

# Chapter C:

# Consent —

## The basis for collecting, using and disclosing CDR data

Version ~~45.0~~, November ~~2022~~2023

# Contents

<b>Key points</b>	<b>3</b>
<b>Why is it important?</b>	<b>3</b>
<b>How is consent in the CDR system different to the Privacy Act?</b>	<b>3</b>
<b>How does consent fit into the CDR system?</b>	<b>4</b>
<b>What are the different categories of consents in the CDR system?</b>	<b>9</b>
<b>How must consent be sought?</b>	<b>11</b>
CDR representative arrangements	12
Sponsorship arrangements	13
<b>Can consents be amended?</b>	<b>13</b>
<b>Requirements for asking a consumer to give or amend a consent</b>	<b>15</b>
General processes	15
Fees for disclosure	17
Name and accreditation number	17
Data minimisation principle	18
Insight disclosure consent	19
Outsourced service providers	19
Withdrawal of consent	20
Treatment of redundant data	20
Collection by a sponsor at an affiliate's request	21
De-identification consents	21
Amendment of consent	23
<b>Restrictions on seeking consents</b>	<b>23</b>
<b>How consents must be managed</b>	<b>24</b>
Consumer dashboards	24
Consumers may withdraw consent	28
Effect of withdrawing consent	29
When a consent expires	31
Notification requirements	33
<b>Authorisation</b>	<b>35</b>
<b>Key points</b>	<b>4</b>
<b>Why is it important?</b>	<b>4</b>
<b>How is consent in the CDR system different to the Privacy Act?</b>	<b>4</b>
<b>How does consent fit into the CDR system?</b>	<b>5</b>

<b>What are the different categories of consents in the CDR system?</b>	<b>8</b>
<b>How must consent be sought?</b>	<b>11</b>
CDR representative arrangements	11
Sponsorship arrangements	12
<b>Can consents be amended?</b>	<b>12</b>
<b>Requirements for asking a consumer to give or amend a consent</b>	<b>15</b>
General processes	15
Fees for disclosure	17
Name and accreditation number	17
Data minimisation principle	17
Insight disclosure consent	19
Outsourced service providers (OSPs)	19
Withdrawal of consent	19
Treatment of redundant data	20
Collection by a sponsor at an affiliate's request	21
De-identification consents	21
Amendment of consent	22
<b>Restrictions on seeking consents</b>	<b>23</b>
<b>How consents must be managed</b>	<b>24</b>
Consumer dashboards	24
Consumers may withdraw consent	28
Effect of withdrawing consent	29
When a consent expires	31
Notification requirements	34
<b>Authorisation</b>	<b>37</b>

## Key points

- An accredited person may only collect, use and disclose CDR data with the consent of the [CDR consumer](#).
- The CDR system sets out specific categories of consents that an accredited person may seek from a CDR consumer. It prohibits an accredited person from seeking a consent which does not fit into these categories.
- The consumer data rules (CDR Rules) seek to ensure that a consumer's consent is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn. An accredited person must ask a CDR consumer to give or amend a consent in accordance with the CDR Rules.
- A CDR representative is responsible for seeking a CDR consumer's consent when CDR data is being collected by a CDR [representative](#) principal under a CDR representative arrangement. However, the CDR [representative](#) principal is liable if the CDR representative does not obtain consent in accordance with the CDR Rules.<sup>1</sup>
- In giving consent to the collection and use of their CDR data, a CDR consumer provides the accredited person with a 'valid request' to seek to collect the relevant CDR data.
- An accredited person's processes for asking a CDR consumer to give or amend a 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 system places the 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 system. Consent enables CDR consumers to be the decision makers in the CDR system, ensuring that they can direct where their data goes in order to obtain the most value from it.

## How is consent in the CDR system different to the Privacy Act?

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

---

<sup>1</sup>[CDR Rules, subrules 1.16A\(3\) and \(4\).](#)

#### C.4 Under the CDR system:

- express consent from consumers is required for the collection, use and disclosure of their CDR data by accredited persons.<sup>2</sup> Without express consent, the accredited person is not able to collect, use, or disclose CDR data
- consent must meet the requirements set out in the CDR Rules
- consent is time limited – a CDR consumer can only give consent for a maximum period of 12 months- (or 7 years for certain consents given by CDR business consumers).

#### C.5 However, under the Privacy Act:

- consent is not the primary basis upon which an entity may collect, use or disclose personal information<sup>3</sup>
- consent can be either express or implied<sup>4</sup>
- there is no maximum period for which a consumer can give consent, although consent given at a particular time in particular circumstances cannot be assumed to endure indefinitely.<sup>5</sup>

#### C.6 The CDR Rules contain specific requirements for an accredited person’s processes for seeking consent in the CDR system, as well as for information that must be presented to a CDR consumer when they are being asked to consent.<sup>6</sup>

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

## How does consent fit into the CDR system?

#### 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.<sup>7</sup>

---

<sup>2</sup> Consent is the only basis on which an accredited person may collect CDR data through the CDR. See [Chapter 3 \(Privacy Safeguard 3\)](#) for information on seeking to collect 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 CDR Rules (which requires consent), unless a use or disclosure is required or authorised by law: *Competition and Consumer Act, 2010 (Competition and Consumer Act)*, paragraph 56E(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 \(Privacy Safeguard 9\)](#).

<sup>3</sup> 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 APP Guidelines, [Chapter 3 \(APP 3\)](#) and [Chapter B \(Key concepts\)](#).

<sup>4</sup> See subsection 6(1) of the Privacy Act and APP Guidelines, [Chapter B \(Key concepts\)](#).

<sup>5</sup> See B.49, APP Guidelines, [Chapter B \(Key concepts\)](#).

<sup>6</sup> CDR Rules, rules 4.10 and 4.11.

<sup>7</sup> An accredited person may make a product data request without the involvement of a consumer, in which case consent is not required because it is not CDR data for which there are one or more consumers. For CDR data for which there are

## C.9 Where an accredited person:

- offers a good or service through the CDR system, and
- needs to collect a consumer's CDR data from a data holder or accredited data recipient ('CDR participant'), or a CDR representative, 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.<sup>8</sup> Under a CDR representative arrangement, the CDR representative asks the consumer for these consents.<sup>9</sup>

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.<sup>10</sup> An accredited person can only collect the CDR data if it has obtained this consent.

C.11 Upon obtaining a 'valid request' from the consumer, the accredited person<sup>11</sup> may seek to collect the consumer's CDR data from the relevant CDR participant, or CDR representative, of the CDR data. The accredited person collects this CDR data by making a 'consumer data request' to the relevant CDR participant/s,<sup>12</sup> or CDR representative/s.<sup>13</sup>

C.12 Privacy Safeguard 3 prohibits an accredited person from seeking to collect data under the CDR system 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. An accredited person can only use theor disclose CDR data if it has obtained a use or disclosure consent.

C.14 The flow charts below paragraph C.15 demonstrate how consent fits in the key information flow between a consumer, accredited person, data holder and (for the energy sector) AEMO as secondary data holder, in relation to CDR data.

---

one or more consumers, while consent is the only basis on which an accredited person may collect such CDR data, consent is a primary basis on which an accredited person may use and disclose such 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.

<sup>8</sup> CDR Rules, ~~rules~~ [rules 4.3 and 4.3B](#).

<sup>9</sup> CDR Rules, subrule 4.3A(2). See 'CDR representative arrangement' and 'CDR representative' in [Chapter B \(Key Concepts\)](#).

<sup>10</sup> CDR Rules, subrules 4.3(3) and 4.3A(4). -Where a consumer has given a CDR representative consent for a CDR representative principal to collect their CDR data and disclose it to the CDR representative, the CDR consumer provides the CDR representative principal (an accredited person) with a valid request.

<sup>11</sup> The accredited person is the CDR representative principal where the CDR consumer has given the CDR representative principal a valid request.

<sup>12</sup> ~~CDR Rules, 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.~~

<sup>13</sup> ~~CDR Rules, 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.15 The following charts demonstrate 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.

*[Note: the three diagrams showing CDR consent and collection process for accredited persons, for sponsors and for CDR representative arrangements have been updated].*

## What are the different categories of consents in the CDR system?

- C.16 The CDR system 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 Consent means a collection consent, a use consent or a disclosure consent (including a consent that has been amended by a consumer under the CDR Rules).<sup>14</sup> The categories of consents that may be given by a consumer to an accredited person in the CDR system are as follows:<sup>15</sup>
- **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.<sup>16</sup>
  - **Use consent** – a consent for an accredited data recipient of particular CDR data, or a CDR representative that holds the CDR data as service data, to use that CDR data in a particular way, for example to provide goods or services requested by the consumer.<sup>17</sup> Types of use consents include 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).<sup>18</sup>
  - **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.<sup>19</sup>

---

<sup>14</sup> CDR Rules, rule 1.7.

<sup>15</sup> 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. See [Chapter B \(Key concepts\)](#) which outlines some key words and phrases that are used in the privacy safeguards and CDR Rules, including in relation to consent.

<sup>16</sup> CDR Rules, paragraphs 1.10A(1)(a) and 1.10A(2)(a). If, in response to a collection consent, an accredited person proposes to make an SR data request to a data holder, the request must be made to the primary data holder and not the secondary data holder: CDR Rules, subrules 1.23(1)-(2). If the CDR consumer authorises the primary data holder to disclose the requested data, the primary data holder will then request any SR data it needs to respond to the request from the secondary data holder: CDR Rules, subrule 1.23(4). Under current arrangements, this is only relevant to the energy sector as the only sector with SR data and a secondary data holder (AEMO). For more information on SR data, see [Chapter B \(Key Concepts\)](#).

<sup>17</sup> CDR Rules, paragraphs 1.10A(1)(b) ~~and~~, 1.10A(2)(b) and 4.3A(2)(b).

<sup>18</sup> CDR Rules, rule 1.7 defines a consent as ‘a collection consent, a use consent or a disclosure consent; or such a consent as amended in accordance with these rules’.

<sup>19</sup> CDR Rules, paragraphs 1.10A(1)(c)(i) and 1.10A(2)(e).

Currently the CDR system only requires a consumer’s consent for disclosures to accredited persons. Consent is not required for disclosures to ~~outsourced service providers~~ [OSPs](#), 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 \(Key Concepts\)](#).



- **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.<sup>20</sup>
  - 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’.<sup>21</sup>

- **TA disclosure consent:** a consent for an accredited data recipient of particular CDR data, or a CDR representative, to disclose that CDR data to a trusted adviser of the CDR consumer, who belongs to one of the classes of ‘trusted advisers’ prescribed by CDR Rule 1.10C(2).<sup>22</sup>

An accredited data recipient or CDR representative must not make any of the following a condition for the supply of the goods or services:

- the consumer nominating a trusted adviser
  - the consumer nominating a particular person as a trusted adviser, or
  - the consumer giving consent to disclosure of data to a trusted adviser.<sup>23</sup>
- **Insight disclosure consent:** a consent for an accredited data recipient or CDR representative to disclose certain insights based on their CDR data to a specified person for a permitted purpose.<sup>24</sup> -These limited permitted purposes are:
    - to verify the CDR consumer’s identity
    - to verify the CDR consumer’s account balance, or
    - to verify the details of credits to, or debits from the consumer’s accounts.<sup>25</sup>

However, where the CDR data relates to more than one transaction, the insight disclosure consent cannot authorise the accredited data recipient or CDR representative to disclose an amount or date in relation to any individual transaction.<sup>26</sup>

- **De-identification consent:** a form of ‘use consent’ for an accredited data recipient of particular CDR data, or a CDR representative, to de-identify some or all of that CDR data in accordance with the CDR data de-identification process<sup>27</sup> and:

---

<sup>20</sup> CDR Rules, paragraphs 1.10A(1)(d) and 1.10A(2)(c).

<sup>21</sup> CDR Rules, paragraph 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.

<sup>22</sup> CDR Rules, paragraph 1.10A(1)(c)(iii).

<sup>23</sup> CDR Rules, subrule 1.10C(4). For the definition of a trusted adviser, including the classes of professions that are listed as trusted advisers, see [Chapter B \(Key concepts\)](#).

<sup>24</sup> CDR Rules, paragraph 1.10A(1)(c)(iv).

<sup>25</sup> CDR Rules, paragraph 1.10A(3)(a)(i)-(iii).

<sup>26</sup> CDR Rules, paragraph 1.10A(3)(b).

<sup>27</sup> See CDR Rules, rule 1.17 and [Chapter 12 \(Privacy Safeguard 12\)](#) for further information on the CDR data de-identification process.

- use the de-identified data for general research,<sup>28</sup> and/or
  - disclose (including by selling) the de-identified data.
- **A Business consumer disclosure consent: a consent for an accredited data recipient of particular CDR data to disclose that CDR data to a specified person,<sup>29</sup> where the CDR consumer providing consent is a CDR business consumer<sup>30</sup> who has given a business consumer statement.<sup>31</sup>**
- C.18 With the exception of business consumer disclosure consents, a CDR representative is also able to seek and obtain these use and disclosure consents in relation to CDR data it holds as service data.<sup>32</sup>
- C.19 An accredited person (or CDR representative) is prohibited from seeking a consent that is not in the list above.<sup>33</sup>
- C.20 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 CDR consumer must be enabled by an accredited person to independently manage each category of consent.<sup>34</sup> 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.<sup>35</sup>
- C.21 The categories of consent are based off the ‘types’ of consents set out in the CDR Rules.<sup>36</sup>

---

<sup>28</sup> ‘General research’ is defined in CDR Rules, 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 consumer.

<sup>29</sup> CDR Rules, paragraph 1.10A(1)(c)(v).

<sup>30</sup> CDR Rules, subrule 1.10A(9).

<sup>31</sup> CDR Rules, subrule 1.10A(10)-(11).

<sup>32</sup> CDR Rules, ~~subrule paragraphs~~ 1.10A(51)(b)-(e). See C.29 for more information.

<sup>33</sup> CDR Rules, paragraph 4.12(3)(a) (and ~~as modified by subrule paragraph 4.3C(120F(3)(a)~~ in relation to CDR representatives).

<sup>34</sup> See the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [7].

<sup>35</sup> 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.90 to C.98 (‘Effect of withdrawing consent’).

<sup>36</sup> The ‘categories’ of consent are listed at CDR Rules, subrule 1.10A(2) and defined by reference to the ‘types’ of consents listed at CDR Rules, ~~paragraph~~ subrule 1.10A(1).

## 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.<sup>37</sup> Division 4.3 sets out the specific requirements for each consent outlined in the section above.<sup>38</sup>
- C.23 The requirements in Division 4.3 are outlined below under the headings ‘Requirements for asking a consumer to give or amend a consent’, ‘Restrictions on seeking consents’ and ‘How consents must be managed’.
- C.24 The object of Division 4.3 of the CDR Rules is to ensure that consent given by a consumer is voluntary, express, informed, specific as to purpose, time limited and easily withdrawn.<sup>39</sup>
- 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<sup>40</sup>
  - information to be presented to the consumer when asking for consent,<sup>41</sup> and
  - restrictions on seeking consent.<sup>42</sup>
- C.26 Where a consumer is not an individual and wishes to use the accredited person’s good or service through the CDR system, 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.<sup>43</sup>

## CDR representative arrangements

- C.27 Under a CDR representative arrangement, the CDR representative seeks the relevant consents from the consumer, including consent for the CDR [representative](#) principal to

---

<sup>37</sup> ~~These requirements are modified in relation to~~ CDR representatives ~~seeking~~ [must seek](#) consent ~~by~~ [in accordance with Division 4.3A of the](#) CDR Rules, ~~rule 4.3C.~~

<sup>38</sup> 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 Rules, subrule 4.3(2). Where a CDR representative is seeking consent from the consumer for their CDR [representative](#) principal to collect CDR data, the ~~requirements~~ [CDR representative must ask for consent](#) in [accordance with](#) Division 4.3 ~~are modified in relation to CDR representatives by~~ [3A of the](#) CDR Rules, ~~rule 4.3C.~~

<sup>39</sup> CDR Rules, rule 4.9. [\(The same object is outlined in CDR Rules, rule 4.20C in relation to consent given by a consumer to a CDR representative\).](#) 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 system are transparent and that consumers understand the potential consequences of what they are consenting to.

<sup>40</sup> CDR Rules, rule 4.10: [\(CDR Rules, rule 4.20D for the corresponding obligations for CDR representatives\).](#)

<sup>41</sup> CDR Rules, rule 4.11: [\(CDR Rules, rule 4.20E for the corresponding obligations for CDR representatives\).](#)

<sup>42</sup> CDR Rules, rule 4.12: [\(CDR Rules, rule 4.20F for the corresponding obligations for CDR representatives\).](#)

<sup>43</sup> 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.

collect the consumer's CDR data.<sup>44</sup> See [Chapter B \(Key concepts\)](#) for more information on 'CDR representative arrangement', 'CDR representative' and 'CDR [representative](#) principal'.

C.28 ~~Like accredited persons, the~~The unaccredited CDR representative must ask for consent in accordance with Division 4.33A of the CDR Rules (~~as modified by subrule 4.3C(1)~~).<sup>45</sup> ~~which contains requirements which largely correspond to those for accredited persons in Division 4.3).~~ The CDR [representative](#) principal ~~must ensure its CDR representative complies with Division 4.3A and~~ is liable for any breach of ~~Division 4.3 (as modified by subrule 4.3C(1))~~that ~~division~~ by its CDR representative.<sup>46</sup>

C.29 A CDR representative can seek certain specific consents from the consumer as follows:<sup>47</sup>

- ~~a collection consent~~[collection consent](#) for the CDR [representative](#) principal to collect ~~the CDR consumer's~~ CDR data from ~~the~~ CDR participant; and
- ~~a use consent for:~~
- ~~the CDR principal to~~ disclose ~~that data (once collected)~~it to the CDR representative, ~~and~~
- ~~a use consent for~~ the CDR representative to use ~~that~~the data ~~in order~~ to provide ~~the requested~~those goods or services ~~to the consumer.~~

Once a collection consent has been given, a CDR representative may also ask the consumer to provide a disclosure consent in relation to the CDR data.<sup>48</sup>

## Sponsorship arrangements

C.30 Under a sponsorship arrangement, an affiliate is responsible for seeking consents from the consumer. This is regardless of whether the affiliate intends to collect the CDR data themselves (which they are permitted to do from an accredited data recipient) or request their sponsors to do so on their behalf.<sup>49</sup>

C.31 Like all accredited persons, an affiliate must ask for consents in accordance with Division 4.3 of the CDR Rules.

## Can consents be amended?

C.32 An accredited person may invite a consumer to amend an existing consent.<sup>50</sup> This includes allowing a consumer to change:

<sup>44</sup> CDR Rules, rule 4.3A.

<sup>45</sup> ~~As the Division 4.3 requirements are drafted to apply to accredited persons seeking consent, CDR Rules, subrule 4.3C(1) sets out how these are to be modified to apply to unaccredited CDR representatives seeking consent.~~

<sup>46</sup> CDR Rules, ~~subrule~~subrules 1.16A(3) and (4.3C(2)).

<sup>47</sup> CDR Rules, subrule 4.3A(2).

<sup>48</sup> CDR Rules, ~~subrules~~paragraph 1.10A(1)(c) (~~with the exception of business consumer disclosure consents~~) and ~~subrule~~ 4.3A(3).

<sup>49</sup> See CDR Rules, rule 5.1B. In particular, where CDR data is to be collected from a data holder, the affiliate must ask their sponsor to collect it as an affiliate cannot collect directly from a data holder: CDR Rules, subrule 5.1B(3).

<sup>50</sup> ~~A CDR representative may also invite a consumer to amend an existing consent – see CDR Rules, rules 4.20G-4.20I.~~

- 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.<sup>51</sup>
- C.33 An invitation to amend a consent may be issued only where the amendment would:<sup>52</sup>
- better enable the accredited person to provide the goods or ~~services~~ requested by the consumer under the existing consent,<sup>53</sup> 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.
- C.34 An invitation to amend an existing consent may be given via the consumer dashboard (if applicable)<sup>54</sup> or in writing to the CDR consumer.<sup>55</sup> An invitation can only be given where the consent is current (i.e. has not expired).<sup>56</sup>
- C.35 Where an accredited person wishes to invite a CDR 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.<sup>57</sup>

**Example:** A CDR consumer has given a consent to an accredited data recipient in relation to CDR data for a period of 3 months. In the 3 weeks prior to expiry, the accredited person invites the consumer on 2 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.<sup>58</sup>

- C.36 Where an accredited person wishes to invite a CDR consumer to extend the duration of their consent, it should first consider whether the invitation would constitute an offer to renew

---

<sup>51</sup> See the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [6].

<sup>52</sup> CDR Rules, subrule 4.12B(3).

<sup>53</sup> That is, the goods or services requested by the consumer as part of their valid request in CDR Rules, paragraph 4.3(1)(a).

<sup>54</sup> It is optional for accredited persons to offer a consent amendment functionality in the consumer dashboard: see CDR Rules, paragraphs 4.12B(2)(a) and 1.14(2A).

<sup>55</sup> CDR Rules, subrule 4.12B(2).

<sup>56</sup> CDR Rules, subrule 4.12B(3). See paragraphs C.99 to C.105 and CDR Rule 4.14 for information on when consent expires.

<sup>57</sup> CDR Rules, subrule 4.12B(4).

<sup>58</sup> Example adapted from the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 15.

existing goods or services under paragraph 7.5(3)(a)(ii) of the CDR Rules (in which case a direct marketing consent would be required).<sup>59</sup>

- C.37 An accredited person cannot ask a CDR consumer to extend the duration of an existing consent for longer than 12 months, unless the CDR consumer is a CDR business consumer and provides a business consumer statement. In this case, the accredited person cannot ask the CDR business consumer to extend the duration of an existing consent for longer than 7 years.<sup>61</sup>
- C.38 An accredited person must ask the CDR consumer to give any amendments to their existing consent in the same manner that it asked the consumer to provide the existing consent (~~i.e. in accordance~~ this includes compliance with Division 4.3 of the CDR Rules).<sup>62</sup> There are some exceptions, as outlined in the following section ('Requirements for asking a consumer to give or amend a consent').<sup>63</sup>
- C.39 Where a consumer data request made on behalf of a CDR consumer has not been completely resolved and the CDR consumer amends ~~their~~ the corresponding collection consent, the accredited person must notify the relevant CDR participant/s that the consent has been amended.<sup>64</sup>
- 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.40 An accredited person must also provide a CDR consumer with certain notifications upon the amendment of a consent. These are outlined under 'Notification requirements' in paragraph C.106.

---

<sup>59</sup> 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 Competition and Consumer Act, subsection 56EJ(1) and CDR Rules, paragraph 7.5(3)(a)(ii). For further information on this requirement, see [Chapter 7 \(Privacy Safeguard 7\)](#).

<sup>60</sup> This is as a result of CDR Rules, subrule 4.12(1) and paragraph 4.14(1)(c), which provides that the duration of a consent cannot exceed 12 months.

<sup>61</sup> This is as a result of CDR Rules, subrule 4.12(~~1A~~) and paragraph 4.14(1)(c), which ~~provides~~ provide that the duration of a consent cannot exceed ~~12 months~~ 7 years for a CDR business consumer who has given a business consumer statement. However, an accredited person may not deal with a person in their capacity as a CDR business consumer until the earlier of 1 December 2023 or the day the Data Standards chair makes related data standards (CDR rules, subrule 1.10A(14)).

<sup>62</sup> CDR Rules, subrule 4.12C(1).

<sup>63</sup> The exceptions are contained in subrule 4.12C(2) of the CDR Rules and allow certain details of the existing consent to be presented as pre-selected options (namely, the details covered by CDR Rules, paragraphs 4.11(1)(a), (b), ~~(ba)~~ and ~~(bae)~~). 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.

<sup>64</sup> CDR Rules, rule 4.18C.

C.41 An amendment of a consent takes effect when the CDR consumer amends the consent.<sup>65</sup>

## Requirements for asking a consumer to give or amend a consent

### General processes

C.42 An accredited person's processes for asking a CDR consumer to give or amend a consent must:

- accord with any consumer experience data standards,<sup>66</sup> and
- be as easy to understand as practicable, including by using concise language and, where appropriate, visual aids.<sup>67</sup>

C.43 In ensuring processes are easy to understand, an accredited person must also have regard to the Consumer Experience Guidelines.<sup>68</sup>

C.44 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
- bundle consents with other directions, agreements, consents or permissions.<sup>69</sup> This practice has the potential to undermine the voluntary nature of the consent.

C.45 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.<sup>70</sup>

C.46 Each time an accredited person seeks a CDR consumer's consent, it must allow the consumer to actively select or clearly indicate:

---

<sup>65</sup> CDR Rules, rule 4.12A. As per the note to this CDR Rule, it is not possible for the consumer to specify a different date or time.

<sup>66</sup> CDR Rules, 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 \(Key concepts\)](#).

<sup>67</sup> CDR Rules, rule 4.10.

<sup>68</sup> CDR Rules, rule 4.10. The 'Consumer Experience Guidelines' provide best practice interpretations of several CDR Rules relating to consent and are discussed in [Chapter B \(Key concepts\)](#). [They are available here: cx.cds.gov.au](https://www.cds.gov.au).

<sup>69</sup> CDR Rules, rule 4.10. Bundled consent refers to the 'bundling' together of multiple requests for a 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.

<sup>70</sup> 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 OSPs](#) (CDR Rules, paragraphs 4.11(3)(f)(i) and (ii)) and general research (CDR Rules, subrule 4.15(c)).

- for collection and disclosure consents,<sup>71</sup> the particular types of CDR data to which the consent will apply<sup>72</sup>
- 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~~, or in the case of a consent given by a CDR business consumer that includes a business consumer statement, 7 years), or
  - collected and, if applicable, disclosed on an ongoing basis and used over a specified period of time (not exceeding 12 months, or in the case of a consent given by a CDR business consumer that includes a business consumer statement, 7 years)<sup>73</sup>
- for a use consent,<sup>74</sup> the specific uses of that CDR data,<sup>75</sup> and
- for a disclosure consent,<sup>76</sup> the person to whom the CDR data may be disclosed.<sup>77</sup>

C.47 Each time an accredited person seeks a CDR consumer's consent, it must also:

- ask for the consumer's express consent for the selections in paragraph C.46 above,<sup>78</sup> and
- not pre-select these options,<sup>79</sup> except where the accredited person is asking the consumer to amend an existing consent.<sup>80</sup> In this situation, the accredited person may pre-select the above options to reflect what the consumer has selected in the past.<sup>81</sup>

---

<sup>71</sup> 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 Rules, paragraph 1.10A(1)(c)(ii).

<sup>72</sup> CDR Rules, paragraphs 4.11(1)(a)(i) and 4.11(1)(c) and subrule 4.11(2).

<sup>73</sup> CDR Rules, paragraphs 4.11(1)(b) and 4.11(1)(c), and subrules 4.11(2), 4.12(1) and 4.12(1)(A).

<sup>74</sup> 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 Rules, rule 1.10A).

<sup>75</sup> CDR Rules, paragraphs 4.11(1)(a)(ii) and 4.11(1)(c) and subrule 4.11(2).

<sup>76</sup> 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 Rules, paragraph 1.10A(1)(c)(ii).

<sup>77</sup> CDR Rules, paragraph 4.11(1)(ba) and subrule 4.11(2).

<sup>78</sup> CDR Rule, paragraph 4.11(1)(c).

<sup>79</sup> CDR Rules, subrule 4.11(2).

<sup>80</sup> CDR Rules, paragraph 4.12C(2)(a).

<sup>81</sup> For example, where this would assist the consumer to make an informed decision as to how they would like to amend their consent.



## Fees for disclosure

- C.48 An accredited person may charge the CDR consumer a fee for the disclosure of CDR data, or pass on to the consumer a fee charged by the data holder [or accredited data recipient](#) for the disclosure of CDR data.<sup>82</sup> This must be made clear to the consumer.
- C.49 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<sup>83</sup>
  - 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,<sup>84</sup> 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.<sup>85</sup>

## Name and accreditation number

- C.50 The accredited person must ensure that its name is clearly displayed in the consent request.<sup>86</sup>
- C.51 The accredited person's accreditation number must also be included in the consent request.<sup>87</sup> This number [has been is](#) assigned to the accredited person by the Data Recipient Accreditor.
- C.52 For more information on the Data Recipient Accreditor and the accreditation process and conditions, see the ACCC's Accreditation Guidelines.

## Data minimisation principle

- C.53 Collection and use of CDR data is limited by the data minimisation principle,<sup>88</sup> which provides that an accredited person:

---

<sup>82</sup> 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 \(Key concepts\)](#).

<sup>83</sup> CDR Rules, paragraph 4.11(1)(d) ([CDR Rules, paragraph 4.20E\(1\)\(e\) where a CDR representative is seeking consent](#)).

<sup>84</sup> CDR Rules, paragraph 4.11(3)(d) ([CDR Rules, paragraph 4.20E\(3\)\(h\) where a CDR representative is seeking consent](#)).

<sup>85</sup> CDR Rules, paragraph 4.11(1)(d) ([CDR Rules, paragraph 4.20E\(1\)\(e\) where a CDR representative is seeking consent](#)).

<sup>86</sup> CDR Rules, paragraph 4.11(3)(a).

<sup>87</sup> CDR Rules, paragraph 4.11(3)(b). Where a CDR representative is seeking consent, it must instead include [its name](#), the [CDR country in which it is located \(if not Australia\)](#), the [CDR representative](#) principal's name and accreditation number, the fact that the data will be collected by the CDR [representative](#) principal at the CDR representative's request, a link to the CDR [representative](#) principal's CDR policy, and a statement that the CDR consumer can obtain further information about collections or disclosures from the CDR [representative](#) principal's CDR policy: CDR Rules, subrule 4.11(3) as modified by rule 4.3C:(a)-(e), (j) and (l).

<sup>88</sup> CDR Rules, subrule 4.12(2).

- must not collect more data than is reasonably needed ~~in order to provide the requested goods or services, including over, or data that relates to~~ a longer time period than is reasonably ~~required~~ needed, for it or its CDR representative to provide the goods or services requested by the consumer, 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.<sup>89</sup>

**Example:** An accredited person is responding to a ‘valid request’ from a CDR 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.54 Where an accredited person is seeking a collection consent or use consent,<sup>90</sup> the accredited person must explain how its collection and use is in line with the data minimisation principle.<sup>91</sup>
- C.55 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.<sup>92</sup>
- For example, the accredited person must explain how the data is necessary to deliver the service that it is providing.<sup>93</sup>
- C.56 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.<sup>94</sup> 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 CDR consumer at the point of consent.

<sup>89</sup> CDR Rules, rule 1.8.

<sup>90</sup> Including a de-identification consent (as defined in CDR Rules, 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 Rules, rule 1.10A).

<sup>91</sup> CDR Rules, paragraph 4.11(3)(c) ([CDR Rules, paragraph 4.20E\(3\)\(f\) where a CDR representative is seeking consent](#)). For further information regarding the data minimisation principle, see [Chapter B \(Key concepts\)](#).

<sup>92</sup> CDR Rules, paragraph 4.11(3)(c)(i).

<sup>93</sup> CDR Rules, paragraph 4.11(3)(c).

<sup>94</sup> CDR Rules, paragraph 4.11(3)(c)(i).

C.57 For a use consent,<sup>95</sup> the accredited person must also explain ~~that it~~ how its use will not ~~use the CDR data~~ go 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.<sup>96</sup>

## Insight disclosure consent

C.58 When seeking an insight disclosure consent, an accredited data recipient must explain to the CDR consumer the CDR insight to be disclosed, including what the CDR insight would reveal or describe about them.<sup>97</sup>

## Outsourced service providers (OSPs)

C.59 Where ~~the accredited person uses an~~ CDR data may be disclosed to or collected by a direct or indirect outsourced service provider<sup>98</sup> ~~to collect CDR data, or may disclose the consumer's CDR data to an outsourced service provider (OSP)~~<sup>99</sup> of the accredited person (including one that is based overseas), the accredited person must:

- ~~tell~~ Tell the CDR consumer that the accredited person will use an ~~outsourced service provider~~ OSP to collect CDR data and/or disclose the consumer's CDR data to an ~~outsourced service provider~~ OSP, and
- provide the CDR consumer with a link to the accredited person's CDR policy, noting that further information about ~~outsourced service providers~~ OSPs can be found in that policy.<sup>100,101</sup>

## Withdrawal of consent

C.60 The accredited person must explain to the CDR consumer:<sup>102</sup>

- that their consent/s can be withdrawn at any time

<sup>95</sup> Including a de-identification consent (as defined in CDR Rules, 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 Rules, rule 1.10A).

<sup>96</sup> CDR Rules, paragraph 4.11(3)(c)(ii).

<sup>97</sup> CDR Rules, paragraph 4.11(3)(ca) (CDR Rules, paragraph 4.20E(3)(g) where a CDR representative is seeking consent).

<sup>98</sup> ~~For further information regarding outsourced service providers, see Chapter B (Key concepts).~~

<sup>99</sup> ~~For further information regarding OSPs, see Chapter B (Key concepts).~~

<sup>100</sup> CDR Rules, paragraph 4.11(3)(f). An accredited data recipient's CDR policy must include, amongst other things, a list of ~~outsourced service providers~~ OSPs, the nature of their services, the CDR data and classes of CDR data that may be disclosed to those ~~outsourced service providers~~ OSPs. For further information, see Chapter 1 (Privacy Safeguard 1) and the Guide to developing a CDR policy.

<sup>101</sup> Where a CDR representative is seeking consent from the CDR consumer, this requirement applies ~~to outsourced service providers~~ in the case of direct or indirect OSPs engaged by either the CDR representative or their CDR representative principal ~~where CDR data may disclosed to or collected by one of those providers, and a link to the CDR principal's CDR policy should be provided.~~ CDR Rules, ~~paragraphs~~ paragraphs 4.11(3)(f) as modified by rule 4.3C(k)-(l).

<sup>102</sup> CDR Rules, paragraph 4.11(3)(g) (CDR Rules, paragraph 4.20E(3)(m) where a CDR representative is seeking consent from the CDR consumer).

- how to withdraw consent, and
- the consequences (if any) of withdrawing consent.

## Treatment of redundant data

C.61 The accredited person must tell the CDR 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.<sup>103</sup>

C.62 Where the accredited person will<sup>104</sup> or may<sup>105</sup> de-identify redundant data, the accredited person must also:

- allow the CDR consumer to elect for their redundant data to be deleted,<sup>106</sup> including by outlining the consumer's right to elect for this to occur and providing instructions for how the consumer can make the election.<sup>107</sup> 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<sup>108</sup>
- tell the CDR 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<sup>109</sup>
- tell the CDR 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,<sup>110</sup> and

---

<sup>103</sup> CDR Rules, paragraph 4.11(3)(h)(i) and subrule 4.17(1) ([CDR Rules, paragraph 4.20E\(3\)\(n\)\(i\) and subrule 4.20N\(1\) where a CDR representative is seeking consent from the CDR consumer](#)).

<sup>104</sup> That is, because the accredited person communicated (when seeking consent) a general policy of de-identifying redundant data.

<sup>105</sup> 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.

<sup>106</sup> CDR Rules, paragraph 4.11(1)(e) and rule 4.16- ([CDR Rules, paragraph 4.20E\(1\)\(f\) and rule 4.20M where a CDR representative is seeking consent from the CDR consumer](#)). 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 Rules, subrule 4.16(1)).

<sup>107</sup> CDR Rules, paragraph 4.11(3)(h) ([CDR Rules, paragraph 4.20E\(3\)\(n\) where a CDR representative is seeking consent from the CDR consumer](#)).

<sup>108</sup> CDR Rules, paragraph 4.12C(2)(b).

<sup>109</sup> CDR Rules, paragraphs 4.17(2)(a), 4.17(2)(b). The prescribed process is the CDR data de-identification process outlined in rule 1.17. Further information on the CDR data de-identification process is in [Chapter 12 \(Privacy Safeguard 12\)](#).

<sup>110</sup> CDR Rules, paragraph 4.17(2)(a).

- if applicable, provide the CDR consumer with examples of how the accredited person could use the redundant data once de-identified.<sup>111</sup>

C.63 See [Chapter 12 \(Privacy Safeguard 12\)](#) for further information on the treatment of redundant data (i.e. destruction or de-identification).

## Collection by a sponsor at an affiliate's request

C.64 When an affiliate is seeking a collection consent from a CDR consumer, and a sponsor will collect the data at the affiliate's request under a sponsorship arrangement, the affiliate must provide the consumer with the following information:

- a statement of the fact that the sponsor will be collecting the consumer's CDR data at the request of the affiliate
- the sponsor's name
- the sponsor's accreditation number
- a link to the sponsor's CDR policy, and
- a statement that the consumer can obtain further information about the sponsor's collection of CDR data (and subsequent disclosure of that data to the affiliate) from the sponsor's CDR policy.<sup>112</sup>

## De-identification consents

C.65 Where an accredited person is asking the CDR consumer for a de-identification consent as defined under rule 1.10A of the CDR Rules, the accredited person must also tell the consumer the additional information in rule 4.15:<sup>113</sup>

- what the CDR de-identification process is<sup>114</sup>
- 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

---

<sup>111</sup> CDR Rules, paragraph 4.17(2)(c).

<sup>112</sup> See CDR Rules, subrule 4.3(2B) and paragraph 4.11(3)(i). ~~Where a CDR representative asks a consumer for consent, the requirement to include this information is replaced by a requirement to include certain information about the CDR principal – see footnote 91 for more information.~~

<sup>113</sup> CDR Rules, paragraph 4.11(3)(e) and rule 4.15: ~~(CDR Rules, paragraph 4.20E(3)(i) and rule 4.20L where a CDR representative is seeking consent from the CDR consumer).~~

<sup>114</sup> The CDR data de-identification process is outlined in CDR Rules, rule 1.17. More information on this requirement is in [Chapter 12 \(Privacy Safeguard 12\)](#).

- 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:<sup>115</sup>
    - a statement of that fact
    - that the CDR 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,<sup>116</sup> and
    - a hyperlink to the relevant section/s of the accredited person's CDR policy, and
  - that the CDR consumer would not be able to elect to have the de-identified data deleted once it becomes redundant data.
- C.66 When seeking a de-identification consent, the accredited person must explain how their collection and use is in line with the data minimisation principle.<sup>117</sup> See paragraphs C.53 to C.57 above.

**Tip:** Where an accredited person is seeking a de-identification consent so that it may use the de-identified data for general research, the accredited person could inform the CDR 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.67 Where an accredited person is inviting a CDR 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:<sup>118</sup>
- 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.

<sup>115</sup> 'General research' is defined in CDR Rules, 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].

<sup>116</sup> 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.

<sup>117</sup> CDR Rules, paragraph 4.11(3)(c) ([CDR Rules, paragraph 4.20E\(3\)\(f\) for CDR representatives](#)). For further information regarding the data minimisation principle, see paragraphs C.53 to C.57 and [Chapter B \(Key concepts\)](#).

<sup>118</sup> CDR Rules, subrule 4.12C(3) ([CDR Rules, subrule 4.20I\(3\) for CDR representatives inviting a consumer to amend consent](#)).

**Example:** Laypac, an accredited person, offers CDR 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 [...].~~ When you withdraw your use consent or when it expires on 1 October, we will delete it,<sup>119</sup> along with all your other data, in accordance with our CDR policy...”<sup>120</sup>*

C.68 When inviting a CDR business consumer to amend a consent, an accredited person must take reasonable steps to re-confirm that either the CDR consumer is not an individual, or that the CDR consumer has an active ABN.<sup>121</sup>

## Restrictions on seeking consents

C.69 CDR Rule 4.12 provides that when seeking consent from a CDR consumer, an accredited person must not ask for:<sup>122</sup>

- consent to collect, use or disclose CDR data over a period exceeding 12 months (unless the CDR consumer is a CDR business consumer)
- if the CDR consumer is a CDR business consumer who provides a business consumer statement, consent to use or disclose CDR data over a period exceeding 7 years. If a consent is sought for a period exceeding 12 months, the accredited person must give the CDR business consumer the option of choosing a period for the consent of 12 months or less
- consent to collect or use the data in a manner that is in breach of the data minimisation principle<sup>123</sup>
- a consent that is not in a ‘category’ of consents (see paragraph C.17 for a list of the categories of consents), or<sup>124</sup>
- 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.<sup>125</sup>

<sup>119</sup> 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.

<sup>120</sup> Example from Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020*, 16.

<sup>121</sup> [CDR Rules, subrule 4.12C\(4\)](#).

<sup>122</sup> CDR Rules, rule 4.12. [Corresponding restrictions on CDR representatives seeking consent are in CDR Rules, rule 4.20F.](#)

<sup>123</sup> The data minimisation principle is discussed in [Chapter B \(Key concepts\)](#), and at paragraph C.53 of this Chapter C.

<sup>124</sup> See CDR Rules, subrule 1.10A(2).

<sup>125</sup> 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.

€.69C.70 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 CDR consumer who is providing the consent. This is permitted where:<sup>126</sup>

- 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

€.70C.71 An accredited person must provide a consumer dashboard for each CDR consumer who has provided a consent in relation to their CDR data.<sup>127</sup>

€.71C.72 Where an accredited person collects a consumer’s CDR data on behalf of another accredited person (the ‘[OSP chain](#) principal’) under a CDR outsourcing arrangement, only the [OSP chain](#) principal needs to provide the relevant consumer with a dashboard.<sup>128</sup>

€.72C.73 Where a sponsor collects a consumer’s CDR data on behalf of their affiliate under a sponsorship arrangement, the affiliate must provide a consumer dashboard for each consumer who has provided a consent to the affiliate in relation to their CDR data.

€.73C.74 Where a CDR [representative](#) principal collects a consumer’s CDR data on behalf of their CDR representative under a CDR representative arrangement, the CDR [representative](#)

<sup>126</sup> CDR Rules, subrule 4.12(4).

<sup>127</sup> CDR Rules, rule 1.14.

<sup>128</sup> See CDR Rules, subrule 1.7(5). For information regarding CDR outsourcing arrangements, see [Chapter B \(Key concepts\)](#).



principal may arrange for the CDR representative to provide a consumer dashboard on its behalf.<sup>129</sup>

**Privacy tip:** To enhance consumer understanding and reduce the risk of confusion, it may be preferable for the CDR representative, rather than the CDR [representative](#) principal, to provide the consumer dashboard. This is because it is the CDR representative, rather than the CDR [representative](#) principal, that has the consumer-facing relationship.

Where this option is chosen, the CDR [representative](#) principal should include an obligation for the CDR representative to provide the dashboard as an additional requirement in the written contract (CDR representative arrangement). The CDR [representative](#) principal should further monitor compliance with these obligations as part of ensuring the CDR representative complies with the minimum requirements of that written contract.

[C.74C.75](#) An accredited person's consumer dashboard is an online service that can be used by each CDR consumer to manage consumer data requests<sup>130</sup> and consents for the accredited person to collect, use and disclose CDR data.

[C.75C.76](#) The consumer dashboard should be provided to the CDR 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.<sup>131</sup> This is so that the accredited data recipient can comply with its obligation under Privacy Safeguard 5 to notify of the collection of CDR data via the consumer's dashboard.<sup>132</sup>

[C.76C.77](#) The consumer dashboard must contain the following details of each consent that has been given by the CDR consumer:<sup>133</sup>

- the CDR data to which the consents relate
- for a use consent,<sup>134</sup> 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

<sup>129</sup> CDR Rules, subrule 1.14(5).

<sup>130</sup> See [Chapter B \(Key concepts\)](#).

<sup>131</sup> For further information regarding 'valid requests', see CDR Rules, rule 4.3 and [Chapter 3 \(Privacy Safeguard 3\)](#).

<sup>132</sup> 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 Rules, rule 7.4 and [Chapter 5 \(Privacy Safeguard 5\)](#) of the CDR Privacy Safeguard Guidelines.

<sup>133</sup> CDR Rules, subrule 1.14(3).

<sup>134</sup> Including a de-identification consent (as defined in CDR Rules, 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 Rules, rule 1.10A).

- if the consents are current – when they will expire
- if the consents are not current – when they expired
- for an insight disclosure consent – a description of the CDR insight and to whom it was disclosed<sup>135</sup>
- if a business consumer statement has been given in relation to the consent – that fact<sup>136</sup>
- 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<sup>137</sup>
- 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<sup>138</sup>
- the information required to notify the consumer when their CDR data has been disclosed to a trusted adviser, being:
  - what CDR data was disclosed
  - when the CDR data was disclosed, and
  - who the trusted adviser was<sup>139</sup>
- the information required to notify the consumer when a disclosure is made to a specified person under a business consumer disclosure consent, being:
  - what CDR data was disclosed
  - when the CDR data was disclosed, and
  - the person to whom it was disclosed<sup>140</sup>

---

<sup>135</sup> CDR Rules, paragraph 1.14(3)(ea).

<sup>136</sup> CDR Rules, paragraph 1.14(3)(eb).

<sup>137</sup> 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 Rules, rule 7.4 and Chapter 5 (Privacy Safeguard 5).

<sup>138</sup> 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 Rules, subrule 7.9(2) and Chapter 10 (Privacy Safeguard 10).

<sup>139</sup> CDR Rules, subrule 7.9(3).

<sup>140</sup> CDR Rules, subrule 7.9(3A).

- the information required to notify the consumer when a CDR insight has been disclosed, being:
  - what CDR data was disclosed
  - when the CDR data was disclosed, and
  - the person to whom it was disclosed<sup>141</sup>
- where the accredited person is an affiliate<sup>142</sup> and the CDR data will be collected by a sponsor at its request under a sponsorship arrangement, the sponsor's name and accreditation number,<sup>143</sup> and
- if applicable, details of each amendment that has been made to a consent.

C.77C.78 The consumer dashboard must also contain a statement that the CDR consumer is entitled to request further records in accordance with rule 9.5 of the CDR Rules (Request from CDR consumers for copies of records), and information about how to make such a request.<sup>144</sup>

C.78C.79 The consumer dashboard must have a functionality that allows the CDR consumer, at any time, to:<sup>145</sup>

- 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.79C.80 These functionalities must be simple and straightforward to use, and prominently displayed.<sup>146</sup>

**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.80C.81 The consumer dashboard may also include a functionality that allows a CDR consumer to amend an existing consent.<sup>147</sup>

<sup>141</sup> CDR Rules, subrule 7.9(4).

<sup>142</sup> An affiliate is a person with sponsored accreditation who has entered into a sponsorship arrangement with another person with unrestricted accreditation (the 'sponsor'). -See Chapter B for more information.

<sup>143</sup> CDR Rules, paragraph 1.14(3)(ha).

<sup>144</sup> CDR Rules, subrule 1.14(3A).

<sup>145</sup> CDR Rules, paragraph 1.14(1)(c).

<sup>146</sup> CDR Rules, paragraph 1.14(1)(c).

<sup>147</sup> See paragraphs C.32 to C.41 for information on amending consents.

~~C.81C.82~~ Data holders also have an obligation under the CDR Rules to offer, and in most circumstances 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.<sup>148</sup>

~~C.82C.83~~ The data holder's consumer dashboard is used to manage the consumer's authorisations to disclose the consumer's CDR data to the accredited person.<sup>149</sup> For further information, see [Chapter B \(Key concepts\)](#) and the [Guide to privacy for data holders](#).

## Consumers may withdraw consent

~~C.83C.84~~ A CDR consumer who has given a consent to an accredited person in relation to their CDR data may withdraw the consent at any time.<sup>150</sup>

~~C.84~~ Where a CDR consumer withdraws a collection consent, the accredited person must notify:

- ~~• the data holder of the withdrawal in accordance with the data standards,<sup>151</sup> and/or~~
- ~~• the accredited data recipient of the CDR data, as soon as practicable.<sup>152,153</sup>~~

~~C.85~~ Where a CDR 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.<sup>154</sup>

~~C.86C.85~~ An accredited person must allow a CDR consumer to withdraw each consent they have provided by:<sup>155</sup>

- using the accredited person's consumer dashboard, or

<sup>148</sup> Energy consumers may be eligible CDR consumers even if they do not have an online account with their retailer: see [Chapter B \(Key concepts\)](#) for further information. For eligible energy consumers without an online account, the retailer must offer the CDR consumer a dashboard and provide it if the CDR consumer accepts: CDR Rules, clause 2.3 of Schedule 4. For other CDR consumers, each data holder must provide a consumer dashboard: CDR Rules, rule 1.15.

<sup>149</sup> CDR Rules, rule 1.15.

<sup>150</sup> [CDR Rules, rule 4.13.](#)

<sup>151</sup> ~~CDR Rules, subrule 4.13(2). Rule 4.13 applies as if the primary data holder were the data holder for any SR data covered by an SR data request: CDR Rules, subrule 1.23(10). For more information on SR data, see [Chapter B \(Key Concepts\)](#).~~

<sup>152</sup> ~~CDR Rules, subrule 4.18B(2).~~

<sup>153</sup> ~~Where the CDR consumer withdraws a consent that was originally given to a CDR representative, it is the CDR principal under the CDR representative arrangement who must notify the data holder and accredited data recipient—CDR Rules, subrules 4.13(2) and 4.18B(2) as modified by subrule 4.3C(1).~~

<sup>154</sup> ~~CDR Rules, subrule 4.18B(3).~~

<sup>155</sup> CDR Rules, 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].

- using a simple alternative method of communication made available by the accredited person.<sup>156</sup>

**C.87C.86** The functionality to withdraw consent on the consumer dashboard must be simple and straightforward to use, and prominently displayed.<sup>157</sup>

**C.88C.87** The alternative method of communicating the withdrawal of consent must be simple.<sup>158</sup> 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.89C.88** An accredited person may wish to ensure its alternative method of communication is consistent with existing channels already made available to its customers,<sup>159</sup> for example:

- through its telephone helpline, or
- in the case of direct marketing consents, through embedded links in any email communications that will allow a CDR consumer to notify the accredited person of their intention to 'opt out' of receiving direct marketing communications.<sup>160</sup>

**C.90C.89** Where an accredited person does not have a general policy of deleting redundant data, and the CDR consumer has not already requested that their redundant data be deleted, it should refer to the requirements in the Consumer Experience Standards.<sup>161</sup>

**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.

## Effect of withdrawing consent

**C.91C.90** The main consequence of the withdrawal of a consent is that the consent expires,<sup>162</sup> 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.

<sup>156</sup> Where the CDR consumer withdraws a consent that was originally given to a CDR representative, it is the CDR [representative](#) principal under the CDR representative arrangement that must allow the consumer to withdraw consent via their consumer dashboard, or by an alternative method made available by the CDR [representative](#) principal [or CDR representative](#) for that purpose: [\(rule 4.20J\)](#).

<sup>157</sup> CDR Rules, paragraph 1.14(1)(c).

<sup>158</sup> CDR Rules, subrule 4.13(1).

<sup>159</sup> Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2020*.

<sup>160</sup> For information about the use and disclosure of CDR data for direct marketing, see [Chapter 7 \(Privacy Safeguard 7\)](#).

<sup>161</sup> The Consumer Experience Standards are available on the Consumer Data Standards website, [consumerdatastandards.gov.au](https://consumerdatastandards.gov.au).

<sup>162</sup> CDR Rules, paragraphs 4.14(1)(a) and (1)(b).

~~C.92~~ 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.<sup>163</sup>

~~C.93~~C.91 Where only a collection consent for particular CDR data is withdrawn, but other use consents,<sup>164</sup> and/or disclosure consents,<sup>165</sup> for that CDR data with the same accredited data recipient remain current, an accredited data recipient may continue to use and/or disclose the relevant CDR data.<sup>166</sup> For use consents in this situation, see 4.18A (for accredited persons) and 4.20Q (for CDR representatives) in relation to consumer notification requirements.

~~C.94~~C.92 Where a consent is withdrawn for an SR data request, the procedures and arrangements for withdrawal of consent in rule 4.~~13~~18AA of the CDR Rules apply to the primary data holder as if it were the data holder for the SR data covered by that request.<sup>167</sup>

~~C.95~~C.93 Where a CDR 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).<sup>168</sup>

~~C.96~~C.94 If a CDR consumer withdraws a consent using the accredited person's consumer dashboard, the withdrawal is immediately effective.<sup>169</sup>

~~C.97~~C.95 If a withdrawal is ~~not~~ communicated ~~over the consumer dashboard~~ through a simple alternative method of communication, the accredited person must give effect to the

---

<sup>163</sup> ~~CDR Rules, paragraph 4.13(2)(b). Where the CDR consumer withdraws a consent that was originally given to a CDR representative, it is the CDR principal under the CDR representative arrangement who must notify the data holder: CDR Rules, subrule 4.13(2) as modified by subrule 4.3C(1). 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 Rules, paragraph 4.26(1)(d).~~

<sup>164</sup> Including a de-identification consent (as defined in CDR Rules, 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 Rules, rule 1.10A).

<sup>165</sup> Including both an AP disclosure consent (as defined in CDR Rules, 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 Rules, paragraph 1.10A(1)(c)(ii).

<sup>166</sup> An accredited person may only collect CDR data in response to a 'valid request' from a consumer: Competition and Consumer Act, section 56EF. A request ceases to be 'valid' if the consumer withdraws their collection consent: CDR Rules, subrule 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 Rules, subrule 4.3(4). See further CDR Rules, rule 4.18A for ongoing notification requirements in this circumstance. For further information, see [Chapter 3 \(Privacy Safeguard 3\)](#).

<sup>167</sup> CDR Rules, subrule 1.23(10). For more information on SR data, see [Chapter B \(Key Concepts\)](#).

<sup>168</sup> More information on 'redundant data' and the requirement to destroy or de-identify redundant data is in [Chapter 12 \(Privacy Safeguard 12\)](#).

<sup>169</sup> CDR Rules, paragraph 4.14(1)(b). The same occurs where a consent given to a CDR representative is withdrawn through the consumer dashboard provided by the CDR representative or CDR representative principal (rule 4.20K(1)(a)).

withdrawal as soon as practicable, but not more than 2 business days after receiving the communication.<sup>170</sup>

~~C.98~~C.96 \_\_\_\_\_ 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.99~~C.97 \_\_\_\_\_ ‘Giving effect’ to the withdrawal includes updating the consumer dashboard to reflect that the consent has expired,<sup>171</sup> as required by rule 4.19 of the CDR Rules.<sup>172</sup>

~~C.100~~C.98 \_\_\_\_\_ Where a CDR consumer has elected for their CDR data to be deleted upon becoming redundant data, withdrawal of a consent will not affect this election.<sup>173</sup>

**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.101~~C.99 \_\_\_\_\_ 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.102~~C.100 \_\_\_\_\_ Where each of a CDR 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).<sup>174</sup>

~~C.103~~C.101 \_\_\_\_\_ ~~Rule~~For accredited persons, rule 4.14 of the CDR Rules provides that a consent expires in the following circumstances.<sup>175</sup>

<sup>170</sup> CDR Rules, paragraph 4.13(2)(a) ~~Where the CDR consumer withdraws a consent that was originally given) and 4.14(1)(a). Similarly, where a simple alternative method of communication is used to notify a CDR representative or a CDR representative, it is the CDR principal under the CDR representative arrangement who of the withdrawal of a consent, both~~ must give effect to the withdrawal ~~as soon as practicable and within 2 business days (subrules 4.20J(5) and (6)). They must also notify each other when one of them has received this withdrawal (subrule 4.20J(4)).~~

<sup>171</sup> See CDR Rules, paragraph 1.14(3)(g).

<sup>172</sup> CDR Rules, 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. CDR Rules, rule 4.19 ~~as modified by subrule 4.3C(1)20I~~ requires: ~~the CDR same of a CDR representative principal under the CDR representative arrangement to make this update where the CDR consumer originally gave consent to a CDR representative, and for the CDR representative to notify the CDR representative principal after the information required to be contained on the CDR representative principal’s consumer dashboard changes.~~

<sup>173</sup> CDR Rules, subrule 4.13(3) provides that withdrawal of a consent does not affect an election under CDR Rules, rule 4.16 that the consumer’s collected CDR data be deleted once it becomes redundant. CDR Rules, rule 4.16 is discussed in [Chapter 12 \(Privacy Safeguard 12\)](#).

<sup>174</sup> More information on ‘redundant data’ and the requirement to destroy or de-identify redundant data is in [Chapter 12 \(Privacy Safeguard 12\)](#).

<sup>175</sup> [See rule 4.20K for equivalent provisions that relate to CDR representatives.](#)

- **If the consent is withdrawn:** if a withdrawal notice is given via the consumer dashboard, the consent expires immediately.<sup>176</sup> Where withdrawal is not given through the consumer dashboard, the consent expires when the accredited person gives effect to the withdrawal, or 2 business days after receiving the communication, whichever is sooner.<sup>177</sup>
- **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.<sup>178</sup> This specified period cannot be longer than 12 months for CDR consumers, and 7 years for CDR business consumers who give a business consumer statement.<sup>179</sup>
- **Twelve months (for CDR consumers) or 7 years (for CDR business consumers) after the consent was given or last amended:** a consent expires at the end of the period of 12 months after:(for CDR consumers) or 7 years (for CDR business consumers who give a business consumer statement) after:
  - the consent was given, or
  - if the duration of the consent has been amended, the consent was last amended.<sup>180</sup>
- **For a collection consent, when the accredited person is notified:**
  - **by the data holder of the withdrawal of authorisation:** upon such notification, the consent expires immediately.<sup>181</sup>
  - **by the accredited data recipient of the expiry of the AP disclosure consent:** upon such notification, the AP disclosure consent expires immediately.<sup>182</sup>
- **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.<sup>183</sup>
- **If the accredited person's accreditation is revoked or surrendered:** consent expires when the revocation or surrender takes effect.<sup>184</sup>

---

<sup>176</sup> CDR Rules, paragraph 4.14(1)(b).

<sup>177</sup> CDR Rules, paragraph 4.14(1)(a).

<sup>178</sup> CDR Rules, paragraph 4.14(1)(~~ed~~).

<sup>179</sup> CDR Rules, subrule 4.12(1) and (1A). CDR Rules, paragraph 4.14(1)(~~ed~~) reinforces this maximum duration by providing that consent expires after the 12 month period after the consent was given.

<sup>180</sup> CDR Rules, paragraph 4.14(1)(~~ed~~) and 4.14(2).

<sup>181</sup> CDR Rules, subrule 4.14(~~A3~~).

<sup>182</sup> CDR Rules, subrule 4.14(~~B4~~).

<sup>183</sup> CDR Rules, subrule 4.14(~~B4~~).

<sup>184</sup> CDR rules, subrule 4.14(6). 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 Rules, rule 5.22. For further information, see the ACCC's Accreditation Guidelines.



- **If an accredited person becomes a data holder, rather than an accredited data recipient, of particular CDR data:** upon becoming a data holder,<sup>185</sup> all consents in relation to the particular CDR data expire.<sup>186</sup>
- **If an affiliate ceases to have a registered sponsor:** upon an affiliate<sup>187</sup> ceasing to have a registered sponsor,<sup>188</sup> any collection consents for the affiliate expire (but any use or disclosure consents continue in effect).<sup>189</sup> The affiliate would be required to notify a CDR consumer of this fact under rule 4.18A of the CDR Rules.
- **If another CDR Rule provides that a consent expires:**<sup>190</sup> (there is only one applicable CDR Rule: CDR Rules, subrule 5.1B(6) in relation to affiliates.)

C.104C.102 The expiry of a CDR consumer's collection consent does not automatically result in expiry of the use consent relating to any CDR data that has already been collected.<sup>191</sup>

C.105C.103 In light of this, where a CDR consumer's collection consent expires, but their use consent to provide the requested goods or services<sup>192</sup> remains current,<sup>193</sup> the accredited person must notify the consumer as soon as practicable that they may, at any time:<sup>194</sup>

- withdraw the use consent, and
- make an election to delete redundant data in respect of that CDR data.<sup>195</sup>

C.106C.104 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.107C.105 This notification is important because where the collection consent expired as a result of the consumer's withdrawal, and the CDR consumer did 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.<sup>196</sup> A consumer might not be aware of this.<sup>197</sup>

---

<sup>185</sup> As a result of subsection 56AJ(4) of the Competition and Consumer Act and related clause 7.2 of Schedule 3- and 9.2 of Schedule 4.

<sup>186</sup> CDR Rules, subrule 4.14(~~4E~~).

<sup>187</sup> An affiliate is a person with sponsored accreditation who has entered into a sponsorship arrangement with another person with unrestricted accreditation (the 'sponsor'). -See [Chapter B \(Key concepts\)](#) for more information.

<sup>188</sup> For example, this would occur if the sponsorship arrangement between the sponsor and affiliate terminates.

<sup>189</sup> CDR Rules, paragraph 4.14(1)(~~fe~~) and subrule 5.1B(6).

<sup>190</sup> CDR Rules, paragraph 4.14(1)(~~fe~~).

<sup>191</sup> See the note under CDR Rules, subrule 4.3(4). See also the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 3) 2020* at [8].

<sup>192</sup> Being the goods or services requested under CDR Rules, subrule 4.3(1) as part of the valid request.

<sup>193</sup> For example, because the consumer withdraws only their collection consent.

<sup>194</sup> CDR Rules, rule 4.18A.

<sup>195</sup> - See CDR Rules, rule 4.16.

<sup>196</sup> See the note under CDR Rules, subrule 4.3(4).

<sup>197</sup> 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 Rules, paragraph 7.2(4)(a).

## Notification requirements

### Notifications to consumers

~~C.108~~C.106 The CDR Rules require an accredited person<sup>198</sup> to provide the following notifications to a CDR consumer about consents, collections and disclosures:

- **Notification following consent:** There is a requirement to provide a notice in the form of a CDR receipt to the CDR consumer after they provide, amend or withdraw a consent.<sup>199</sup> The matters that must be included in the CDR receipt are outlined in rule 4.18 of the CDR Rules.<sup>200</sup>
- **Ongoing notification for collection and use consents:** There is an ongoing notification requirement regarding the currency of the CDR consumer's collection and use consents. Rule 4.20 of the CDR Rules 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:<sup>201</sup>
  - 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 CDR 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 rule 4.18A of the CDR Rules as soon as practicable.<sup>202</sup>
- **Notification of collection:** There is a requirement to notify the CDR consumer of the collection of their CDR data as soon as practicable after the collection of CDR data.<sup>203</sup>

---

<sup>198</sup> However, these notification requirements do not apply to an accredited person acting on behalf of a principal in its capacity as the provider of an outsourced service arrangement, in accordance with the arrangement, see CDR Rules, subrule 1.7(5). For information on 'CDR outsourcing arrangements', see [Chapter B \(Key concepts\)](#), 'Outsourced service provider'.

<sup>199</sup> CDR Rules, subrule 4.18(1). [A corresponding obligation applies to CDR representatives under CDR Rules, rule 4.20Q.](#)

<sup>200</sup> CDR Rules, ~~subrule~~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 Rules, rule 4.18.

<sup>201</sup> CDR Rules, subrules 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. [Corresponding obligations apply to CDR representatives under CDR Rules, rule 4.20U.](#)

<sup>202</sup> CDR Rules, rule 4.18A. For further information on when a consent expires, see paragraphs C.99 to C.105. [Corresponding obligations apply to CDR representatives under CDR Rules, rule 4.20Q.](#)

<sup>203</sup> Privacy Safeguard 5 requires an accredited data recipient to notify the consumer of the collection of their CDR data by updating the consumer's consumer dashboard to include certain matters. For further information, see CDR Rules, rule 7.4 and [Chapter 5 \(Privacy Safeguard 5\)](#).

- **Notification of disclosure:** There is requirement to notify the CDR consumer of the disclosure of their CDR data to an accredited person as soon as practicable after the disclosure of the CDR data.<sup>204</sup>
- **Updating the consumer's dashboard:** There is a general obligation to update the CDR consumer's dashboard as soon as practicable after the information required to be contained on the consumer dashboard changes.<sup>205</sup>

~~C.109 Where a CDR representative has obtained consents from the CDR consumer under a CDR representative arrangement, the CDR principal must comply with the notification requirements set out in paragraph C.108.<sup>206</sup> However, the CDR Rules provide that, where a CDR principal is required to provide one of these notifications, the notice may be given through the CDR representative.<sup>207</sup>~~

~~**Tip:** To enhance consumer understanding and reduce the risk of confusion, it may be preferable for the CDR representative, rather than the CDR principal, to provide the notifications required by subdivision 4.3.5 of the CDR Rules. This is because it is the CDR representative, rather than the CDR principal, that has the consumer-facing relationship.~~

~~Where this option is chosen, the CDR principal should include an obligation for the CDR representative to provide the notifications as an additional requirement in the written contract (CDR representative arrangement). The CDR principal should further monitor compliance with these obligations, as part of ensuring the CDR representative complies with the minimum requirements of that arrangement.~~

~~Where a CDR principal decides it is preferable to provide the notifications required by subdivision 4.3.5 of the CDR Rules themselves, the first time a notification is provided to the consumer, they could consider explaining their relationship to the CDR representative.~~

~~The above tips will help to aid the consumer's informed understanding of these important notifications (as the consumer might otherwise be confused as to why they are being contacted by an entity other than the CDR representative, in relation to the relevant goods or services).~~

~~C.110~~C.107 Data holders also have a general obligation under the CDR Rules to update the CDR consumer's consumer dashboard as soon as practicable, where there is a change in the information required for that dashboard.<sup>208</sup> In addition, data holders must notify the

<sup>204</sup> 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 consumer dashboard to include certain matters. For further information, see CDR Rules, subrules 7.9(2), 7.9(3) and 7.9(4) and [Chapter 10 \(Privacy Safeguard 10\)](#). [Subrule 7.9\(5\) also requires a CDR representative principal to notify a CDR consumer where its CDR representative discloses the CDR consumer's CDR data.](#)

<sup>205</sup> CDR Rules, rule 4.19.

<sup>206</sup> ~~CDR Rules, subdivision 4.3.5 as modified by rule 4.3C.~~

<sup>207</sup> ~~CDR Rules, subdivision 4.3.5 as modified by paragraph 4.3C(1)(i).~~

<sup>208</sup> CDR Rules, rule 4.27.

consumer of the disclosure of their CDR data as soon as practicable after the disclosure of CDR data.<sup>209</sup>

## Notifications to CDR participants

~~C.111C.108~~ C.108 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 CDR consumer's collection consent expires, and ~~the CDR~~ an accredited person has made a consumer data is being collected from request to an accredited data recipient based on that collection consent, and the request has not been completely resolved, the accredited person must notify that accredited data recipient of the CDR data, as soon as practicable.<sup>210</sup>
- **Notification to data holder if collection consent ~~is withdrawn~~ expires:** Where a CDR ~~consumer withdraws their~~ consumer's collection consent, ~~and the CDR expires, and an accredited person has made a consumer data is being collected from request to~~ a data holder based on that collection consent, and the request has not been completely resolved, the accredited person must notify that data holder of the withdrawal in accordance with the data standards.<sup>211</sup>
- **Notification if collection consent is amended:** Where a CDR consumer amends their collection consent, and the accredited person has made a consumer data request based on that collection consent, and the request has not been completely resolved, the accredited person must notify the relevant CDR participant/s that the consent has been amended, in accordance with rule 4.18C of the CDR Rules.<sup>212</sup>
- **Notification if AP disclosure consent expires:** Where a CDR consumer's AP disclosure consent expires, and an accredited person has made a consumer data request to an accredited data recipient on behalf of a CDR representative that has not been completely resolved, the accredited person must notify the accredited data recipient to whom the data is being disclosed to, as soon as practicable.<sup>213</sup>

<sup>209</sup> Privacy Safeguard 10 requires a data holder to notify the consumer of the collection of their CDR data by updating the consumer's consumer dashboard to include certain matters. For further information, see CDR Rules, rule 7.9 and [Chapter 10 \(Privacy Safeguard 10\)](#).

<sup>210</sup> ~~CDR Rules, subrule 4.18B(2); CDR Rules, subrule 4.18AA(2)(b).~~ Where consent expires that was originally given to a CDR representative, it is the CDR representative principal under the CDR representative arrangement who must notify the accredited data recipient of the expiry of consent. See CDR Rules, subrule 4.18B(2) and rule 4.20P.

<sup>211</sup> ~~CDR Rules, subrule 4.13(2); CDR Rules, subrule 4.18AA(2)(a).~~ Where consent expires that was originally given to a CDR representative, it is the CDR representative principal under the CDR representative arrangement who must notify the data holder of the expiry of consent. See CDR Rules, rule 4.20P.

<sup>212</sup> For further information on the requirements under CDR Rules, rule 4.18C, see paragraph C.39. Where consent is amended that was originally given to a CDR representative, it is the CDR representative principal under the CDR representative arrangement who must notify the relevant CDR participant that the consent has been amended. See CDR Rules, rule 4.20S.

<sup>213</sup> CDR Rules, ~~subrules~~ subrules 4.18B(3) and 4.20R(3).

# Authorisation

**C.112C.109** Before an accredited person can receive a CDR 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.113C.110** After receiving a CDR 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,<sup>214</sup> unless an exception applies.<sup>215</sup>

**C.114C.111** 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, in addition to the authorisation provided by the requesting CDR consumer<sup>216</sup>.

**C.115C.112** 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.<sup>217</sup>

**C.116C.113** The flow charts below demonstrate the role of authorisation in the key information flow between a CDR consumer, accredited person and data holder.

**C.117C.114** If the consumer data request relates to SR data, the primary data holder must request that the secondary data holder provide it with the SR data, so the primary data holder can disclose that SR data to the relevant accredited person.<sup>218</sup> Currently, the energy sector is the only CDR sector with a secondary data holder (AEMO) and SR data.

**C.118C.115** For further information on a data holder's authorisation obligations, see the [Guide to privacy for data holders](#).

**[Note: the two diagrams showing the key information flows in the CDR system for collection by accredited persons and by sponsors are unchanged. The third diagram about the key information flows under CDR representative arrangements has been updated].**

<sup>214</sup> See CDR Rules, rule 4.5.

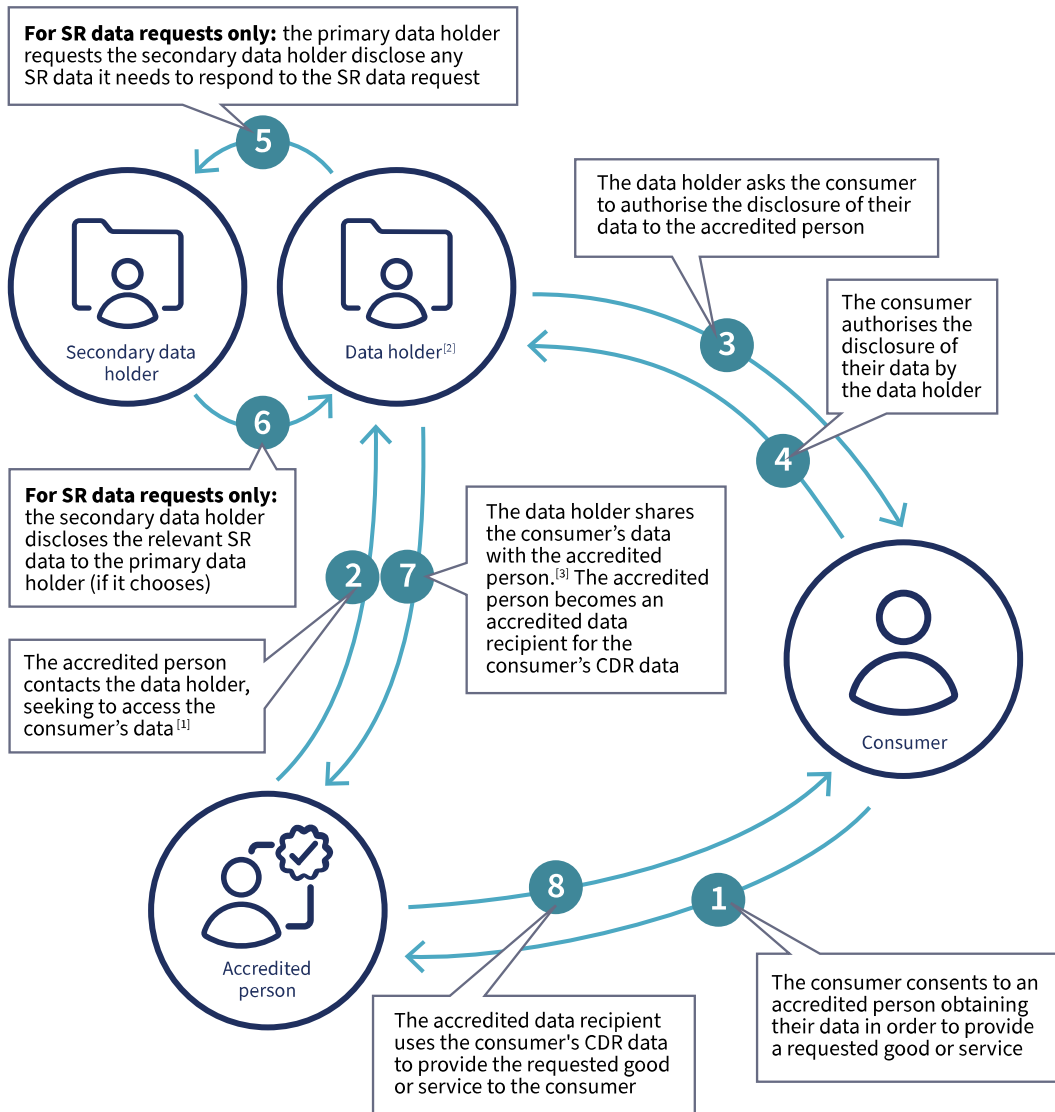
<sup>215</sup> See CDR Rules, rule 4.7.

<sup>216</sup> See CDR Rules, subdivision 4A.3.2, which sets out how consumer data requests to data holders that relate to joint accounts are handled in the CDR system.

<sup>217</sup> See CDR Rules, rule 4.6A.

<sup>218</sup> It is not mandatory for the secondary data holder to disclose the requested SR data to the primary data holder: CDR Rules, subrule 1.22(4). However, if a secondary data holder chooses not to disclose the requested SR data to the primary data holder, it must notify the primary data holder of its refusal: CDR Rules, subrule 1.22(5). For more information on SR data and primary data holders, see [Chapter B \(Key Concepts\)](#).

## Overview: key information flow in the CDR system

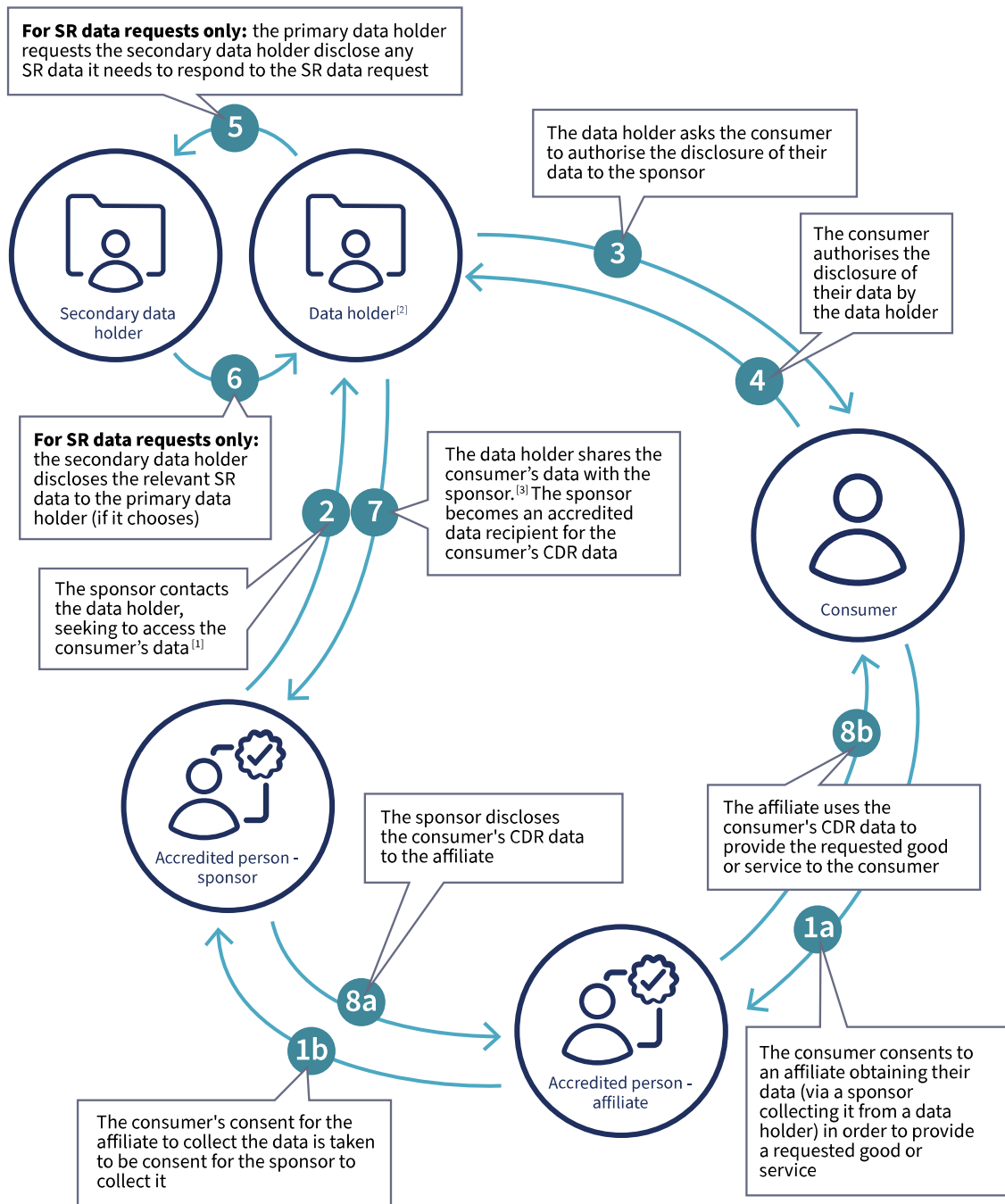


[1] If the accredited person is seeking CDR data that is or includes SR (shared responsibility) data, it contacts the primary data holder (rather than the secondary data holder)

[2] For SR data requests, this will be the primary data holder

[3] Where the data holder is a primary data holder and the secondary data holder has refused to disclose SR data to it, the primary data holder will not be able to share that SR data with the accredited person

## Overview: key information flow for collection by sponsors



[1] If the sponsor is seeking CDR data that is or includes SR (shared responsibility) data, it contacts the primary data holder (rather than the secondary data holder)

[2] For SR data requests, this will be the primary data holder

[3] Where the data holder is a primary data holder and the secondary data holder has refused to disclose SR data to it, the primary data holder will not be able to share that SR data with the sponsor