Chapter C:

Consent —

The basis for collecting and using CDR data

Version 2.0, July 2020

OAIC

Contents

Key points

- An accredited person may only collect and use consumer data right (CDR) data with the consent of the consumer.
- An accredited person must ask for a consumer's 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to ensure that a consumer's consent is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.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 for consent must be compliant with the data standards 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 and use of their CDR data.

C.2 Consumer consent for the collection and use of their data 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 and use of their CDR data by accredited persons. Consent must meet the requirements set out in the CDR Rules, and can only remain valid for a maximum period of 12 months. Without express consent, the accredited person is not able to collect or use CDR data.

C.5 However, under the Privacy Act, consent is not the primary basis upon which an entity may collect or use personal information.[1] In addition, where consent is involved, the consent can be either express or implied.[2]

[1] 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.

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

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 and use CDR data for which there are one or more consumers.[3]

C.9 Where an accredited person:

- offers a good or service through the CDR regime and
- needs to access a consumer's CDR data in order to provide such goods or services,

the accredited person must obtain the consumer's consent to the collection and use of their CDR data to provide the good or service.

C.10 An accredited person may only collect data in response to a 'valid request' from the consumer. The consumer's consent to the collection and use of their CDR data is a fundamental component of the 'valid request'.

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 data holder/s of the CDR data. The accredited person collects this CDR data by making a 'consumer data request' to the relevant data holder/s.[4]

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 CDR data under Privacy Safeguard 6. An accredited person may only use or disclose a consumer's CDR data in accordance with a current consent from the consumer.[5]

C.14 The flow chart at paragraph C.75 demonstrates how the role of 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.

---

[3] 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 CDR data. See Chapter 6 (Privacy Safeguard 6) for further information regarding use of CDR data.

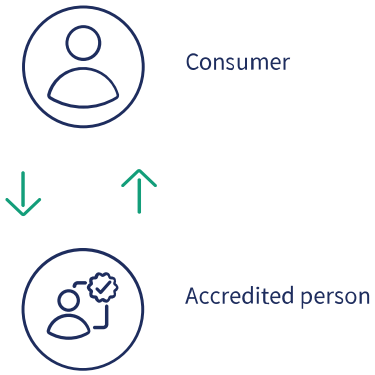
[4] For information regarding 'valid requests' and 'consumer data requests', see Chapter 3 (Privacy Safeguard 3). See also the flow chart underneath paragraph C.15 which demonstrates the points at which a valid request is given by the consumer and consumer data request is made on behalf of the consumer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

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

Consent and collection process for accredited persons

Obtaining consumer consent for the collection and use of CDR data

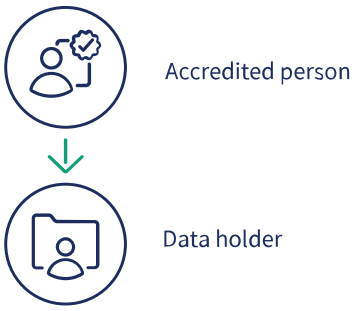
- Accredited person offers a good or service which requires CDR data
- Consumer wants to be provided the good or service
- Accredited person asks the consumer to consent to the collection and use of their CDR data for this purpose, for up to 12 months
- Consumer provides their express consent



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 data holder to disclose the consumer's CDR data
- Accredited person requests the data using the data holder's 'accredited person request service'



Data holder sends the consumer's CDR data to the accredited person, after obtaining consumer authorisation to do so

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

Consents to collect and use CDR data

C.16 An accredited person must ask the consumer to give consent to collect and use CDR data in accordance with Division 4.3 of the CDR Rules.

C.17 The requirements in Division 4.3 are outlined below under 'Requirements for asking for consent', 'Restrictions on seeking consent' and 'How consents to collect and use CDR data must be managed'.

C.18 The CDR Rules state that the objective of Division 4.3 is to ensure that consent given by a consumer to collect and use CDR data is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.[6]

C.19 In obtaining a valid request from a consumer, an accredited person must comply with requirements[7] relating to:

- an accredited person's processes for asking for consent[8]
- information to be presented to the consumer when asking for consent[9]
- restrictions on seeking consent,[10] and
- providing information, including in relation to withdrawal[11] and expiry of consent.[12]

C.20 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.[13]

Requirements for asking for consent

General processes

C.21 An accredited person's processes for asking for consent must:

- accord with the data standards, and
- be as easy to understand as practicable, including by using concise language and, where appropriate, visual aids.[14]

[6] CDR Rule 4.9. The Explanatory Statement to the CDR Rules provides that the CDR Rules are intended to ensure that requests for consent to collect and use CDR data are transparent and that consumers understand the potential consequences of what they are consenting to.

[7] in Subdivision 4.3.2 of the CDR Rules.

[8] CDR Rule 4.10.

[9] CDR Rule 4.11.

[10] CDR Rule 4.12.

[11] CDR Rule 4.13.

[12] CDR Rule 4.14.

[13] 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.

[14] CDR Rule 4.10.

C.22 In ensuring processes are easy to understand, an accredited person must also have regard to the Consumer Experience Guidelines.[15]

C.23 An accredited person must not:

- include or refer to other documents so as to reduce comprehensibility in seeking consent. This makes the consent harder to understand, or
- bundle consents with other consents or permissions.[16] This practice has the potential to undermine the voluntary nature of the consent.

C.24 Each time an accredited person seeks a consumer's consent, they must allow the consumer to actively select or clearly indicate:[17]

- the particular types of CDR data to which they are consenting
- the specific uses of that CDR data, and
- whether the data will be:
  - collected on a single occasion and used over a specified period of time (not exceeding 12 months), or
  - collected on an ongoing basis and used over a specified period of time (not exceeding 12 months).

C.25 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.24 above
- ask for the consumer's express consent to any direct marketing they intend to undertake, and
- not pre-select these options.[18]

Where voluntary consumer data is involved

C.26 If a consumer's request covers voluntary consumer data,[19] the data holder may decide to charge the accredited person a fee. If the accredited person intends to pass on the fee to the consumer, the accredited person must make this clear to the consumer.

C.27 To do this, the accredited person must:

- clearly distinguish between the required consumer data and the voluntary consumer data they are seeking to collect
- inform the consumer of the amount of the fee, and the consequences if the consumer does not consent to the collection of the voluntary consumer data, and

[15] 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).

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

[17] CDR Rules 4.11(1)(b) and 4.12(1).

[18] CDR Rule 4.11.

[19] For information regarding 'required consumer data' and 'voluntary consumer data', see Chapter B (Key concepts).

- allow the consumer to actively select or otherwise clearly indicate whether they consent to the collection of that data.

Name and accreditation number

C.28 The accredited person must ensure that their name is clearly displayed in the consent request.

C.29 The accredited person's accreditation number must also be included in the consent request.[20] This number has been assigned to the accredited person by the Data Recipient Accreditor.

C.30 For more information on the Data Recipient Accreditor and the accreditation process and conditions, see the ACCC's Accreditation Guidelines.

Data minimisation principle

C.31 Collection of CDR data is limited by the data minimisation principle,[21] 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.[22]

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.32 The accredited person must explain how their collection and use is in line with the data minimisation principle.[23]

C.33 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.[24]

- For example, the accredited person must explain how the data is necessary to deliver the service they are providing.[25]

[20] CDR Rule 4.11(3).

[21] CDR Rule 4.12(2).

[22] CDR Rule 1.8.

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

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

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

C.34 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.[26]

- 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.35 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.[27]

Disclosure to outsourced service providers

C.36 Where the accredited person might disclose the consumer's CDR data to an outsourced service provider[28] (including one that is based overseas), the accredited person must:

- tell the consumer that the accredited person will 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 disclosures to outsourced service providers can be found in that policy.[29]

Withdrawal of consent

C.37 The accredited person must explain to the consumer:

- that their consent can be withdrawn at any time
- how to withdraw consent, and
- the consequences (if any) of withdrawing consent, including what will happen to redundant data.[30]

Treatment of redundant data

C.38 The accredited person must tell the consumer whether the accredited person has a general policy of:

- deleting redundant data
- de-identifying redundant data, or

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

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

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

[29] 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. For further information, see Chapter 1 (Privacy Safeguard 1).

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

- deciding, when the CDR data becomes redundant, whether to delete or de-identify the redundant data.[31]

C.39 Where the accredited person will[32] or may[33] de-identify redundant data, the accredited person must also:

- allow the consumer to elect for their redundant data to be deleted, [34] including by outlining the consumer's right to elect for this to occur and providing instructions for how the consumer can make the election[35]
- 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[36]
- 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,[37] and
- if applicable, provide the consumer with examples of how the accredited person could use the redundant data once de-identified.[38]

C.40 See Chapter 12 (Privacy Safeguard 12) for further information on the treatment of redundant data (i.e. destruction or de-identification).

De-identification of CDR data

C.41 Where an accredited person asks for the consumer's consent to de-identify some or all of the CDR data for the purpose of disclosing (including by selling) the de-identified data, the accredited person must tell the consumer:[39]

- what the CDR de-identification process is[40]
- that the accredited person would disclose (for example, by sale) the de-identified data to one or more other persons
- 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)
- 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), and

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

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

[33] 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.

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

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

[36] CDR Rule 4.17(2)(a), 4.17(2)(b).

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

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

[39] CDR Rule 4.15.

[40] More information on this requirement is in Chapter 12 (Privacy Safeguard 12).

- that the consumer would not be able to elect to have the de-identified data deleted once it becomes redundant data.

C.42 Where the accredited person is seeking consent to de-identify some or all of the consumer's CDR data for the purpose of disclosing (including by selling) the de-identified data, the accredited person must explain how the collection and use (i.e. de-identification) of the CDR data is in line with the data minimisation principle (see paragraphs C.31 – C.35).

C.43 This necessarily involves explaining how de-identification and disclosure of the consumer's CDR data is reasonably needed to provide the goods or services to the consumer.[41]

Restrictions on seeking consent

C.44 CDR Rule 4.12 provides that when seeking consent from a consumer, an accredited person must not ask for consent to:[42]

- collect and use CDR data for a period exceeding 12 months
- collect or use the data in a manner that is in breach of the data minimisation principle[43]
- sell the CDR data (unless the CDR data will be de-identified in accordance with the prescribed de-identification process, and the accredited person has complied with the requirements in paragraphs C.41–C.43 above), or
- 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.[44]

C.45 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:[45]

- 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.

[41] This is because an accredited person is required under CDR Rule 4.11(3)(c) to indicate how it would comply with the data minimisation principle in relation to CDR data it seeks consent to de-identify. See paragraphs C.31–C.35. See Chapter 12 (Privacy Safeguard 12) for information about de-identification.

[42] CDR Rule 4.12.

[43] The data minimisation principle is discussed in Chapter B (Key concepts), and at paragraph C.31.

[44] 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.

[45] CDR Rule 4.12(4).

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 to collect and use CDR data must be managed

Consumer dashboards

C.46 An accredited person must provide a consumer dashboard for each consumer who has provided consent to the collection and use of their CDR data.

C.47 An accredited person's consumer dashboard is an online service that can be used by each consumer to manage consumer data requests[46] and associated consents for the accredited person to collect and use CDR data.

C.48 The consumer dashboard should be provided to the consumer as soon as practicable after the accredited person receives the relevant consumer data request.[47]

C.49 The consumer dashboard must contain the following details of each consent to collect and use CDR data that has been given by the consumer:[48]

- the CDR data to which the consent relates
- the specific use or uses for which the consumer has given consent
- the date on which the consumer gave consent
- whether the consent was for the collection of CDR data on a single occasion or over a period of time
- if the consumer consented to collection of CDR data over a period of time – what that period is and how often data has been (and is expected to be) collected over that period
- if the consent is current – when it will expire
- if the consent is not current – when it expired, and

[46] See Chapter B (Key concepts).

[47] This is to assist the accredited person in complying with its obligation under Privacy Safeguard 5 and Rule 7.4 to update the consumer's dashboard 'as soon as practicable' after the collection of CDR data to notify the consumer of certain matters. See Chapter 5 (Privacy Safeguard 5) of the CDR Privacy Safeguard Guidelines for further information.

[48] CDR Rule 1.14(3).

- 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 data holder/s of the CDR data that was collected.[49]

C.50 The consumer dashboard must have a functionality that allows the consumer, at any time, to:[50]

- withdraw 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.51 These functionalities must be simple and straightforward to use, and prominently displayed.

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.52 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.[51] For further information, see Chapter B (Key concepts) and the Guide to privacy for data holders.

Consumers may withdraw consent

C.53 A consumer who has given consent for an accredited person to collect and use their CDR data may withdraw the consent at any time.

C.54 Where a consumer withdraws consent, the accredited person must notify the data holder of the withdrawal in accordance with the data standards.[52]

C.55 An accredited person must allow a consumer to withdraw consent by:

- using the accredited person's consumer dashboard, or
- using a simple alternative method of communication made available by the accredited person.[53]

[49] 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).

[50] CDR Rule 1.14(c).

[51] CDR Rule 1.15.

[52] CDR Rule 4.13(2).

[53] CDR Rule 4.13.

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.[54]

C.56 The functionality to withdraw consent on the consumer dashboard must be simple and straightforward to use, and prominently displayed.[55]

C.57 The alternative method of communicating the withdrawal of consent must be simple.[56] 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.58 An accredited person may wish to ensure their alternative method of communication is consistent with existing channels already made available to its customers,[57] for example through their telephone helpline.

Effect of withdrawing consent

C.59 The main consequence of the withdrawal of consent is that the consent expires,[58] and CDR data can no longer be collected. Information about when consent expires is contained in the following section.

C.60 In addition, once a consumer withdraws consent 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).[59]

C.61 If a consumer withdraws consent using the accredited person's consumer dashboard, the withdrawal is immediately effective.[60]

C.62 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.[61]

C.63 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,

---

[54] For example, if an accredited data recipient 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 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).

[55] CDR Rule 1.14(c).

[56] CDR Rule 4.13(1).

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

[58] CDR Rule 4.26(1)(b).

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

[60] CDR Rule 4.14(1).

[61] CDR Rule 4.13(2).

the accredited person must be able to justify any delay in giving effect to the consumer's communication of withdrawal.

C.64 'Giving effect' to the withdrawal includes updating the consumer dashboard to reflect that the consent has expired,[62] as required by CDR Rule 4.19.[63]

C.65 Where a consumer has elected for their CDR data to be deleted upon becoming redundant data, their withdrawal of consent will not affect this election.[64]

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.66 Where a consent expires, the CDR data that the accredited person is required to delete or de-identify in accordance with Privacy Safeguard 12 is likely to become redundant data unless an exception applies.[65]

C.67 CDR Rule 4.14 provides that 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.[66] 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.[67]
- **When the accredited person is notified by the data holder of the withdrawal of authorisation:** upon notification from the data holder that the consumer has withdrawn authorisation, the consent expires immediately.[68]
- **At the end of the period of consent (no longer than 12 months after consent was given):** consent expires at the end of the specified period for which the consumer gave consent for the accredited person to collect and use the CDR data. This specified period cannot be longer than 12 months.[69]

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

[63] 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.

[64] CDR Rule 4.13(3) provides that withdrawal of 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).

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

[66] CDR Rule 4.14(1).

[67] CDR Rule 4.14(1).

[68] If the consumer has given the data holder an authorisation to disclose CDR data to the accredited person, and then withdraws that authorisation, the data holder must notify the accredited person under CDR Rule 4.25(2).

[69] 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.

- **If another CDR Rule provides that consent expires:** for example, a consent to collect CDR data expires once a person becomes a data holder rather than an accredited data recipient for the CDR data.[70]
- If the accredited person's accreditation is revoked or surrendered: consent expires when the revocation or surrender takes effect.[71]

Notification requirements

C.68 An accredited person must also comply with the following notification requirements under the CDR Rules:

- **CDR receipt:** There is a requirement to provide a notice in the form of a CDR receipt to the consumer after receiving a consumer consent or withdrawal of consent. A CDR receipt is a notice given by an accredited person to a consumer who has consented to the accredited person collecting and using their CDR data, or given to a consumer who has withdrawn such a consent.[72]
- **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.[73]
- **Update consumer's dashboard:** There is a general obligation to update the consumer's consumer dashboard as soon as practicable after the information required to be contained on the consumer dashboard changes.[74]
- **Ongoing notification:** There is an ongoing notification requirement regarding the currency of the consumer's consent.[75] CDR Rule 4.20 requires an accredited person to notify the consumer that their consent is still current where 90 days have elapsed since the latest of the following events:[76]
  - the consumer consenting to the collection and use of their CDR data
  - the consumer last using their consumer dashboard, or
  - the accredited person last sending the consumer a notification that their consent is still current.

C.69 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

[70] As a result of clause 7.2(3)(a) of Schedule 3 to the CDR Rules and section 56AJ(4) of the Competition and Consumer Act.

[71] For further information, see the ACCC's Accreditation Guidelines.

[72] 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.

[73] 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).

[74] CDR Rule 4.19.

[75] CDR Rule 4.20.

[76] CDR Rules 4.20(2) and (3) 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.

required for that dashboard.[77] 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.[78]

Authorisation

C.70 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.71 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 applicable data standards.

C.72 For the banking sector, for requests that relate to joint accounts, in some cases, the data holder might need to seek an authorisation from the other joint account holder.[79]

C.73 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.

C.74 The flow chart below demonstrates the role of authorisation in the key information flow between a consumer, accredited person and data holder.

C.75 For further information on authorisation, see the Guide to privacy for data holders.

[77] CDR Rule 4.27.

[78] 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).

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

Overview: key information flow in the CDR regime