

Chapter C:

Consent —

The basis for collecting and using CDR data

Consultation draft, October 2019

Contents

Key points	3
Why is it important?	3
How is consent in the CDR regime different to the Privacy Act?	3
How does consent fit into the CDR regime?	4
Consents to collect and use CDR data	6
Requirements for asking for consent	6
General processes	6
Where voluntary consumer data is involved	7
Name and accreditation number	8
Data minimisation principle	8
Disclosure to outsourced service providers	9
Withdrawal of consent	9
Treatment of redundant data	9
De-identification of CDR data	10
Restrictions on seeking consent	11
How consents to collect and use CDR data must be managed	12
Consumer dashboards	12
Withdrawal of consent	13
Expiry of consent	14

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, 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to ensure that a consumer's consent is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.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.

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 consumers' 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* (Cth) (the Privacy Act).
- C.4 The CDR regime requires express consent from consumers for the collection and use of their CDR data. Consent must meet the requirements set out in the Consumer Data Rules. 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 only 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
- C.6 The Consumer Data 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.

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](#) and [Chapter B: Key Concepts](#) of the OAIC Australian Privacy Principles Guidelines (22 July 2019),

² See s 6(1) of the Privacy Act and [Chapter B: Key Concepts](#) of the OAIC Australian Privacy Principles Guidelines.

How does consent fit into the CDR regime?

C.8 Consent is the only basis on which an accredited person may collect and use CDR data.

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.³

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.

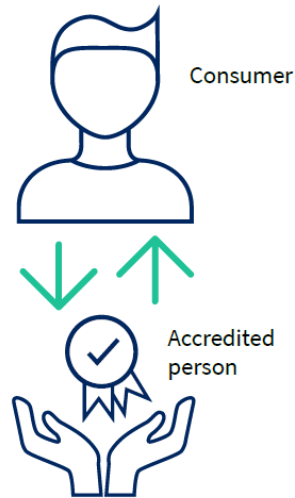
C.13 Consent also underpins how an accredited person may use CDR data under [Privacy Safeguard 6](#). An accredited person may only use or disclose CDR data in accordance with a current consent from the consumer.⁴


³ For information regarding 'valid requests' and 'consumer data requests', see [Chapter 3 \(Privacy Safeguard 3\)](#). See also the flow chart underneath paragraph C.13 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.

⁴ One way in which an accredited person is authorised to use or disclose CDR data under the Consumer Data Rules is to provide goods or services requested by the consumer. This must be done in compliance with the data minimisation principle and in accordance with a current consent from the consumer (Consumer Data Rule 7.5(1)(a)). For further information, see [Chapter 6 \(Privacy Safeguard 6\)](#).

Obtaining consumer consent for the collection and use of CDR data

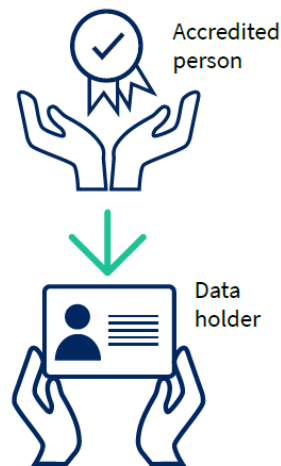
- Accredited person offers a good or service which requires CDR data
- Consumer wishes to be provided the good or service
- Accredited person asks the consumer to consent to the collection and use of their CDR data for this purpose, for up to 12 months
- Consumer provides their express consent



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 consumer data to accredited data recipient



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

Consents to collect and use CDR data

- C.14 An accredited person must ask the consumer to give consent to collect and use CDR data in accordance with Division 4.3 of the Consumer Data Rules.
- C.15 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.16 The Consumer Data 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.⁵
- C.17 In obtaining a valid request from a consumer, an accredited person must comply with requirements⁶ relating to:
- an accredited person’s processes for asking for consent⁷
 - information to be presented to the consumer when asking for consent⁸
 - restrictions on seeking consent⁹
 - providing information, including in relation to withdrawal¹⁰ and expiry of consent.¹¹
- C.18 Where a consumer is a business¹² 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 Importantly, the CDR regime currently extends only to business accounts in an individual’s name.

Requirements for asking for consent

General processes

- C.19 An accredited person’s processes for asking for consent must:
- accord with the data standards and

⁵ Consumer Data Rule 4.9. The explanatory statement to the Rules states that while the CDR regime places a high threshold on consent, it is not intended to make consent so complex as to discourage participation in the CDR regime. The focus of consents to collect and use should be on transparency and ensuring consumers understand the potential consequences of what they are agreeing to.

⁶ in Subdivision 4.3.2 of the Consumer Data Rules.

⁷ Consumer Data Rule 4.10.

⁸ Consumer Data Rule 4.11.

⁹ Consumer Data Rule 4.12.

¹⁰ Consumer Data Rule 4.13.

¹¹ Consumer Data Rule 4.14.

¹² And more broadly, where a consumer is not a natural person (i.e. they are a legal person).

¹³ An entity is entitled, under s 128 of the *Corporations Act 2001* (Cth), to make the assumptions set out in s 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.

- be as easy to understand as practicable, including by using concise language and, where appropriate, visual aids.¹⁴
- C.20 In ensuring processes are easy to understand, an accredited person should, at a minimum, be guided by the language and processes of the [Consumer Experience Guidelines](#).¹⁵
- C.21 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.
 - bundle consents with other consents or permissions¹⁶: this practice has the potential to undermine the voluntary nature of the consent.
- C.22 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
 - 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.23 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.22 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.24 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.25 To do this, the accredited person must:
- clearly distinguish between the required consumer data and the voluntary consumer data they are seeking to collect

¹⁴ Consumer Data Rule 4.10

¹⁵ Consumer Data Rule 4.10. The ‘Consumer Experience Guidelines’ provide best practice interpretations of the Consumer Data Rules relating to consent and are discussed in [Chapter B \(Key Concepts\)](#).

¹⁶ Consumer Data 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 Consumer Data Rule 4.11(1)(b) and 4.12(1).

¹⁸ Consumer Data Rule 4.11.

¹⁹ For information regarding ‘required consumer data’ and ‘voluntary consumer data’, see [Chapter B, Key Concepts](#).

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

Name and accreditation number

- C.26 The accredited person must ensure that their name is clearly displayed in the consent request.
- C.27 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.28 For more information on the Data Recipient Accreditor and the accreditation process and conditions, see the ACCC’s [Accreditation Guidelines](#).

Data minimisation principle

- C.29 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 is in breach of the data minimisation principle.

- C.30 The accredited person must explain how their collection and use is in line with the data minimisation principle.²³
- C.31 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 Consumer Data Rule 4.11(3).

²¹ Consumer Data Rule 4.12(2).

²² Consumer Data Rule 1.8.

²³ For further information regarding the data minimisation principle, see [Chapter B Key Concepts](#).

²⁴ Consumer Data Rule 4.11(3)(c)(i)

²⁵ Consumer Data Rule 4.11(3)(c).

C.32 The accredited person must also explain the reason for the data collection period. The collection period must be no longer than is ‘reasonably required’ to provide the goods or services.²⁶

- This means that the accredited recipient 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.33 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.34 Where the accredited person might disclose the consumer’s CDR data to an outsourced service provider²⁸ (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
- 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.35 The accredited person must explain to the consumer:

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

Treatment of redundant data

C.36 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 Consumer Data Rule 4.11(3)(c)(i)

²⁷ Consumer Data Rule 4.11(3)(c)(ii)

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

²⁹ Consumer Data Rule 4.11(f). An accredited person’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 Consumer Data Rule 4.11(g).

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

C.37 Where the accredited person will³² or may³³ de-identify redundant data, the accredited person must also:

- allow the consumer to elect for their redundant CDR 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 election³⁵
- 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 means³⁶
- 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 consumer³⁷ and
- if applicable, provide the consumer with examples of how the accredited person could use the redundant data once de-identified.³⁸

C.38 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.39 Where an accredited person is asking 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:

- what the CDR de-identification process is³⁹
- 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)

³¹ Consumer Data Rule 4.11(h).

³² That is, because the accredited person communicated (when seeking consent) a general policy of de-identifying redundant CDR 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 Consumer Data 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 (4.16(1)).

³⁵ Consumer Data Rule 4.11(h).

³⁶ Consumer Data Rule 4.17(2)(a), 4.17(2)(b).

³⁷ Consumer Data Rule 4.17(2)(a).

³⁸ Consumer Data Rule 4.17(2)(c).

³⁹ 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.40 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.30–C.33 above).

C.41 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.⁴⁰

Restrictions on seeking consent

C.42 Consumer Data Rule 4.12 provides that when seeking consent from a consumer, an accredited person must not ask for consent to:⁴¹

- 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 principle⁴²
- 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.39–C.41 above)
- 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.⁴³

C.43 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:

- 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.

⁴⁰ This is because an accredited person is required under Consumer Data 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.30–C.33 above. See [Chapter 12 \(Privacy Safeguard 12\)](#) for information about de-identification.

⁴¹ Consumer Data Rule 4.12.

⁴² The data minimisation principle is discussed in [Chapter B \(Key Concepts\)](#), and at paragraph C.29 above.

⁴³ 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.

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.44 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.45 An accredited person's consumer dashboard is an online service that can be used by each consumer to manage consumer data requests⁴⁴ and associated consents for the accredited person to collect and use CDR data.
- C.46 The consumer dashboard must contain the following details of each consent to collect and use CDR data that has been given by the consumer:⁴⁵
- the CDR data to which the consent relates
 - the specific use or uses for which the consumer has given consent
 - when 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
 - what CDR data was collected
 - when the CDR data was collected
 - the data holder/s of the CDR data that was collected.
- C.47 The consumer dashboard must have a functionality that allows the consumer, at any time, to:
- withdraw consent
 - elect their CDR data be deleted once it becomes redundant
 - withdraw an election regarding whether their CDR data should be deleted once it becomes redundant.

⁴⁴ See [Chapter B \(Key Concepts\)](#).

⁴⁵ Consumer Data Rule 1.14(3).

- C.48 These functionalities must be simple and straightforward to use, and prominently displayed.
- C.49 For examples of how to present this information on the consumer dashboard, and other best practice recommendations relating to the consumer dashboard, see the [Consumer Experience Guidelines](#).

Withdrawal of consent

- C.50 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.51 The main consequence of the withdrawal of consent is that the consent expires,⁴⁶ and 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).⁴⁷
- C.52 A consumer may withdraw consent by communicating the withdrawal in writing to the accredited person or by using the accredited person’s consumer dashboard.⁴⁸
- C.53 For examples of how to implement the withdrawal functionality on the consumer dashboard, and other best practice recommendations relating to the withdrawal functionality of the consumer dashboard, see the [Consumer Experience Guidelines](#).⁴⁹
- C.54 If a consumer withdraws consent using the accredited person’s consumer dashboard, the automatic processes required by the data standards mean that the withdrawal is immediately effective.
- C.55 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. This communication may be by electronic means such as email, or non-electronic means such as by post.
- C.56 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.
- C.57 An accredited person ‘gives effect’ to the withdrawal by ensuring that the same processes and procedures have occurred in relation to the withdrawal of that consent through writing as if the withdrawal had been effected through the consumer dashboard.⁵⁰

⁴⁶ 4.26(1)(b).

⁴⁷ More information on ‘redundant data’ and the requirement to destroy or de-identify redundant data is in [Chapter 12 \(Privacy Safeguard 12\)](#).

⁴⁸ 4.13.

⁴⁹ 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).

⁵⁰ The accredited person’s consumer dashboard must have a functionality that allows a consumer to withdraw consents: Rule 1.14(c)(i)(A).

- C.58 ‘Giving effect’ to the withdrawal includes updating the consumer dashboard to reflect that the consent has expired,⁵¹ as required by Consumer Data Rule 4.19.⁵²
- C.59 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.⁵³
- C.60 For examples of how to present this information on the consumer dashboard, and other best practice recommendations relating to the consumer dashboard, see the [Consumer Experience Guidelines](#).

Expiry of consent

- C.61 Where a consent expires, 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.⁵⁴
- C.62 Consumer Data 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.⁵⁵ 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.⁵⁶
 - **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.⁵⁷
 - **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.⁵⁸
 - **If another Consumer Data 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 data⁵⁹ or

⁵¹ See Consumer Data Rule 1.14(3)(g).

⁵² Consumer Data 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.

⁵³ Consumer Data Rule 4.13(3) provides that withdrawal of consent does not affect an election under Consumer Data Rule 4.16 that the consumer’s collected CDR data be deleted once it becomes redundant. Consumer Data Rule 4.16 is discussed in [Chapter 12 \(Privacy Safeguard 12\)](#).

⁵⁴ More information on ‘redundant data’ and the requirement to destroy or de-identify redundant data is in [Chapter 12 \(Privacy Safeguard 12\)](#).

⁵⁵ Consumer Data Rule 4.14(1)(b).

⁵⁶ Consumer Data Rule 4.14(1)(a).

⁵⁷ 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 Consumer Data Rule 4.25(2).

⁵⁸ Consumer Data Rule 4.12(1). Consumer Data Rule 4.14(1)(d) reinforces this maximum duration by providing that consent expires after the 12 month period after the consent was given.

⁵⁹ As a result of clause 7.2(3)(a) of Schedule 3 to the Consumer Data Rules and section 56AJ(4).

- **If the accredited person's accreditation is revoked or surrendered:** consent expires when the revocation or surrender takes effect.⁶⁰

⁶⁰ For further information, see the [ACCC Consumer Data Right Draft Accreditation Guidelines](#).