Chapter C:

Consent —

The basis for collecting, using and disclosing CDR data

Version 3.0, June 2021

OAIC

Contents

Key points

- An accredited person may only collect, use and disclose consumer data right (CDR) data with the consent of the consumer.
- The CDR regime sets out specific categories of consents that an accredited person may seek from a consumer. It further prohibits an accredited person from seeking a consent which does not fit into these categories.
- An accredited person must ask a consumer to give or amend a consent in accordance with the consumer data rules (CDR Rules), which seek to ensure that a consumer's consent is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.
- An accredited person's processes for asking a consumer to give or amend a consent must be compliant with the data standards (subject to the exceptions in CDR Rule 4.10(2)), and have regard to the Consumer Experience Guidelines.
- An accredited person must comply with the data minimisation principle when collecting or using CDR data.
- A data holder may disclose CDR data only with the authorisation of the relevant CDR consumers.

Why is it important?

C.1 The CDR regime places the value and control of consumer data in the hands of the consumer. This is achieved by requiring the consumer's consent for the collection, use and disclosure of their CDR data.

C.2 Consumer consent is the bedrock of the CDR regime. Consent enables consumers to be the decision makers in the CDR regime, ensuring that they can direct where their data goes in order to obtain the most value from it.

How is consent in the CDR regime different to the Privacy Act?

C.3 It is important to understand how consent in the CDR regime differs from consent under the *Privacy Act 1988* (the Privacy Act).

C.4 The CDR regime requires express consent from consumers for the collection, use and disclosure of their CDR data by accredited persons.[1] Consent must meet the requirements set out in the CDR Rules. A consumer can only give consent for a maximum period of 12

[1] Consent is the only basis on which an accredited person may collect CDR data. See Chapter 3 (Privacy Safeguard 3) for information on seeking to collect of CDR data.

Consent is the primary basis on which an accredited data recipient of CDR data may use and disclose that data. For example, under Privacy Safeguard 6 an accredited data recipient may use or disclose CDR data where in accordance with the Rules (which requires consent), unless a use or disclosure is required or authorised by law: s 56EI(1)(c). For information regarding use or disclosure of CDR data, see Chapter 6 (Privacy Safeguard 6), Chapter 7 (Privacy Safeguard 7), Chapter 8 (Privacy Safeguard 8) and Chapter 9 (Privacy Safeguard 9).

months. Without express consent, the accredited person is not able to collect, use, or disclose CDR data.[2]

C.5 However, under the Privacy Act, consent is not the primary basis upon which an entity may collect, use or disclose personal information.[3] In addition, where consent is involved, the consent can be either express or implied.[4]

C.6 The CDR Rules contain specific requirements for the accredited person's processes for seeking consent in the CDR regime, as well as for information that must be presented to a consumer when they are being asked to consent.

C.7 The requirements by which an accredited person must seek consent from a consumer are discussed in this Chapter.

How does consent fit into the CDR regime?

C.8 Consent is the primary basis on which an accredited person may collect, use and disclose CDR data for which there are one or more consumers.[5]

C.9 Where an accredited person:

- offers a good or service through the CDR regime, and
- needs to collect a consumer's CDR data from a data holder or accredited data recipient ('CDR participant') in order to use it to provide such goods or services,

the accredited person may ask for the consumer's consent to the collection and use of their CDR data to provide the good or service.[6]

C.10 In giving the above consents, the CDR consumer provides the accredited person with a 'valid request' to seek to collect the relevant CDR data.[7] An accredited person can only collect and use the CDR data if it has obtained these consents.

C.11 Upon obtaining a 'valid request' from the consumer, the accredited person may seek to collect the consumer's CDR data from the relevant CDR participant of the CDR data. The accredited person collects this CDR data by making a 'consumer data request' to the relevant CDR participant/s.[8]

---

[2] Consent is the only basis on which an accredited person may collect CDR data, and the primary basis on which an accredited data recipient of CDR data may use and disclose that data. For further information, see footnote 1 above.

[3] For example, an APP entity can collect personal information (other than sensitive information) if the information is reasonably necessary for one or more of the entity's functions or activities. See Chapter 3: APP 3 — Collection of solicited personal information of the APP Guidelines and Chapter B: Key concepts of the APP Guidelines.

[4] See section 6(1) of the Privacy Act and Chapter B: Key concepts of the APP Guidelines.

[5] An accredited person may make a product data request without the involvement of a consumer, for instance. In addition, while consent is the only basis on which an accredited person may collect CDR data, consent is a primary basis on which an accredited person may use and disclose CDR data. See Chapter 6 (Privacy Safeguard 6), Chapter 7 (Privacy Safeguard 7), Chapter 8 (Privacy Safeguard 8) and Chapter 9 (Privacy Safeguard 9) for further information regarding use and disclosure of CDR data.

[6] CDR Rule 4.3.

[7] CDR Rule 4.3(3).

[8] CDR Rules 4.4 and 4.7A. For information regarding 'valid requests' and 'consumer data requests', see Chapter 3 (Privacy Safeguard 3). See also the flow chart underneath paragraph C.15 which demonstrates the points at which a valid request is given by the consumer and consumer data request is made on behalf of the consumer by the accredited person.

C.12 Privacy Safeguard 3 prohibits an accredited person from seeking to collect data under the CDR regime unless it is in response to a 'valid request' from the consumer.

C.13 Consent also underpins how an accredited person may use or disclose CDR data under Privacy Safeguard 6 and Privacy Safeguard 7.

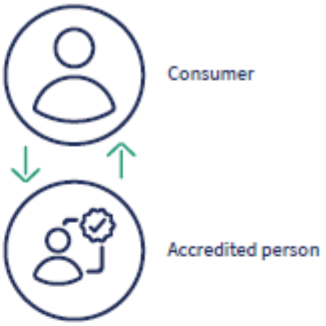
C.14 The flow chart below paragraph C.105 demonstrates how consent fits in the key information flow between a consumer, accredited person and data holder.

C.15 The flow chart following demonstrates the points at which a valid request is given by the consumer and a consumer data request is made on behalf of the consumer by the accredited person.

Consent and collection process for accredited persons

Obtaining consumer consent for the collection and use of CDR data

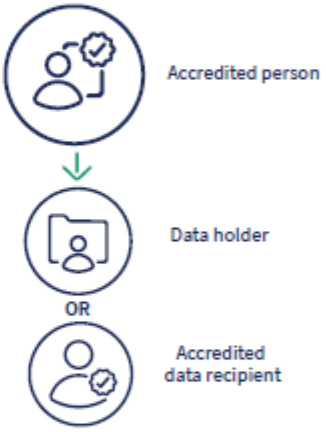
- Accredited person offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- Accredited person asks the consumer to consent to the collection and use of their CDR data for this purpose, for up to 12 months
- Consumer provides their express consent to the collection and use of their CDR data



The consumer has given the accredited person a valid request ✓

Making a consumer data request on behalf of the consumer

- Consumer gives accredited person a valid request
- Accredited person asks the CDR participant [1] to disclose the consumer's CDR data
- Where the request is to a data holder, the accredited person makes the request using the data holder's 'accredited person request service', and in accordance with the data standards [2]



CDR participant sends the consumer's CDR data to the accredited person after obtaining:

- the consumer's authorisation (in the case of a data holder)
- the consumer's AP disclosure consent (in the case of an accredited data recipient)

The accredited person becomes an accredited data recipient for the consumer's CDR data.

[1] This may be a data holder or accredited data recipient

[2] Note: there are no equivalent requirements for how an accredited person must make a request to another accredited data recipient

What are the different categories of consents in the CDR regime?

C.16 The CDR regime requires an accredited person to obtain different categories of consents from a consumer depending on what data-handling activity they propose to undertake.

C.17 The categories of consents that may be given by a consumer to an accredited person in the CDR regime are as follows:[9]

- **Collection consent** – a consent for an accredited person to collect particular CDR data from a data holder or accredited data recipient of that CDR data.[10]
- **Use consent** – a consent 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.[11] 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 below).
- **AP disclosure consent** – a consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person in response to a consumer data request.[12]
- **Direct marketing consent** – a consent for an accredited data recipient of particular CDR data to use or disclose that CDR data for the purposes of direct marketing.[13]
  - 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'.
  - A direct marketing consent for an accredited data recipient to disclose CDR data to another accredited person for the purposes of direct marketing is a form of 'disclosure consent'.[14]

---

[9] Note: Each category of consent (except a 'collection consent') refers to an 'accredited data recipient of particular CDR data', rather than an 'accredited person'. This is because, while the entity will be an 'accredited person' when seeking this category of consents, the entity would become an 'accredited data recipient of particular CDR data' in relation to that consumer upon collecting the relevant CDR data.

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

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

[12] CDR Rules 1.10(1)(c)(i) and 1.10A(2)(e). CDR Rule 7.5A prohibits an accredited data recipient 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.

Currently the CDR regime only requires a consumer's consent for disclosures to accredited persons. Consent is not required for disclosures to outsourced service providers, however before doing so an accredited person must comply with other requirements in the CDR Rules. See Chapter 6 (Privacy Safeguard 6), Chapter 7 (Privacy Safeguard 7) and 'outsourced service provider' in Chapter B (Key Concepts).

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

[14] 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.

- **De-identification consent** – a form of 'use consent' 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[15] and:
  - use the de-identified data for general research,[16] and/or
  - disclose (including by selling) the de-identified data.

C.18 An accredited person is prohibited from seeking a consent that is not in the list above.[17]

C.19 Each category of consent operates independently of each other. This means that an accredited person can ask for more than one category of consent, and that a consumer must be enabled by an accredited person to independently manage each category of consent.[18] For example, an accredited person may ask a consumer for a collection consent and use consent, and the consumer can (in future) choose to withdraw only the collection consent, if they wish.[19]

C.20 The requirements that an accredited person must comply with when asking for a consent are contained in Division 4.3 of the CDR Rules. The specific requirements differ depending on which category of consent is being sought.

C.21 The categories of consent are based off the 'types' of consents set out in the CDR Rules.[20]

How must consent be sought?

C.22 An accredited person must ask the consumer to give consent in accordance with Division 4.3 of the CDR Rules. Division 4.3 sets out the specific requirements for each consent outlined in the section above.[21]

C.23 The requirements in Division 4.3 are outlined below under 'Requirements for asking a consumer to give or amend a consent', 'Restrictions on seeking consents' and 'How consents must be managed'.

---

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

[16] '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.

[17] CDR Rule 4.12(3)(a).

[18] See the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [7].

[19] For example, where the consumer wishes to allow the accredited data recipient to keep using their CDR data so they may continue to receive the relevant good or service. Where a consumer withdraws both their collection consent and use consent, it is likely the CDR data would become redundant data that must be deleted or de-identified under Privacy Safeguard 12, unless an exception applies. For further information, see paragraphs C .81 to C.89 'Effect of withdrawing consent'.

[20] The 'categories' of consent are listed at CDR Rule 1.10A(2) and defined by reference to the 'types' of consents listed at CDR Rule 1.10A(1).

[21] Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 13, which provides that an accredited person must ask for consent in accordance with Division 4.3 of the CDR Rules which now encompass provisions relating to all types and categories of consent. See also CDR Rule 4.3(2).

C.24 The CDR Rules state that the objective of Division 4.3 is to ensure that consent given by a consumer is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.[22]

C.25 In obtaining consent from a consumer, an accredited person must comply with requirements relating to:

- an accredited person's processes for asking for consent[23]
- information to be presented to the consumer when asking for consent,[24] and
- restrictions on seeking consent.[25]

C.26 Where a consumer is not an individual and wishes to use the accredited person's good or service through the CDR regime, the accredited person should ensure the consent is given by a person who is duly authorised to provide the consent on the entity's behalf.[26]

Can consents be amended?

C.27 An accredited person will be allowed to invite a consumer to amend their existing consent on and from 1 July 2021.[27] This includes allowing a consumer to change:

- the types of CDR data that can be collected and/or disclosed
- what the CDR data can be used for
- what accounts or data holders CDR data is to be collected from, and/or
- the duration of the consent.[28]

C.28 An invitation to amend a consent may be issued only where the amendment would:[29]

- better enable the accredited person to provide the goods or service requested by the consumer under the existing consent,[30] or
- be consequential to an agreement between the accredited person and consumer to modify those goods or services, and enable the accredited person to provide the modified goods or services.

---

[22] CDR Rule 4.9. The Explanatory Statement to the CDR Rules, together with the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, provides that the CDR Rules are intended to ensure that all consents sought in the CDR regime are transparent and that consumers understand the potential consequences of what they are consenting to.

[23] CDR Rule 4.10.

[24] CDR Rule 4.11.

[25] CDR Rule 4.12.

[26] A person is entitled, under section 128 of the *Corporations Act 2001*, to make the assumptions set out in section 129 of that Act when dealing with corporations, including that persons held out by the company as directors, officers and agents are duly appointed and have authority to exercise customary powers.

[27] CDR Rule 4.12B(5). See generally Subdivision 4.3.2A of the CDR Rules.

[28] See the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [6].

[29] CDR Rule 4.12B(3).

[30] That is, the goods or services requested by the consumer as part of their valid request in CDR Rule 4.3(1)(a).

C.29 An invitation to amend an existing consent may be given via the consumer dashboard (if applicable)[31] or in writing to the consumer.[32] An invitation can only be given where the consent is current (i.e. has not expired).[33]

C.30 Where an accredited person wishes to invite a consumer to amend the duration of their consent, the invitation must not be given:

- any earlier than a reasonable period before the existing consent expires, and
- more than a reasonable number of times within this period.[34]

Example: A consumer has given a consent to an accredited data recipient in relation to CDR data for a period of three months. In the three weeks prior to expiry, the accredited person invites the consumer on two occasions to extend the duration of their existing consent. The accredited data recipient has decided, based on their circumstances, that they have provided the invitation within a reasonable period before the existing consent expires, and a reasonable number of times within that period.[35]

C.31 Where the accredited person wishes to invite a consumer to extend the duration of their consent, they should first consider whether the invitation would constitute an offer to renew existing goods or services under CDR Rule 7.5(3)(a)(ii) (in which case a direct marketing consent would be required).[36]

C.32 An accredited person cannot ask a consumer to extend the duration of an existing consent for longer than 12 months.[37]

C.33 An accredited person must ask the consumer to give any amendments to their existing consent in the same manner that they asked the consumer to provide the existing consent (i.e. in accordance with Division 4.3 of the CDR Rules).[38] There are some exceptions, as outlined in the following section.[39]

C.34 Where a consumer amends their collection consent, the accredited person must notify the relevant CDR participant/s that the consent has been amended:[40]

---

[31] It is optional for accredited persons to offer a consent amendment functionality in the consumer dashboard: see CDR Rules 4.12B(2)(a) and 1.14(2A).

[32] CDR Rule 4.12B(2).

[33] CDR Rule 4.12B(3). See paragraphs C.90 to C.96 and CDR Rule 4.14 for information on when consent expires.

[34] CDR Rule 4.12B(4).

[35] Example adapted from the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 15.

[36] Sending the consumer an offer to renew existing goods or services when they expire is direct marketing, and is only permitted if the accredited person has obtained a direct marketing consent from the consumer to send them information for these purposes. See s 56EJ(1) of the Competition and Consumer Act and CDR Rule 7.5(3)(a)(ii). For further information on this requirement, see Chapter 7 (Privacy Safeguard 7).

[37] This is as a result of CDR Rule 4.12(1), which provides that the duration of a consent cannot exceed 12 months.

[38] CDR Rule 4.12(C)(1).

[39] The exceptions are contained in CDR Rule 4.12(C)(2) and allow certain details of the existing consent to be presented as pre-selected options (namely, the details covered by CDR Rules 4.11(1)(a), (b) and (ba)). They also require additional information to be presented to the consumer to explain: the consequences of amending consent; and that the accredited person would be able to continue to use CDR data already disclosed to it to the extent allowed by the amended consent.

[40] CDR Rule 4.18C.

- where the CDR data is being collected from a data holder, in accordance with the data standards, and/or
- where the CDR data is being collected from an accredited data recipient, as soon as practicable. This notice should contain sufficient detail to enable the accredited data recipient to understand the types of CDR data to which the amended collection consent now applies.

C.35 An accredited person must also provide a consumer with certain notifications upon the amendment of a consent. These are outlined under 'Notification requirements' in paragraph C.97 of this Chapter.

C.36 An amendment of a consent takes effect when the consumer amends the consent.[41]

Requirements for asking a consumer to give or amend a consent

General processes

C.37 An accredited person's processes for asking a consumer to give or amend a consent must:

- accord with any consumer experience data standards[42]
- for all consents, accord with any other data standards[43] (except in the case of a consent to collect CDR data from an accredited data recipient, or a disclosure consent),[44] and
- be as easy to understand as practicable, including by using concise language and, where appropriate, visual aids.[45]

C.38 In ensuring processes are easy to understand, an accredited person must also have regard to the Consumer Experience Guidelines.[46]

C.39 An accredited person must not:

- include or refer to the accredited person's CDR policy or other documents in a way that would reduce consumer comprehension when seeking consent, or

[41] CDR Rule 4.12A. As per the note to this Rule, it is not possible for the consumer to specify a different date or time.

[42] CDR Rule 4.10. The consumer experience standards are data standards regarding the obtaining and withdrawal of consents, the collection and use of CDR data, and the types of CDR data and description of those types to be used by CDR participants when making requests. Further information is available in Chapter B (Key concepts).

[43] 'CDR Rule 4.10(2) does not affect the application of other data standards in relation to any other processes for which an accredited person is responsible (for example data standards that may apply to encryption of data in transit in accordance with Schedule 2, Part 2 of the CDR Rules.)': Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 15. Other data standards include the API standards and information security standards, and are discussed in Chapter B (Key concepts).

[44] CDR Rule 4.10(2).

[45] CDR Rule 4.10.

[46] CDR Rule 4.10. The 'Consumer Experience Guidelines' provide best practice interpretations of several CDR Rules relating to consent and are discussed in Chapter B (Key concepts).

- bundle consents with other directions, agreements, consents or permissions.[47] This practice has the potential to undermine the voluntary nature of the consent.

C.40 However, an accredited person may refer to its CDR policy when seeking consent, so long as doing so would not be likely to reduce consumer comprehension.[48]

C.41 Each time an accredited person seeks a consumer's consent, they must allow the consumer to actively select or clearly indicate:

- for collection and disclosure consents,[49] the particular types of CDR data to which the consent will apply [50]
- for all consents, whether the data will be:
  - collected and, if applicable, disclosed on a single occasion and used over a specified period of time (not exceeding 12 months), or
  - collected and, if applicable, disclosed on an ongoing basis and used over a specified period of time (not exceeding 12 months).[51]
- for a use consent,[52] the specific uses of that CDR data,[53] and
- for a disclosure consent,[54] the accredited person to whom the CDR data may be disclosed.[55]

C.42 Each time an accredited person seeks a consumer's consent, they must also:

- ask for the consumer's express consent for the selections in paragraph C.41 above,[56] and

[47] CDR Rule 4.10. Bundled consent refers to the 'bundling' together of multiple requests for consumer's consent to a wide range of collections, uses and/or disclosures of CDR data, without giving the consumer the opportunity to choose which collections, uses or disclosures they agree to and which they do not.

[48] Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 14. Indeed, accredited persons are required to provide links to their CDR policy at certain points in the consent-seeking process, for example when providing information about outsourced service providers (CDR Rule 4.11(3)(f)(i) and (ii)) and general research (CDR Rule 4.15(c)).

[49] Including both an AP disclosure consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person for the purposes of direct marketing: CDR Rule 1.10A(1)(c)(ii).

[50] CDR Rules 4.11(1)(a)(i), 4.11(1)(c) and 4.11(2).

[51] CDR Rules 4.11(1)(b), 4.11(1)(c), 4.11(2) and 4.12(1).

[52] Including a de-identification consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rule 1.10A).

[53] CDR Rules 4.11(1)(a)(ii), 4.11(1)(c) and 4.11(2).

[54] Including both an AP disclosure consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person for the purposes of direct marketing: CDR Rule 1.10A(1)(c)(ii).

[55] CDR Rules 4.11(1)(ba) and 4.11(2).

[56] CDR Rule 4.11(1)(c).

- not pre-select these options,[57] except where the accredited person is asking the consumer to amend an existing consent.[58] In this situation, the accredited person may pre-select the above options to reflect what the consumer has selected in the past.[59]

C.43 An accredited person must not ask a consumer to give a disclosure consent[60] unless the consumer has already given their consent for the relevant CDR data to be collected and used.[61] This means that an accredited person may:

- ask a consumer to give a collection consent and use consent, and subsequently ask for a disclosure consent, or
- ask a consumer to give a consent to collect, use and disclose at the same time.[62]

Fees for disclosure

C.44 An accredited person may charge the consumer a fee for the disclosure of CDR data, or pass on to the consumer a fee charged by the data holder for the disclosure of CDR data.[63] This must be made clear to the consumer

C.45 To do this, the accredited person must:

- clearly distinguish between the CDR data for which a fee will, and will not, be charged or passed on[64]
- inform the consumer of the amount of the fee, and the consequences if the consumer does not consent to the collection or disclosure, as appropriate, of the CDR data for which a fee will be charged or passed on,[65] and
- allow the consumer to actively select or otherwise clearly indicate whether they consent to the collection or disclosure, as appropriate, of the CDR data for which a fee will be charged or passed on.[66]

[57] CDR Rule 4.11(2).

[58] CDR Rule 4.12C(2)(a).

[59] For example, where this would assist the consumer to make an informed decision as to how they would like to amend their consent.

[60] Including both an AP disclosure consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person for the purposes of direct marketing: CDR Rule 1.10A(1)(c)(ii).

[61] CDR Rule 4.11(1A).

[62] See the note to CDR Rule 4.11(1A) which clarifies that this Rule does not prevent the accredited person from asking for a disclosure consent in relation to CDR data that has yet to be collected.

[63] For example, where the consumer's request covers voluntary consumer data, the data holder may decide to charge the accredited person a fee. For information regarding 'required consumer data' and 'voluntary consumer data', see Chapter B (Key concepts).

[64] CDR Rule 4.11(1)(d).

[65] CDR Rule 4.11(3)(d).

[66] CDR Rule 4.11(1)(d).

Name and accreditation number

C.46 The accredited person must ensure that their name is clearly displayed in the consent request.[67]

C.47 The accredited person's accreditation number must also be included in the consent request.[68] This number has been assigned to the accredited person by the Data Recipient Accreditor.

C.48 For more information on the Data Recipient Accreditor and the accreditation process and conditions, see the ACCC's Accreditation Guidelines.

Data minimisation principle

C.49 Collection and use of CDR data is limited by the data minimisation principle,[69] which provides that an accredited person:

- must not collect more data than is reasonably needed in order to provide the requested goods or services, including over a longer time period than is reasonably required, and
- may use the collected data only in accordance with the consent provided, and only as reasonably needed in order to provide the requested goods or services or to fulfil any other purpose consented to by the consumer.[70]

Example: An accredited person is responding to a 'valid request' from a consumer to collect their CDR data from their data holder in relation to the consumer's eligibility to open a bank account. The accredited person asks the consumer to consent to the collection of their transaction data. However, transaction data has no bearing on the applicant's eligibility for the delivery of the service. The accredited person would therefore likely be in breach of the data minimisation principle.

C.50 Where an accredited person is seeking a collection consent or use consent,[71] the accredited person must explain how their collection and use is in line with the data minimisation principle.[72]

C.51 For a collection consent, this explanation must include an outline of why the accredited person believes collecting the data is 'reasonably needed' to provide the relevant goods or services or to fulfil another purpose for which the accredited person is seeking consent.[73]

---

[67] CDR Rule 4.11(3)(a).

[68] CDR Rule 4.11(3)(b).

[69] CDR Rule 4.12(2).

[70] CDR Rule 1.8.

[71] Including a de-identification consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rule 1.10A).

[72] CDR Rule 4.11(3)(c). For further information regarding the data minimisation principle, see Chapter B (Key concepts).

[73] CDR Rule 4.11(3)(c)(i).

- For example, the accredited person must explain how the data is necessary to deliver the service they are providing.[74]

C.52 The accredited person must also explain the reason for the data collection period. The collection period must be no longer than is 'reasonably needed' to provide the goods or services or to fulfil any other purpose for which the accredited person is seeking consent.[75]

- This means that the accredited person needs to explain why the data is collected over the collection period.
- There should be a reason why historical data is collected, and that reason must be both in line with the data minimisation principle and explained to the consumer at the point of consent.

C.53 For a use consent,[76] the accredited person must also explain that they will not use the CDR data beyond what is reasonably needed to provide the relevant goods or services or to fulfil another purpose for which the accredited person is seeking consent.[77]

Outsourced service providers

C.54 Where the accredited person uses an outsourced service provider[78] to collect CDR data, or may disclose the consumer's CDR data to an outsourced service provider (including one that is based overseas), the accredited person must:

- tell the consumer that the accredited person will use an outsourced service provider to collect CDR data and/or disclose the consumer's CDR data to an outsourced service provider, and
- provide the consumer with a link to the accredited person's CDR policy, noting that further information about outsourced service providers can be found in that policy.[79]

Withdrawal of consent

C.55 The accredited person must explain to the consumer: [80]

- that their consent/s can be withdrawn at any time
- how to withdraw consent, and
- the consequences (if any) of withdrawing consent.

---

[74] CDR Rule 4.11(3)(c).

[75] CDR Rule 4.11(3)(c)(i).

[76] Including a de-identification consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rule 1.10A).

[77] CDR Rule 4.11(3)(c)(ii).

[78] For further information regarding outsourced service providers, see Chapter B (Key concepts).

[79] CDR Rule 4.11(3)(f). An accredited data recipient's CDR policy must include, amongst other things, a list of outsourced service providers, the nature of their services, the CDR data and classes of CDR data that may be disclosed to those outsourced service providers. For further information, see Chapter 1 (Privacy Safeguard 1) and the Guide to developing a CDR policy.

[80] CDR Rule 4.11(3)(g).

Treatment of redundant data

C.56 The accredited person must tell the consumer whether the accredited person has a general policy of:

- deleting redundant data
- de-identifying redundant data, or
- deciding, when the CDR data becomes redundant, whether to delete or de-identify the redundant data.[81]

C.57 Where the accredited person will[82] or may[83] de-identify redundant data, the accredited person must also:

- allow the consumer to elect for their redundant data to be deleted, [84] including by outlining the consumer's right to elect for this to occur and providing instructions for how the consumer can make the election.[85] Where the accredited person is asking the consumer to amend an existing consent, and the consumer previously made an election, the accredited person may pre-select this election.[86]
- tell the consumer that the accredited person would de-identify redundant data in accordance with the prescribed process for de-identification of CDR data, and explain what this means[87]
- tell the consumer that, once the data is de-identified, the accredited person would be able to use or, if applicable, disclose the de-identified redundant data without seeking further consent from the consumer,[88] and
- if applicable, provide the consumer with examples of how the accredited person could use the redundant data once de-identified.[89]

C.58 See Chapter 12 (Privacy Safeguard 12) for further information on the treatment of redundant data (i.e. destruction or de-identification).

[81] CDR Rules 4.11(3)(h)(i) and 4.17(1).

[82] That is, because the accredited person communicated (when seeking consent) a general policy of de-identifying redundant data.

[83] That is, because the accredited person communicated (when seeking consent) a general policy of deciding, when the CDR data becomes redundant, whether to delete or de-identify the redundant data.

[84] CDR Rules 4.11(1)(e) and 4.16. The accredited person must allow the consumer to make this election when providing consent to the accredited person in relation to their CDR data, and at any other point in time before the consent expires (CDR Rule 4.16(1)).

[85] CDR Rule 4.11(3)(h).

[86] CDR Rule 4.12C(2)(b).

[87] CDR Rule 4.17(2)(a), 4.17(2)(b). The prescribed process is the CDR data de-identification process outlined in CDR Rule 1.17. Further information on the CDR data de-identification process is in Chapter 12 (Privacy Safeguard 12).

[88] CDR Rule 4.17(2)(a).

[89] CDR Rule 4.17(2)(c).

De-identification consents

C.59 Where an accredited person is asking the consumer for a de-identification consent as defined under CDR Rule 1.10A, the accredited person must also tell the consumer the additional information in CDR Rule 4.15:[90]

- what the CDR de-identification process is[91]
- if the accredited person would disclose (for example, by sale) the de-identified data to one or more other persons:
  - a statement of that fact
  - the classes of persons to whom the accredited person would disclose the de-identified data (for example, to market research organisations or university research centres), and
  - the purpose/s for which the accredited person would disclose the de-identified data (for example, to sell the de-identified data or to provide to a university for research)
- if the accredited person would use the de-identified data for general research:[92]
  - a statement of that fact
  - that the consumer can find further information in the accredited person's CDR policy of the research to be conducted and any additional benefit to be provided to the consumer for consenting to this use of their data,[93] and
  - a hyperlink to the relevant section/s of the accredited person's CDR policy, and
- that the consumer would not be able to elect to have the de-identified data deleted once it becomes redundant data.

C.60 When seeking a de-identification consent, the accredited person must explain how their collection and use is in line with the data minimisation principle.[94] See paragraphs C.50 to C.53 above.

---

[90] CDR Rules 4.11(3)(e) and 4.15.

[91] The CDR data de-identification process is outlined in CDR Rule 1.17. More information on this requirement is in Chapter 12 (Privacy Safeguard 12).

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

[93] For example, a benefit may include the accredited data recipient paying a fee to the consumer for using their data or providing a discount on the services they provide to the consumer: ACCC, CDR Rules Expansion Amendments Consultation Paper, September 2020, 48.

[94] CDR Rule 4.11(3)(c). For further information regarding the data minimisation principle, see paragraphs C.49 to C.53 and Chapter B (Key concepts).

Tip: Where an accredited person is seeking a de-identification consent so they may use the de-identified data for general research, the accredited person could inform the consumer that the general research does not relate to the provision of the requested goods or services. This will help to ensure a consumer is aware of this fact so they may make an informed decision when deciding whether to provide the de-identification consent.

Amendment of consent

C.61 Where an accredited person is inviting a consumer to amend their existing consent, in addition to the other requirements outlined in the above sections, the accredited person must give the consumer statements that outline:[95]

- the consequences of amending a consent, and
- the extent to which the accredited person will be able to use any CDR data that has already been disclosed to it.

Example: Laypac, an accredited person, offers consumers the ability to amend their collection consent, in order to remove certain data types. Prior to making an amendment, Laypac tells a consumer:

"If you amend your consent, we will no longer collect your account balance and details, but we will use the data we've already collected. Don't worry – when you withdraw your use consent or when it expires on 1 October, we will delete it,[96] along with all your other data, in accordance with our CDR policy…"[97]

Restrictions on seeking consents

C.62 CDR Rule 4.12 provides that when seeking consent from a consumer, an accredited person must not ask for:[98]

- consent to collect, use or disclose CDR data over a period exceeding 12 months
- consent to collect or use the data in a manner that is in breach of the data minimisation principle,[99] or
- a consent that is not in a 'category' of consents (see paragraph C.17 for a list of the categories of consents)[100]

[95] CDR Rule 4.12C(3).

[96] See Chapter 12 (Privacy Safeguard 12) for information on when CDR data will become 'redundant data' that must be deleted or de-identified in accordance with the CDR Rules, unless an exception applies.

[97] Example from Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 16.

[98] CDR Rule 4.12.

[99] The data minimisation principle is discussed in Chapter B (Key concepts), and at paragraph C.49.

[100] See CDR Rule 1.10A(2).

- consent to use the CDR data, including by aggregating it, for the purpose of identifying, compiling insights or building a profile in relation to any identifiable person who is not the consumer who is providing the consent.[101]

C.63 However, in some circumstances an accredited person can use the CDR data, including by aggregating it, for the purpose of identifying, compiling insights or building a profile in relation to any identifiable person who is not the consumer who is providing the consent. This is permitted where:[102]

- the person's identity is readily apparent
- the accredited person is seeking consent to derive, from the consumer's CDR data, CDR data about the non-CDR consumer's interactions with the consumer, and
- the accredited person will use that derived CDR data only for the purpose of providing the goods or services requested by the consumer.

Example: ChiWi is an accredited person offering a budgeting service that tracks a person's spending. One category of spending is 'gifts'.

Antonio has recently moved out of home and receives an allowance from his mother, Maria, each week. He has Maria's account saved in his banking address book under her full name.

Antonio transfers his transaction data to ChiWi to track his spending. Maria's identity is readily apparent from Antonio's transaction data.

ChiWi may consider Maria's behaviour only in so far as it is relevant to Antonio's spending and saving habits for the purpose of providing Antonio with the budgeting service.

How consents must be managed

Consumer dashboards

C.64 An accredited person must provide a consumer dashboard for each consumer who has provided a consent in relation to their CDR data.[103]

C.65 Where an accredited person collects a consumer's CDR data on behalf of another accredited person (the 'principal') under a CDR outsourcing arrangement, only the principal needs to provide the relevant consumer with a dashboard.[104]

C.66 An accredited person's consumer dashboard is an online service that can be used by each consumer to manage consumer data requests[105] and consents for the accredited person to collect, use and disclose CDR data.

---

[101] For example, where an accredited person receives information such as BSB numbers and account numbers as part of a consumer's payee list, the accredited person is prohibited from using that information to discover the name or identity of the payee or compile insights or a profile of that payee.

[102] CDR Rule 4.12(4).

[103] CDR Rule 1.14.

[104] See CDR Rule 1.7(5). For information regarding CDR outsourcing arrangements, see Chapter B (Key concepts).

[105] See Chapter B (Key concepts).

C.67 The consumer dashboard should be provided to the consumer as soon as practicable after the accredited person receives a valid request from that consumer for the collection and use of their CDR data.[106] This is so that the accredited person can comply with its obligation under Privacy Safeguard 5 to notify of the collection of CDR data via the consumer's dashboard.[107]

C.68 The consumer dashboard must contain the following details of each consent that has been given by the consumer:[108]

- the CDR data to which the consents relate
- for a use consent,[109] the specific use or uses for which the consumer has given consent
- the date on which the consumer gave the consents
- whether the consents were for the collection of CDR data on a single occasion or over a period of time
- if the consumer consented to collection and/or disclosure of CDR data over a period of time – what that period is and how often data has been (and is expected to be) collected and/or disclosed over that period
- if the consents are current – when they will expire
- if the consents are not current – when they expired
- the information required to notify the consumer of the collection of their CDR data, being:
  - what CDR data was collected
  - when the CDR data was collected, and
  - the CDR participant of the CDR data that was collected.[110]
- the information required to notify the consumer of the disclosure of their CDR data to an accredited person, being:
  - what CDR data was disclosed
  - when the CDR data was disclosed, and
  - the accredited person to whom the CDR data was disclosed, identified in accordance with any entry on the Register of Accredited Persons specified as being for that purpose, [111]and

---

[106] For further information regarding 'valid requests', see CDR Rule 4.3 and Chapter 3 (Privacy Safeguard 3).

[107] Privacy Safeguard 5 requires an accredited person to notify the consumer of the collection of their CDR data by updating the consumer's dashboard as soon as practicable to include certain matters. For further information, see CDR Rule 7.4 and Chapter 5 (Privacy Safeguard 5) of the CDR Privacy Safeguard Guidelines.

[108] CDR Rule 1.14(3).

[109] Including a de-identification consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rule 1.10A).

[110] Privacy Safeguard 5 requires an accredited person to notify the consumer of the collection of their CDR data by updating the consumer's dashboard to include certain matters. For further information, see CDR Rule 7.4 and Chapter 5 (Privacy Safeguard 5).

[111] Privacy Safeguard 10 requires an accredited data recipient to notify the consumer of the disclosure of their CDR data to an accredited person by updating the consumer's dashboard to include certain matters. For further information, see CDR Rule 7.9(2) and Chapter 10 (Privacy Safeguard 10).

- from 1 July 2021, if applicable, details of each amendment that have been made to a consent.

C.69 The consumer dashboard must have a functionality that allows the consumer, at any time, to:[112]

- withdraw each consent
- elect for their CDR data be deleted once it becomes redundant, and
- withdraw an election regarding whether their CDR data should be deleted once it becomes redundant.

C.70 These functionalities must be simple and straightforward to use, and prominently displayed.[113]

Tip: For best practice examples of how to present this information on the consumer dashboard, and other related recommendations, see the Consumer Experience Guidelines.

C.71 From 1 July 2021, the consumer dashboard may also include a functionality that allows a consumer to amend an existing consent.[114]

C.72 Data holders also have an obligation under the CDR Rules to provide a consumer dashboard to a consumer when the data holder receives a consumer data request on behalf of the consumer by an accredited person. The consumer dashboard is used to manage the consumer's authorisations to disclose the consumer's CDR data to the accredited person.[115] For further information, see Chapter B (Key concepts) and the Guide to privacy for data holders.

Consumers may withdraw consent

C.73 A consumer who has given a consent to an accredited person in relation to their CDR data may withdraw the consent at any time.

C.74 Where a consumer withdraws a collection consent, the accredited person must notify:

- the data holder of the withdrawal in accordance with the data standards,[116] and/or
- the accredited data recipient of the CDR data, as soon as practicable.[117]

C.75 Where a consumer withdraws an AP disclosure consent, the accredited person must notify the accredited data recipient to whom the data is being disclosed to, as soon as practicable.[118]

---

[112] CDR Rule 1.14(1)(c).

[113] CDR Rule 1.14(1)(c).

[114] See paragraphs C.27 to C.36 for information on amending consents.

[115] CDR Rule 1.15.

[116] CDR Rule 4.13(2).

[117] CDR Rule 4.18B(2).

[118] CDR Rule 4.18B(3).

C.76 An accredited person must allow a consumer to withdraw each consent they have provided by:[119]

- using the accredited person's consumer dashboard, or
- using a simple alternative method of communication made available by the accredited person.

C.77 The functionality to withdraw consent on the consumer dashboard must be simple and straightforward to use, and prominently displayed.[120]

C.78 The alternative method of communicating the withdrawal of consent must be simple.[121] In addition, it:

- should be accessible and straightforward for a consumer to understand and use, and
- may be written or verbal. Where it is written, the communication may be sent by electronic means (such as email) or non-electronic means (such as by post).

C.79 An accredited person may wish to ensure their alternative method of communication is consistent with existing channels already made available to its customers,[122] for example:

- through their telephone helpline, or
- in the case of direct marketing consents, through embedded links in any email communications that will allow a consumer to notify the accredited person of their intention to 'opt out' of receiving direct marketing communications.[123]

C.80 Where an accredited person does not have a general policy of deleting redundant data, and the consumer has not already requested that their redundant data be deleted, the accredited recipient:[124]

- must allow consumers to elect to have their redundant data deleted prior to the final withdrawal step, and
- should consider prompting consumers to exercise their right to elect to have their redundant data deleted at appropriate times (e.g. when inaction on the part of the consumer may cause them to lose the opportunity to exercise this right).

Tip: For examples of how to implement the withdrawal functionality on the consumer dashboard, and best practice recommendations for how to do this, see the Consumer Experience Guidelines.

[119] CDR Rule 4.13. A consumer must be enabled by an accredited person to independently withdraw each type of consent. For example, where a consumer provided a collection consent and use consent, the consumer can choose to withdraw only the collection consent. See the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [7].

[120] CDR Rule 1.14(1)(c).

[121] CDR Rule 4.13(1).

[122] Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2020*.

[123] For information about the use and disclosure of CDR data for direct marketing, see Chapter 7 (Privacy Safeguard 7).

[124] Consumer Experience Standards #16, Version 1.4.0.

Effect of withdrawing consent

C.81 The main consequence of the withdrawal of a consent is that the consent expires,[125] and the accredited person may no longer collect, use or disclose the CDR data (as applicable, depending on what category of consent has been withdrawn). Information about when a consent expires is contained in the following section.

C.82 Where a collection consent for the collection of CDR data from a data holder is withdrawn, the accredited person must notify the data holder of the withdrawal in accordance with the data standards.[126]

C.83 Where only a collection consent of particular CDR data is withdrawn, but other use consents[127] and/or disclosure consents[128] for that CDR data with the same accredited data recipient remain current, an accredited data recipient may continue to use[129] and/or disclose the relevant CDR data.

C.84 Where a consumer withdraws each of their collection, use and disclosure consents, the CDR data is likely to become redundant data that the accredited person is required to delete or de-identify in accordance with Privacy Safeguard 12 (unless an exception applies).[130]

C.85 If a consumer withdraws a consent using the accredited person's consumer dashboard, the withdrawal is immediately effective.[131]

C.86 If a withdrawal is not communicated over the consumer dashboard, the accredited person must give effect to the withdrawal as soon as practicable, but not more than two business days after receiving the communication.[132]

C.87 The test of practicability is an objective test. In adopting a timetable that is 'practicable' an accredited person can take technical and resource considerations into account. However, the accredited person must be able to justify any delay in giving effect to the consumer's communication of withdrawal.

---

[125] CDR Rules 4.14(1)(a) and (1)(b).

[126] CDR Rule 4.13(2)(b). When a data holder is notified of the withdrawal of the collection consent, the authorisation given by the consumer to the data holder to disclose that CDR data expires: see CDR Rule 4.26(1)(d).

[127] Including a de-identification consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to use that CDR data for the purposes of direct marketing (as per CDR Rule 1.10A).

[128] Including both an AP disclosure consent (as defined in CDR Rule 1.10A) and a direct marketing consent for an accredited data recipient of particular CDR data to disclose that CDR data to another accredited person for the purposes of direct marketing: CDR Rule 1.10A(1)(c)(ii).

[129] An accredited person may only collect CDR data in response to a 'valid request' from a consumer: s 56EF of the Competition and Consumer Act. A request ceases to be 'valid' if the consumer withdraws their collection consent: CDR Rule 4.3(4). However, if the consumer does not also withdraw their use consent, the accredited person may continue to use the CDR data it has already collected to provide the requested goods or services: see the note under CDR Rule 4.3(4). See further CDR Rule 4.18A for ongoing notification requirements in this circumstance. For further information, see Chapter 3 (Privacy Safeguard 3).

[130] More information on 'redundant data' and the requirement to destroy or de-identify redundant data is in Chapter 12 (Privacy Safeguard 12).

[131] CDR Rule 4.14(1)(b).

[132] CDR Rule 4.13(2)(a).

C.88 'Giving effect' to the withdrawal includes updating the consumer dashboard to reflect that the consent has expired,[133] as required by CDR Rule 4.19.[134]

C.89 Where a consumer has elected for their CDR data to be deleted upon becoming redundant data, withdrawal of a consent will not affect this election.[135]

Tip: For best practice examples of how to present this information on the consumer dashboard, and other related recommendations, see the Consumer Experience Guidelines.

When a consent expires

C.90 Where a consent expires, the accredited person may no longer collect, use or disclose the CDR data (as applicable, depending on what category of consent has expired).

C.91 Where each of a consumer's collection, use and disclosure consents expire, the CDR data is likely to become redundant data that the accredited person is required to delete or de-identify in accordance with Privacy Safeguard 12 (unless an exception applies).[136]

C.92 CDR Rule 4.14 provides that a consent expires in the following circumstances:

- **If the consent is withdrawn**: if a withdrawal notice is given via the consumer dashboard, the consent expires immediately.[137] Where withdrawal is not given through the consumer dashboard, the consent expires when the accredited person gives effect to the withdrawal, or two business days after receiving the communication, whichever is sooner.[138]
- **At the end of the period of consent (no longer than 12 months after consent was given):** a consent expires at the end of the specified period for which the consumer gave the consent.[139] This specified period cannot be longer than 12 months.[140]
- **Twelve months after the consent was given or last amended:** a consent expires at the end of the period of 12 months after:
  - the consent was given, or
  - if the duration of the consent has been amended, the consent was last amended.[141]
- **For a collection consent, when the accredited person is notified:**

[133] See CDR Rule 1.14(3)(g).

[134] CDR Rule 4.19 requires an accredited person to update the consumer dashboard as soon as practicable after the information required to be contained on the dashboard changes.

[135] CDR Rule 4.13(3) provides that withdrawal of a consent does not affect an election under CDR Rule 4.16 that the consumer's collected CDR data be deleted once it becomes redundant. CDR Rule 4.16 is discussed in Chapter 12 (Privacy Safeguard 12).

[136] More information on 'redundant data' and the requirement to destroy or de-identify redundant data is in Chapter 12 (Privacy Safeguard 12).

[137] CDR Rule 4.14(1)(b).

[138] CDR Rule 4.14(1)(a).

[139] CDR Rule 4.14(1)(e).

[140] CDR Rule 4.12(1). CDR Rule 4.14(1)(d) reinforces this maximum duration by providing that consent expires after the 12 month period after the consent was given.

[141] CDR Rule 4.14(1)(d).

- **by the data holder of the withdrawal of authorisation:** upon such notification, the consent expires immediately.[142]
- **by the accredited data recipient of the expiry of the AP disclosure consent:** upon such notification, the AP disclosure consent expires immediately.[143]

- **For an AP disclosure consent, when the accredited data recipient is notified by the accredited person of the expiry of the collection consent:** upon such notification, the collection consent expires immediately.[144]
- **If the accredited person's accreditation is revoked or surrendered:** consent expires when the revocation or surrender takes effect.[145]
- **If an accredited person becomes a data holder, rather than an accredited data recipient, of particular CDR data:** upon becoming a data holder,[146] all consents in relation to the particular CDR data expire.[147]
- **If another CDR Rule provides that a consent expires:**[148] (however, there are currently no such CDR Rules.)

C.93 The expiry of a consumer's collection consent does not automatically result in expiry of the use consent relating to any CDR data that has already been collected.[149]

C.94 In light of this, where a consumer's collection consent expires, but their use consent to provide the requested goods or services[150] remains current,[151] the accredited person must notify the consumer as soon as practicable that they may, at any time:[152]

- withdraw the use consent, and
- make the election to delete redundant data in respect of that CDR data.[153]

C.95 This notification must be given in writing (though not through the consumer's dashboard - although a copy of the notification may also be included in the consumer's dashboard).

C.96 This notification is important because where the collection consent expired as a result of the consumer's withdrawal, and the consumer did not also withdraw their use consent, the

---

[142] CDR Rule 4.14(1A).

[143] CDR Rule 4.14(1B).

[144] CDR Rule 4.14(1B).

[145] A revocation or surrender takes effect when the fact that the accreditation has been revoked or surrendered is included in the Register of Accredited Persons: CDR Rule 5.22. For further information, see the ACCC's Accreditation Guidelines.

[146] As a result of s 56AJ(4) of the Competition and Consumer Act and related clause 7.2 of Schedule 3.

[147] CDR Rule 4.14(1C).

[148] CDR Rule 4.14(1)(f).

[149] See the note under CDR Rule 4.3(4). See also the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [8].

[150] Being the goods or services requested under CDR Rule 4.3(1) as part of the valid request.

[151] For example, because the consumer withdraws only their collection consent.

[152] CDR Rule 4.18A.

[153] See CDR Rule 4.16.

accredited person may continue to use the CDR data it has already collected to provide the requested goods or services.[154] A consumer might not be aware of this.[155]

Notification requirements

Notifications to consumers

C.97 The CDR Rules require an accredited person to provide the following notifications to a consumer about consents, collections and disclosures:[156]

- **Notification following consent:** There is a requirement to provide a notice in the form of a CDR receipt to the consumer after they provide, amend or withdraw a consent.[157] The matters that must be included in the CDR receipt are outlined in CDR Rule 4.18.[158]
- **Ongoing notification for collection and use consents:** There is an ongoing notification requirement regarding the currency of the consumer's collection and use consents. CDR Rule 4.20 requires an accredited person to notify the consumer that their collection consent and/or use consent is still current where 90 days have elapsed since the latest of the following events:[159]
  - the consumer consenting to the collection and/or use of their CDR data
  - the consumer last amending their collection and/or use consents
  - the consumer last using their consumer dashboard, or
  - the accredited person last sending the consumer a notification that their collection consent or use consent is still current.
- **Notification if collection consent expires:** Where a consumer's collection consent expires, but their use consent to provide the requested goods or services remains current, the accredited person must notify the consumer of the matters in CDR Rule 4.18A as soon as practicable.[160]

---

[154] See the note under CDR Rule 4.3(4).

[155] An accredited data recipient must also provide a statement in its CDR policy indicating the consequences to the consumer for withdrawing a consent to collect and use CDR data: CDR Rule 7.2(4)(a).

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

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

[157] CDR Rule 4.18(1).

[158] CDR Rule 4.18(1). A CDR receipt must be given in writing other than through the consumer dashboard (although a copy of the CDR receipt may be included in the consumer's consumer dashboard). For more information, see CDR Rule 4.18.

[159] CDR Rules 4.20(3) and (4) state that this notification must be given in writing otherwise than through the consumer's consumer dashboard, however a copy may be included on the consumer dashboard.

[160] CDR Rule 4.18A. For further information on when a consent expires, see paragraphs C.90 to C.96.

- **Notification of collection:** There is a requirement to notify the consumer of the collection of their CDR data as soon as practicable after the collection of CDR data.[161]
- **Notification of disclosure:** There is requirement to notify the consumer of the disclosure of their CDR data to an accredited person as soon as practicable after the disclosure of the CDR data.[162]
- **Updating the consumer's dashboard:** There is a general obligation to update the consumer's dashboard as soon as practicable after the information required to be contained on the consumer dashboard changes.[163]

C.98 Data holders also have a general obligation under the CDR Rules to update the consumer's consumer dashboard as soon as practicable, where there is a change in the information required for that dashboard.[164] In addition, data holders must notify the consumer of the disclosure of their CDR data as soon as practicable after the disclosure of CDR data.[165]

Notifications to CDR participants

C.99 An accredited person must provide the following notifications about consents to CDR participants under the CDR Rules:

- **Notification to accredited data recipient if collection consent expires:** Where a consumer's collection consent expires, and the CDR data is being collected from an accredited data recipient, the accredited person must notify that accredited data recipient of the CDR data, as soon as practicable.[166]
- **Notification to data holder if collection consent is withdrawn:** Where a consumer withdraws their collection consent, and the CDR data is being collected from a data holder, the accredited person must notify that data holder of the withdrawal in accordance with the data standards.[167]
- **Notification if collection consent is amended:** Where a consumer amends their collection consent, the accredited person must notify the relevant CDR participant/s that the consent has been amended, in accordance with CDR Rule 4.18C.[168]

[161] Privacy Safeguard 5 requires an accredited data recipient to notify the consumer of the collection of their CDR data by updating the consumer's dashboard to include certain matters. For further information, see CDR Rule 7.4 and Chapter 5 (Privacy Safeguard 5).

[162] Privacy Safeguard 10 requires an accredited data recipient to notify the consumer of the disclosure of their CDR data to an accredited person by updating the consumer's dashboard to include certain matters. For further information, see CDR Rule 7.9(2) and Chapter 10 (Privacy Safeguard 10).

[163] CDR Rule 4.19.

[164] CDR Rule 4.27.

[165] Privacy Safeguard 10 requires a data holder to notify the consumer of the collection of their CDR data by updating the consumer's dashboard to include certain matters. For further information, see CDR Rule 7.9 and Chapter 10 (Privacy Safeguard 10).

[166] CDR Rule 4.18B(2).

[167] CDR Rule 4.13(2).

[168] For further information on the requirements under CDR Rule 4.18C, see paragraph C.34.

- **Notification if AP disclosure consent expires:** Where a consumer's AP disclosure consent expires, the accredited person must notify the accredited data recipient to whom the data is being disclosed to, as soon as practicable.[169]

Authorisation

C.100 Before an accredited person can receive a consumer's CDR data from a data holder, the consumer must authorise the data holder to disclose the particular data to that accredited person.

C.101 After receiving a consumer data request, the data holder must seek the consumer's authorisation for required or voluntary consumer data in accordance with Division 4.4 of the CDR Rules and the data standards,[170] unless an exception applies.[171]

C.102 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.[172]

C.103 Once a data holder has received this authorisation it:

- must disclose the required consumer data, and
- may disclose the relevant voluntary consumer data

through its accredited person request service and in accordance with the data standards, unless an exception applies.[173]

C.104 The flow chart below demonstrates the role of authorisation in the key information flow between a consumer, accredited person and data holder.

C.105 For further information on a data holder's authorisation obligations, see the Guide to privacy for data holders.

[169] CDR Rule 4.18B(3).

[170] See CDR Rule 4.5.

[171] See CDR Rule 4.7.

[172] See subdivision 4.3.2 of Schedule 3 to the CDR Rules, which set out how consumer data requests to data holders that relate to joint accounts are handled in the CDR regime.

[173] See CDR Rule 4.6A.

Overview: key information flow in the CDR regime