraphs 1.100 and 1.101. See also s 2C of the *Acts Interpretation Act 1901* (Cth), which provides that in any Act (including the references to 'person' in s 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.

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

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

Relates to

B.51 As outlined in paragraph B.43, for a person to be a 'CDR consumer' the CDR data must 'relate to' that person.[44]

B.52 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.[45] The relevant context in the CDR regime is the Competition and Consumer Act and the Privacy Act.

B.53 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.[46]

B.54 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.55 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.58 to B.63 below).

B.56 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.[47]

B.57 By using the broad phrase 'relates to', the CDR regime captures meta-data.[48]

Associate

B.58 As outlined in paragraph B.43, 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'.[49]

B.59 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.[50]

---

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

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

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

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

[48] 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.

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

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

B.60 In this context, 'associate' has the same meaning as in the *Income Tax Assessment Act 1936* (ITA Act).[51] Section 318 of the ITA Act defines 'associates' with respect to natural persons, companies, trustees and partnerships.[52]

B.61 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.62 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.63 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.64 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.65 A consumer for the banking sector is 'eligible' if, at that time:[53]

- for any consumer – the consumer is an account holder or a secondary user[54] for an account with the data holder that is open and set up in such a way that it can be accessed online by that consumer
- for a consumer that is an individual – the consumer is 18 years or older, and

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

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

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

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

Any provisions in the CDR Rules which impose obligations on data holders in relation to secondary users only apply to initial data holders in respect of NAB, CBA, ANZ, Westpac branded products on and from 1 November 2021 (and for all other data holders, on and from 1 November 2022): see cl 6.7 of Schedule 3 to the CDR Rules.

- for a consumer that is a partner in a partnership for which there is partnership account[55] with the data holder – the partnership account is open and set up in such a way that it can be accessed online.[56]

B.66 For guidance regarding 'consumers' and 'CDR consumers', see paragraphs B.42 to B.46.

Consumer dashboard, or dashboard

B.67 Each accredited person and each data holder must provide a 'consumer dashboard' for CDR consumers.

B.68 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 they have given to the accredited person (for example, to withdraw such consents).
- The service must also provide the consumer with certain details of each consent.

B.69 The requirements for an accredited person's consumer dashboard are set out in CDR Rule 1.14. For more information, see Chapter C (Consent).

B.70 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 consumer of information related to CDR data disclosed pursuant to an authorisation.

B.71 The requirements for a data holder's consumer dashboard are set out in CDR Rule 1.15. For more information, see the Guide to privacy for data holders.

B.72 These guidelines use the term 'dashboard' and 'consumer dashboard' interchangeably.

Consumer data request

B.73 A 'consumer data request' is either:

- a request made directly by a CDR consumer to a data holder,[57] or
- a request made by an accredited person to a data holder[58] or accredited data recipient[59] 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.

---

[55] 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 Rule 1.7.

[56] Any provisions in the CDR Rules which impose obligations on data holders in relation to partnerships only apply to initial data holders in respect of NAB, CBA, ANZ, Westpac branded products on and from 1 November 2021 (and for all other data holders, on and from 1 November 2022): see cl 6.7 of Schedule 3 to the CDR Rules.

[57] CDR Rule 3.3. For the banking sector, a data holder's obligations under Part 3 of the CDR Rules (regarding consumer data requests made by consumers) do not commence until 1 November 2021: clause 6.6 of Schedule 3 to the CDR Rules.

[58] CDR Rule 4.4.

[59] CDR Rule 4.7A.

B.74 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.[60]

B.75 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 consumer to collect and use.[61]

B.76 A request from an accredited person to a data holder or accredited data recipient must comply with the data minimisation principle.[62]

B.77 Refer to Chapter 3 (Privacy Safeguard 3) and Chapter C (Consent) for further information.

Direct request service

B.78 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.[63]

B.79 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.80 This service must conform with the data standards.

Accredited person request service

B.81 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.[64]

B.82 It also allows accredited persons to receive requested data in machine-readable form.

B.83 This service must conform with the data standards.

Valid request

B.84 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).

B.85 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.[65]

B.86 An 'eligible' consumer for the banking sector is discussed above at paragraphs B.64 to B.66.

---

[60] CDR Rule 3.3(1). For the banking sector, a data holder's obligations under Part 3 of the CDR Rules (regarding consumer data requests made by consumers) do not commence until 1 November 2021: clause 6.6 of Schedule 3 to the CDR Rules.

[61] CDR Rule 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.

[62] CDR Rules 4.4(1) and 4.7A(1).

[63] CDR Rule 1.13(2). For the banking sector, a data holder's obligations under Part 3 of the CDR Rules (regarding consumer data requests made by consumers) do not commence until 1 November 2021: clause 6.6 of Schedule 3 to the CDR Rules.

[64] CDR Rule 1.13(3).

[65] CDR Rule 3.3(3). For the banking sector, a data holder's obligations under Part 3 of the CDR Rules (regarding consumer data requests made by consumers) do not commence until 1 November 2021: clause 6.6 of Schedule 3 to the CDR Rules.

B.87 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 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
- 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).[66]

B.88 Refer to Chapter 3 (Privacy Safeguard 3) for further information regarding valid requests, and Chapter C (Consent) for information regarding collection and use consents.

CDR Rules

B.89 The consumer data rules (CDR Rules) refer to the *Competition and Consumer (Consumer Data Right) Rules 2020*.

B.90 The Minister has the power to make rules to determine how the CDR functions in each sector.[67] CDR Rules may be made on aspects of the CDR regime (as provided in Part IVD the Competition and Consumer Act) including the privacy safeguards,[68] 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.[69]

Current

Current consent

B.91 A consent is 'current' if it has not expired under CDR Rule 4.14.[70]

B.92 CDR Rule 4.14 provides that a consent expires:

- if it is withdrawn
- at the end of the period of consent
- once 12 months has 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
- for a collection consent, when the accredited person is notified by the accredited data recipient of the expiry of the AP disclosure consent

[66] CDR Rule 4.3.

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

[68] Part IVD, Division V of the Competition and Consumer Act.

[69] Section 56BB of the Competition and Consumer Act.

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

- for an AP disclosure consent, when the accredited data recipient is notified by the accredited person of the expiry of the collection consent
- if the accredited person's accreditation is revoked or surrendered, when this revocation or surrender takes effect
- 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), or
- if another CDR Rule provides that consent expires.

B.93 For further information on when a consent expires, see Chapter C (Consent).

Current authorisation

B.94 Authorisation to disclose particular CDR data to an accredited person is 'current' if it has not expired under CDR Rule 4.26.[71]

B.95 CDR Rule 4.26 provides that authorisation expires:

- if it is withdrawn
- if the 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 has 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.

B.96 For further information on when an authorisation expires, see the Guide to privacy for data holders.

Consumer Experience Guidelines

B.97 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 regime.

B.98 The Consumer Experience Guidelines are made by the Data Standards Body and cover matters including:

[71] CDR Rule 1.7.

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

B.100 The Consumer Experience Guidelines are available on the Data Standards Body website, consumerdatastandards.gov.au.

Data holder

B.101 A person is a data holder of CDR data if:[72]

- the CDR data falls within a class of information specified in the designation instrument for the relevant sector[73]
- the CDR data is held by (or on behalf of) the person on or after the earliest holding day[74]
- 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),[75] and is not about the provision of a product or service by (or on behalf of) the person before the earliest holding day[76] (e.g. a transaction on an account)[77]
- 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

[72] Section 56AJ of the Competition and Consumer Act.

[73] For the banking sector, the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 sets out matters including the classes of information that are subject to the CDR regime. The designation instrument for the banking sector is available here. See also s 56AC(2)(a) of the Competition and Consumer Act.

[74] Being the earliest holding date specified in the designation instrument for the relevant sector. 1 January 2017 is the 'earliest holding day' specified in the designation instrument for the banking sector: s 5(3) of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.

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

[76] 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
- will 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.101 are met by the entity): see Note 2 to s 56AJ of the Competition and Consumer Act.

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

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.[78]

- **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.[79]
- **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.[80]

B.102 For further information on the privacy obligations for data holder, see the Guide to privacy for data holders.

Earliest holding day

B.103 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.[81]

B.104 Under the designation instrument for the banking sector, the earliest holding day is 1 January 2017.[82]

Data minimisation principle

B.105 The data minimisation principle limits the scope and amount of CDR data an accredited person may collect and use.

B.106 An accredited person collects and uses CDR data in compliance with the data minimisation principle if:[83]

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
   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

[78] 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 1.10.

[79] 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 Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019only 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.

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

[81] Section 56AC(2)(c) of the Competition and Consumer Act.

[82] Section 5(3) of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.

[83] CDR Rule 1.8.

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 or to fulfill any other purpose consented to by the consumer.

Data standards

B.107 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.108 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.[84]

B.109 The current data standards are available on Consumer Data Standards website, consumerdatastandards.gov.au and include the following:

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

Consumer Experience Standards

B.110 The 'Consumer Experience Standards' are data standards[85] 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.111 The Consumer Experience Standards are available on Consumer Data Standards website, consumerdatastandards.gov.au.

[84] Section 56FA of the Competition and Consumer Act and CDR Rule 8.11.

[85] Section 56FA of the Competition and Consumer Act and CDR Rule 8.11.

Data Language Standards

B.112 The 'Data Language Standards' are data standards[86] regarding the types of CDR data and descriptions of those types to be used by CDR participants in making and responding to requests.

B.113 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.114 A 'designated gateway' is a person specified as a gateway in a legislative instrument made under s 56AC(2) of the Competition and Consumer Act.[87]

B.115 There is no designated gateway for the banking sector.

Designation instrument

B.116 A 'designation instrument' is a legislative instrument made by the Minister under section 56AC(2) of the Competition and Consumer Act.

B.117 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.118 The designation instrument for the banking sector is the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019, dated 4 September 2019.

Disclosure

B.119 'Disclosure' is not defined in the Competition and Consumer Act or the Privacy Act.

B.120 Under the CDR regime 'disclose' takes its ordinary, broad meaning.

B.121 An entity discloses CDR data when it makes the data accessible or visible to others outside the entity.[88] 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.[89]

B.122 For example, an entity discloses CDR data when it transfers a copy of the data in machine-readable form to another entity.

---

[86] Section 56FA of the Competition and Consumer Act and CDR Rule 8.11.

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

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

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

B.123 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.172 to B.173 for the limited circumstances where it will be a 'use').

B.124 '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.170 to B.173 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.125 'Eligible' CDR consumers are discussed at paragraphs B.64–B.66.

General research

B.126 '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.[90]

Holds

B.127 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)[91] that contains the information.[92] This definition is comparable to the definition of 'holds' in the Privacy Act.[93]

B.128 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 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)

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

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

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

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

- 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.

Outsourced service provider

B.129 The CDR Rules provide that an 'outsourced service provider' is a person:

- who is accredited and collects CDR data from a CDR participant on behalf of an accredited person under a CDR outsourcing arrangement, and/or
- to whom an accredited person discloses CDR data under a CDR outsourcing arrangement for the purpose of the provider providing goods or services to the accredited person.[94]

B.130 For the meaning of 'collects', refer to B.26 to B.28 above.

B.131 For the meaning of 'discloses', refer to B.119 to B.124 above.

CDR outsourcing arrangement

B.132 A CDR outsourcing arrangement is a written contract between an accredited person (the 'principal') and an outsourced service provider (the 'provider'). Under this arrangement a provider will collect CDR data on behalf of the principal (if the provider is an accredited person) and/or provide goods or services to the principal using CDR data disclosed to it by the principal.[95]

B.133 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 contract
- 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
- if directed by the principal:
  - provide access to any service data that it holds
  - 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, and

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

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

- where the provider is to collect CDR data on the principal's behalf, not further outsource that collection.

B.134 For information on the meaning of 'service data' in relation to a CDR outsourcing arrangement, see B.169 below.

Purpose

B.135 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.[96]

B.136 The purpose of an act is the reason or object for which it is done.

B.137 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.[97] 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.138 '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.[98]

B.139 '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.140 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.[99]

B.141 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',[100] and 'involves an evaluation of the known facts, circumstances and considerations which may bear

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

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

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

[99] 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).

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

rationally upon the issue in question'.[101] 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.142 References to 'reasonable steps' are used in the privacy safeguards and CDR Rules. An example is in 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.[102]

B.143 The 'reasonable steps' test is an objective test and is to be applied in the same manner as 'reasonable' and 'reasonably'.

B.144 An entity must be able to justify that reasonable steps were taken.

Redundant data

B.145 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.[103]

B.146 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.147 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.148 'Required consumer data' for the banking sector is defined in clause 3.2 of Schedule 3 to the CDR Rules.[104]

---

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

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

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

[104] 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.

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

B.149 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.[105]

Australian law

B.150 '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
- a rule of common law or equity.[106]

Court/tribunal order

B.151 '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.[107]

B.152 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.153 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.154 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.155 The obligation will usually be indicated by words such as 'must' or 'shall' and may be accompanied by a sanction for non-compliance.

---

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

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

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

Authorised

B.156 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.157 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.158 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[108] 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.159 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.[109]

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

B.160 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.[110]

B.161 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.[111]

Required

B.162 A data holder is 'required' to disclose required consumer data[112] under the CDR Rules:

- in response to a valid consumer data request under CDR Rule 3.4(3), subject to CDR Rule 3.5, and

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

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

[110] Section 56EP(1)(c) of the Competition and Consumer Act. See Chapter 13 (Privacy Safeguard 13) for further information.

[111] Section 56EI(1)(b) of the Competition and Consumer Act. See Chapter 6 (Privacy Safeguard 6) for further information.

[112] See paragraphs B.147 to B.148 for further information about 'required consumer data'.

- 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 Rules 4.6A and 4.7, where the data holder has a current authorisation to disclose the data from the CDR consumer.

B.163 An accredited data recipient is never 'required' to use or disclose CDR data under the CDR Rules.

Authorised

B.164 A data holder may be 'authorised' to disclose a consumer's CDR data to an accredited person by the relevant CDR consumer.[113] Such an authorisation must be in accordance with Division 4.4 of the CDR Rules.

B.165 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.166 In the banking sector, 'required product data' means CDR data for which there are no CDR consumers, and which is:[114]

- 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.167 The privacy safeguards do not apply to required product data.[115]

Service data

B.168 'Service data' 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.[116]

B.169 For guidance regarding 'outsourced service providers' and 'CDR outsourcing arrangements', see B.129 to B.134.

[113] CDR Rule 4.5.

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

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

[116] CDR Rule 1.10(4).

Use

B.170 '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.119 to B.124 above.

B.171 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.172 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.119 to B.124). 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 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.173 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.132 to B.134).

Voluntary consumer data

B.174 '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.175 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.[117]

B.176 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

[117] 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.

instrument for the banking sector,[118] 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.177 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.[119]

B.178 The privacy safeguards do not apply to voluntary product data.[120]

[118] Section 10 of the Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019 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.

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

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