Maddocks

Australian Competition and Consumer Commission

CONSUMER DATA RIGHT REGIME

Update 2 to Privacy Impact Assessment

STAKEHOLDER CONSULTATION DOCUMENT

Analysis as at 29 September 2020

Contents

Part A Introduction

1. Overview

1.1 Maddocks is very pleased to provide this Consultation Document, which will be used to inform a second privacy impact assessment update report (**PIA Update 2 report**) for the Australian Competition and Consumer Commission (**ACCC**).

1.2 On 11 December 2019, the Department of the Treasury published the Privacy Impact Assessment into the Consumer Data Right Regime (**Original CDR PIA report**), together with the responses to the recommendations made in that report.

1.3 As the CDR PIA report was undertaken as a "point in time" analysis of the development of the legislative framework (that is, the *Competition and Consumer Act 2010* (Cth) (**CC Act**), *Competition and Consumer (Consumer Data Right) Rules 2020 (Cth)* (**CDR Rules**), Data Standards and the Open Banking Designation), the Original CDR PIA report recommended that it be treated as a "living document", which should be further updated and/or supplemented as the various components of the legislative framework are amended and/or developed[1].

1.4 Since the CDR Rules commenced on 6 February 2020, the ACCC has been reviewing, considering and revising the CDR Rules and a number of amendments to the CDR Rules have been made. Further stakeholder consultation processes have also been undertaken during that time.

1.5 Maddocks has been engaged to consider the privacy impacts of a further round of proposed amendments to the CDR Rules, including a number of changes that have been developed in parallel with our engagement. We have based our discussion and analysis in this Consultation Document on a consolidated version of the CDR Rules provided to us on 29 September 2020, which includes:

1.5.1 proposed changes to consents;

1.5.2 the introduction of changes that will allow a CDR Consumer to consent to disclosure of their CDR Data, which has been collected and is held by an Accredited Data Recipient, to another Accredited Person (**AP Disclosure Consents**);

1.5.3 the introduction of changes that will allow a CDR Consumer to consent to disclosure of their CDR Data, which has been collected and is held by an Accredited Data Recipient, to a Trusted Adviser who is not an Accredited Person (**TA Disclosure Consents**);

1.5.4 the introduction of changes that will allow a CDR Consumer to consent to disclosure of a "CDR insight", derived from their CDR Data by an Accredited Data Recipient, to any person (**Insight Disclosure Consent**);

1.5.5 the introduction of new levels and kinds of accreditation, so that a person may apply for unrestricted accreditation, data enclave accreditation, limited data accreditation, or affiliate accreditation; and

[1] Recommendation 1 in the Original CDR PIA report.

1.5.6 changes to the application of the CDR regime to joint account holders.

1.6 Our work has occurred in parallel with the drafting of the proposed amendments to the CDR Rules. We understand that a version of those proposed amendments has been published by the ACCC for stakeholder consultation. This version includes further proposed amendments that we have not had the opportunity to review and consider whether they pose any additional privacy risks. These further amendments include:

1.6.1 changes to the way that partnerships are managed for the purposes of the CDR regime, including the introduction of the concept of nominated representatives;

1.6.2 the introduction of the concept of account privileges and secondary users for an account;

1.6.3 changes in relation to management of CDR complaint data;

1.6.4 requirements in relation to use of the CDR logo;

1.6.5 changes in relation to product data requests;

1.6.6 the introduction of a new ability for the Accreditation Registrar to temporarily prevent the making of consumer data requests or responding to such requests, in order to ensure the security, integrity and stability of the Accreditation Register;

1.6.7 new civil penalty provisions; and

1.6.8 for the banking sector, changes to eligible CDR Consumers, required consumer data, and the introduction of the concept of pre-application CDR Data.

1.7 These additional proposed amendments are not discussed in this Consultation Document.

Note to Stakeholders: *Maddocks is keen to consult with interested and affected stakeholders, to ensure that the PIA Update 2 process properly identifies and considers all privacy risks and issues, from a broad range of perspectives. Timing requirements have meant that this process has not yet been possible. This document should only be considered as a preliminary analysis of the privacy risks, current or proposed mitigation strategies in relation to those risks, and our identified gaps and proposed recommendations. These will be subject to further consideration, including as part of the stakeholder consultation process.*

We are particularly interested in Stakeholders' views about any additional privacy risks that have not been fully or appropriately discussed in ***Part C*** *and any additional mitigation strategies that are already in place or which are proposed in the amendments to the CDR Rules, or further strategies that should be considered in relation to the proposed CDR Rule changes (as discussed in* ***Part C*** *of this Consultation Document).*

2. Structure of this Consultation Document

2.1 This Consultation Document is comprised of the following sections:

2.1.1 **Part B - Project Description:** This section contains a summary of the further proposed changes to the CDR Rules discussed in paragraph 1.5 of this **Part A**, and discusses the various concepts and information flows relevant to those proposed changes.

2.1.2 **Part C - Analysis of Risks:** We have analysed the potential privacy risks that we have identified as being associated with the relevant proposed changes to the CDR Rules. We have identified the current mitigation strategies and conducted a gap analysis to identify any areas of concern, as well as outline our preliminary proposed recommendations.

2.1.3 **Attachment 1 - Glossary:** This section sets out a list of some capitalised terms that we have used in this Consultation Document, and their definitions.

Note to Stakeholders: *All capitalised terms will be included in the Glossary in the PIA Update report (not yet completed).*

Part B Project Description

3. Changes to consents

3.1 As discussed in the Original CDR PIA report[2], the CDR Rules (as currently drafted) provide that the CDR Consumer must provide the Accredited Data Recipient with their consent to:

3.1.1 collect their CDR Data from the Data Holder; and

3.1.2 use their CDR Data for specific purposes once it is received.

3.2 The provision of this consent constitutes a 'valid request' by the CDR Consumer that the Accredited Data Recipient collect their CDR Data from the relevant Data Holder (so that the Accredited Data Recipient can use the CDR Consumer's CDR Data for the provision of goods and services).

3.3 There are several changes being proposed to the concept of "consent" in the proposed amendments to the CDR Rules. Changes to the operation of consent in the CDR regime are discussed below.

3.4 In the Original CDR PIA report, for convenience, we used "Accredited Data Recipient" to refer to an accredited person who either has, or may, receive CDR Data under the CDR Regime. As discussed in the Original CDR PIA report:

3.4.1 a person is an **Accredited Person** if they hold an accreditation under section 56CA(1) of the CC Act; and

3.4.2 a person is an **Accredited Data Recipient** of CDR Data (under section 56AK of the CC Act) if:

(a) they are an Accredited Person;

(b) the CDR Data is held by (or on behalf of) the person;

(c) the CDR Data was disclosed to the person under the CDR Rules; and

(d) the person is not a Data Holder for the CDR Data.[3]

3.5 The distinction between an Accredited Person and an Accredited Data Recipient is important in relation to the proposed amendments. Accordingly, in this Consultation Document, we have used the terms Accredited Person and Accredited Data Recipient, as defined in the legislative framework.

[2] Paragraph 15 of **Part D [Project Description]** of the Original CDR PIA report.
[3] For further discussion on when an Accredited Person is an Accredited Data Recipient, please see concept (f) in **Part E [Fundamental Concepts]** of the Original CDR PIA report.

Types of consent in the CDR regime

3.6 The proposed amendments to the CDR Rules include dividing the concept of "consent" into three different categories. These three types of consent include the following:

3.6.1 **Collection Consent**, which is a consent given by a CDR Consumer for an Accredited Person to collect particular CDR Data from a CDR Participant[4] for that CDR Data;

3.6.2 **Use Consent**, which is a consent given by a CDR Consumer for an Accredited Data Recipient of particular CDR Data to use that CDR Data in a particular way; and

3.6.3 **Disclosure Consent**, which is a consent given by a CDR Consumer for an Accredited Data Recipient of particular CDR Data to disclose that CDR Data:

(a) to an Accredited Person in response to a Consumer Data Request (**AP Disclosure Consent**);

(b) to a Trusted Advisor of the CDR Consumer (**TA Disclosure Consent**);

(c) where the CDR Data is an insight[5] (**CDR Insight**) (**Insight Disclosure Consent**); or

(d) to an Accredited Person for the purposes of direct marketing.

3.7 In addition, the proposed amendments to the CDR Rules categorise the above types of consents, as follows:

3.7.1 Collection Consents;

3.7.2 Use Consents relating to the goods or services requested by the CDR Consumer;

3.7.3 Use Consents and Disclosure Consents relating to CDR Insights;

3.7.4 Use Consents and Disclosure Consents relating to direct marketing;

3.7.5 Use Consents to de-identify some or all of the collected CDR Data for the purpose of disclosing (including by selling) the de-identified data;

3.7.6 Use Consents relating to general research;

3.7.7 AP Disclosure Consents; and

3.7.8 TA Disclosure Consents.

3.8 We understand that an Accredited Person must, when asking a CDR Consumer for their consent, allow a CDR Consumer to provide their express consent to each of the following choices for each category of consent:

3.8.1 the types of CDR Data to which the consent will apply (for Collection Consents and Disclosure Consents):

3.8.2 the specific uses of collected CDR Data to which they are consenting (for Use Consents);

[4] A CDR Participant for CDR Data is a Data Holder, or an Accredited Data Recipient, of the CDR Data (section 56 AL of the CC Act).

[5] See paragraph 7.3 of this of this **Part B [Project Description]** for further information on CDR Insights**.**

3.8.3 the period of the Collection Consent, Use Consent, or Disclosure Consent; and

3.8.4 the person to whom CDR Data may be disclosed (for Disclosure Consents).

3.9 The CDR Rules currently refer to 'consent', which collectively refers to collection and uses of CDR Data (as captured by the new definitions of Collection Consent, and Use Consent). The concept of Disclosure Consent is new for the CDR Regime, as it will facilitate an Accredited Data Recipient being able to disclose CDR Data to new categories of persons.

Requirements when asking for CDR Consumer's Disclosure Consent

3.10 The proposed amendments contain new requirements that an Accredited Person must comply with when asking for a CDR Consumer's Disclosure Consent.

3.11 The proposed amendments specify that an Accredited Person must not ask a CDR Consumer to give a Disclosure Consent in relation to CDR Data unless the CDR Consumer has already given the Collection Consent and Use Consent required to collect, and where relevant, derive the CDR Data to be disclosed.[6]

3.12 When a CDR Consumer provides a Disclosure Consent, the Accredited Person must allow the CDR Consumer to:

3.12.1 actively select the particular types of CDR Data to which the Disclosure Consent applies; and

3.12.2 choose the period of this Disclosure Consent; and

3.12.3 select the person to whom the CDR Data may be disclosed.

3.13 The proposed amendments to the CDR Rules also specify that if the Accredited Person charges the CDR Consumer a fee for disclosure of CDR Data, the Accredited Person must, when asking for the CDR Consumer's consent:

3.13.1 clearly distinguish between the CDR Data (if any) for which a fee will be charged and the CDR Data (if any) for which a fee will not be charged; and

3.13.2 allow the CDR Consumer to actively select or otherwise clearly indicate whether they consent to the disclosure of the CDR Data (if any) for which a fee will be charged.

3.14 In addition, if the Accredited Person intends to charge a fee for the disclosure of the CDR Consumer's CDR Data, the Accredited Person must specify the fee amount and the consequences if the CDR Consumer does not consent to the disclosure of that data.

3.15 The proposed amendments to the CDR Rules provide that an Accredited Person's processes for asking a CDR Consumer to give or amend a Disclosure Consent is not required to accord with the Data Standards.

[6] This does not prevent the Accredited Person from asking for a Disclosure Consent in relation to CDR Data that has yet to be collected or derived.

Amendment of a CDR Consumer's Collection Consent, Use Consent or Disclosure Consent

3.16 The current CDR Rules do not permit a CDR Consumer to amend their consent.

3.17 The proposed amendments to the CDR Rules will permit a CDR Consumer to, at any time, amend any consents they have provided to an Accredited Person through the Accredited Person's Consumer Dashboard.[7] An amendment to a CDR Consumer's consent takes effect when the CDR Consumer amends their consent (and a CDR Consumer cannot specify a different day or time for this date of effect).

Accredited Person invites CDR Consumer to amend consent

3.18 The Accredited Person may also invite a CDR Consumer to amend their consent via the Accredited Person's Consumer Dashboard, or in writing directly to the CDR Consumer, if:

3.18.1 the amendment would better enable the Accredited Person to provide the goods or services requested by the CDR Consumer; or

3.18.2 the amendment would:

(a) be consequential to an agreement between the Accredited Person and the CDR Consumer to modify those requested goods or services; and

(b) enable the Accredited Person to provide the modified goods or services.

3.19 If an Accredited Person invites a CDR Consumer to amend the validity period of their current consent, they must not:

3.19.1 give the invitation more than a reasonable period before the current consent is expected to expire; or

3.19.2 give more than a reasonable number of such invitations within this period.

Process for amending consent

3.20 For the purposes of amending a consent, the Accredited Person may present the CDR Consumer with pre-selected options. These pre-selection options will reflect the following details of the CDR Consumer's current consent:

3.20.1 the types of CDR Data to which the consent applies;

3.20.2 the specific uses of the CDR Data;

3.20.3 the validity period of the consent;

3.20.4 any persons to whom CDR Data may be disclosed; and

3.20.5 if the CDR Consumer has elected to the deletion of their redundant data.

[7] We note that the proposed amendments, as currently drafted, also require an Accredited Person to allow a CDR Consumer to amend a consent in the same manner that it asks for a CDR Consumer to give a consent, which overlap with the requirements for this amendment to occur through the Accredited Person's Consumer Dashboard.

3.21 When a CDR Consumer amends their consent, the Accredited Person must give the CDR Consumer:

3.21.1 a statement that indicates the consequences of amending the consent; and

3.21.2 a statement that the Accredited Person will be able to continue to use any CDR Data that has already been disclosed to it to the extent allowed by the amended consent.

3.22 The proposed amendments to the CDR Rules broaden the definitions of authorisation and consent to include any amended authorisation or consent.

Expiry of Consumer Data Request, consent and authorisation

Withdrawal of authorisation

3.23 If an Accredited Person is notified by the Data Holder that the CDR Consumer's authorisation has been withdrawn, and the Collection Consent has not expired, the Collection Consent expires when the Accredited Person receives this notification from the Data Holder.

3.24 This notification from the Data Holder would not cause the expiry of any Use Consents in relation to CDR Data already collected. However, the Accredited Person would need to notify the CDR Consumer of this fact (as specified in paragraphs 3.28 to 3.29 of this **Part B [Project Description]**).

Revocation or surrender of accreditation

3.25 If an Accredited Person's accreditation is revoked or surrendered, all of their Collection Consents, Use Consents and Disclosure Consents expire when the revocation or surrender takes effect.

Amendment of consent validity period

3.26 As discussed in the Original CDR PIA report[8], a CDR Consumer's consent expires if a particular event occurs. The proposed amendments to the CDR Rules expands on one of those situations to provide that, if the CDR Consumer has amended the validity period of their consent, that consent expires 12 months after the consent was amended (unless a listed event occurs earlier).

Amendment of authorisation validity period

3.27 Similarly, the proposed amendments to the CDR Rules will mean that if a CDR Consumer has amended the validity period of their authorisation, that authorisation expires at the end of the amended validity period (unless a listed event occurs earlier).

Notification to CDR Consumer if Collection Consent expires, but Use Consent does not

3.28 If a CDR Consumer's Collection Consent expires, but their Use Consent does not, the Accredited Person must notify the CDR Consumer that they may, at any time:

3.28.1 withdraw the Use Consent; and

3.28.2 make the election to delete redundant data in respect of that CDR Data.

[8] See paragraphs 15.30-15.31 of **Part D [Project Description]** in the Original CDR PIA report for further information.

3.29 This Accredited Person may provide this notification:

3.29.1 via its Consumer Dashboard; or

3.29.2 in writing directly to the CDR Consumer.

Notification if Collection Consent for CDR Data is amended

3.30 If a CDR Consumer amends their Collection Consent provided to an Accredited Person, the Accredited Person must then notify:

3.30.1 if the Collection Consent is in relation to a Data Holder Request, the Data Holder; and

3.30.2 if the Collection Consent is in relation to an Accredited Data Recipient Request, the other Accredited Data Recipient.

3.31 If a Data Holder receives a notification that the CDR Consumer's Collection Consent has been amended (as specified in 3.30.1), the Data Holder must invite the CDR Consumer to amend their authorisation to disclose CDR Data. The Data Holder must, when inviting the CDR Consumer to amend their authorisation, comply with the CDR Rules that apply to asking a CDR Consumer to give authorisation to disclose CDR Data.

3.32 The proposed amendments also require the Data Holder to, when asking a CDR Consumer to authorise the disclosure of CDR Data or amend a current authorisation, give a CDR Consumer any information the Accreditation Register holds in relation to the Accredited Person (we understand the intention is that this may require provision of information about specific goods and services).

Ongoing notification requirement for Collection Consents and Use Consents

3.33 Requirements in relation to notification of current Collection Consents and Use Consents will be amended, to reflect that if 90 days have elapsed since the latest of several situations (including, as introduced by the proposed amendments, since the CDR Consumer gave their consent, or the CDR Consumer last amended their consent), the Accredited Person must notify the CDR Consumer that their Collection Consent and/or Use Consent (as relevant) is current.

Information provided to CDR Consumers in relation to their consents

3.34 CDR Consumers are provided with information on their consents in many forms in the CDR regime. Due to many of the changes mentioned above, the proposed amendments also include changes to the information with which a CDR Consumer must be provided. These sources of information have been grouped, as follows:

3.34.1 information provided to CDR Consumers when they provide any consent;

3.34.2 information on an Accredited Person's Consumer Dashboard;

3.34.3 information included in a CDR receipt; and

3.34.4 information contained in an Accredited Data Recipient's CDR Policy.

3.35 We have discussed these stages separately below.

Information provided to CDR Consumers when they give any consent

3.36 As discussed above, the proposed amendments to the CDR Rules require additional information to be provided to CDR Consumers when they are asked to provide their consent (including to reflect other changes made in the proposed amendments, such as the introduction of Disclosure Consents).

3.37 In addition, when an Accredited Person asks a CDR Consumer to provide a Collection Consent or a Use Consent, the Accredited Person must specify how the collection, or use, complies with the data minimisation principle, including how:

3.37.1 for Collection Consents, that collection is reasonably needed, and relates to no longer a time period than is reasonably needed; and

3.37.2 for Use Consents, that use would not go beyond what is reasonably needed,

in order to provide the goods or services to the CDR Consumer, or make the other uses the CDR Consumer has consented to (such as for the purposes of general research).

Information on an Accredited Person's Consumer Dashboard

3.38 The CDR Rules, as currently drafted, contain requirements for an Accredited Person to provide CDR Consumer's with a Consumer Dashboard that meets the requirements specified in the CDR Rules. As noted in the Original CDR PIA report[9], the CDR Rules provide that the Consumer Dashboard must have several functionalities, and contain certain pieces of information prescribed in the CDR Rules. Given the changes being proposed to the CDR Rules (as noted above), the proposed amendments also amend the requirements for an Accredited Person's Consumer Dashboard.

3.39 The proposed amendments include requiring the Accredited Person's Consumer Dashboard to have a functionality that allows a CDR Consumer, at any time, to amend or withdraw any current Collection Consents, Use Consents or Disclosure Consents.

3.40 Further, the proposed amendments will require an Accredited Person's Consumer Dashboard to also contain the following details in relation to particular consents given by the CDR Consumer:

3.40.1 for Collection Consent or Disclosure Consent, if the consent applies over a period of time:

(a) what that period is; and

(b) how often the data has been, and is expected to be, collected or disclosed over that period;

3.40.2 for an Insight Disclosure Consent, a description of each CDR Insight disclosed, to whom it was disclosed, and when it was disclosed; and

3.40.3 details of each amendment that has been made to the consent.

[9] For further information, please see paragraph 15.17-15.18 of **Part D [Project Description]** in the Original CDR PIA report.

3.41 The proposed amendments will require an Accredited Data Recipient (i.e. an Accredited Person who becomes an Accredited Data Recipient upon collection of CDR Data) to update their Consumer Dashboard to[10]:

3.41.1 in relation to collection of CDR Data, indicate the CDR Participant[11] from which the Accredited Person collected the CDR Data; and

3.41.2 in relation to disclosure of CDR Data, indicate:

(a) what CDR Data was disclosed;

(b) when the CDR Data was disclosed; and

(c) the Accredited Person to whom the CDR Data was disclosed, identified in accordance with any entry on the Accredited Register specified as being for that purpose.

Information included in a CDR receipt

3.42 As detailed in the Original CDR PIA report[12], the CDR Rules, as currently drafted, contain requirements for an Accredited Person to give a CDR Consumer a CDR receipt. The proposed amendments specify that this CDR receipt must be provided as soon as practicable after the CDR Consumer gives, amends, or withdraws, a Collection Consent, a Use Consent or a Disclosure Consent.

3.43 The proposed amendments clarify that a CDR receipt must set out, in the case of:

3.43.1 a Collection Consent, the name of each CDR Participant the CDR Consumer has consented to the collection of CDR Data from; and

3.43.2 a Disclosure Consent, the name of the person the CDR Consumer has consented to the disclosure of CDR Data to.

3.44 A CDR receipt given for an amendment of a consent must set out details of each amendment that has been made to the consent.

Information contained in an Accredited Data Recipient's CDR Policy

3.45 Under the current CDR Rules an Accredited Data Recipient must have a CDR Policy, which must contain several pieces of information.[13] The proposed amendments will also require an Accredited Data Recipient's CDR Policy to contain, if the Accredited Data Recipient wishes to undertake general research using the CDR Data:

3.45.1 a description of the research; and

3.45.2 a description of any additional benefit to the CDR Consumer for consenting to the use of their CDR Data.

[10] The proposed amendments for lower levels of accreditation contain additional Rules about updating Consumer Dashboards. See paragraphs 8.14 to 8.16, and 8.39.2 to 8.39.3, of this **Part B [Project Description]**.
[11] The Data Holder for a Data Holder Request, or Accredited Data Recipient for an Accredited Data Recipient Request (as relevant).
[12] For further information, please see paragraph 15.15-15.16 of **Part D [Project Description]** in the Original CDR PIA report.
[13] Please see the table in **Part F [Analysis of APP Application and Compliance]** in the Original CDR PIA report for further information on the requirements for a CDR Policy, and the information required to be contained in that CDR Policy.

Other relevant matters

3.46 Under the current CDR Rules, an Accredited Person may not ask a CDR Consumer for consent to:

3.46.1 sell the CDR Data that it receives under the CDR regime; and

3.46.2 aggregate CDR Data for the purposes of identifying, compiling insights in relation to, or building a profile in relation to, any person who is not the CDR Consumer who made the Consumer Data Request.[14]

3.47 The proposed amendments to the CDR Rules amend these restrictions, by:

3.47.1 removing the restriction on an Accredited Person asking for consent to sell CDR Data; and

3.47.2 including a restriction that an Accredited Person must not ask a CDR Consumer for consent that is not in a category of consents (i.e. the consent must fall into one of the categories specified in paragraph 3.7 of this **Part B [Project Description]**).

Use and Disclosure of CDR Data for the purposes of general research

3.48 The proposed amendments to the CDR Rules introduce a concept of permitting an Accredited Data Recipient to:

3.48.1 use CDR Data for the purposes of general research, in accordance with a current Use Consent for that purpose from the CDR Consumer; and

3.48.2 for the purposes of general research, disclose to the CDR Consumer any of their CDR Data.

3.49 General research is defined as research by the Accredited Data Recipient that does not relate to the provision of goods or services to any particular CDR Consumer.

3.50 In addition to the matters a CDR Consumer is asked to provide their consent to, the proposed amendments require an Accredited Person to ask for the CDR Consumer's express Use Consent for the purposes of any general research the Accredited Person intends to undertake, and must provide a link to a description in the Accredited Person's CDR Policy of:

3.50.1 the research to be conducted; and

3.50.2 any additional benefit to the CDR Consumer for consenting to the use of their CDR Data.

Use of CDR Data for the purposes of de-identifying the data

3.51 As described above, a category of consent includes where an Accredited Person may ask a CDR Consumer to provide a Use Consent to de-identify some or all of the collected CDR Data for the purpose of disclosing (including by selling) the de-identified data. Accordingly, the proposed amendments permit the Accredited Data Recipient to use the CDR Consumer's CDR Data for the purposes of de-identifying collected CDR Data for the purposes of disclosing (including by selling) the de-identified data.

[14] As noted in the Original CDR PIA report, the CDR Rules specify some situations in which this restriction does not apply (see paragraph 15.12 of **Part D [Project Description]** in the Original CDR PIA report for further information).

Uses and Disclosures relating to direct marketing

3.52 In accordance with a CDR Consumer's direct marketing Use Consent and/or Disclosure Consent, an Accredited Data Recipient may:

3.52.1 send to the CDR Consumer information about other goods or services provided by another Accredited Person, if the Accredited Data Recipient:

(a) reasonably believes that the CDR Consumer might benefit from those other goods or services; and

(b) sends such information to the CDR Consumer on no more than a reasonable number of occasions; and

3.52.2 disclose CDR Data to an Accredited Person to enable the Accredited Person to provide the goods and services specified in paragraph 3.51.1 of this **Part B [Project Description]**, if the CDR Consumer has:

(a) given the Accredited Person:

(i) a Collection Consent to collect the CDR Data from the Accredited Data Recipient; and

(ii) a Use Consent; and

(b) given the Accredited Data Recipient a Disclosure Consent to disclose the CDR Data to the Accredited Person.

Records to be kept and maintained

Data Holder

3.53 In addition to the requirements of the CDR Rules as currently drafted, the proposed amendments to the CDR Rules require a Data Holder to keep and maintain records that record and explain:

3.53.1 amendments to authorisations to disclose CDR Data;

3.53.2 instances where the Data Holder has refused to disclose requested CDR Data and the Rule or Data Standard relied upon in refusing to disclose the CDR Data; and

3.53.3 the processes (including a video of each process) by which the Data Holder asks CDR Consumers:

(a) for their authorisation to disclose CDR Data; and

(b) for an amendment to their authorisation.

Accredited Data Recipient

3.54 In addition to the requirements of the CDR Rules as currently drafted, the proposed amendments to the CDR Rules require an Accredited Data Recipient to keep and maintain records that record and explain:

3.54.1 all consents, including, if applicable, the uses of the CDR Data that the CDR Consumer has consented to under any Use Consents;

3.54.2 amendments to consents by CDR Consumers;

3.54.3 the fact that CDR Data has been disclosed to Accredited Persons, and the identity of Accredited Persons to whom any CDR Data was disclosed;

3.54.4 the fact that CDR Data has been disclosed to Trusted Advisors, and the identity of Trusted Advisors to whom CDR Data was disclosed;

3.54.5 disclosures of CDR Insights, including a description of each CDR Insight disclosed, to whom it was disclosed and when;

3.54.6 the processes (including a video of each process) by which the Accredited Data Recipient asks CDR Consumers:

(a) for their consent; and

(b) for an amendment to their consent; and

3.54.7 any terms and conditions on which the Accredited Data Recipient offers goods or services, where the Accredited Data Recipient discloses to an Accredited Person, CDR Data in order to provide the good or service.

4. AP Disclosure Consent (and Accredited Data Recipient Requests)

Types of Consumer Data Requests

4.1 Currently, the CDR Rules provide for a Consumer Data Request to be made by an Accredited Person to a Data Holder. The proposed amendments to the CDR Rules will permit an Accredited Person to make a Consumer Data Request to an Accredited Data Recipient. In summary, this means that a CDR Consumer can:

4.1.1 request an Accredited Person to collect their CDR Data from a Data Holder (who, after receiving CDR Data, will become an Accredited Data Recipient) (**Data Holder Request**); and

4.1.2 request an Accredited Person (A2) to collect their CDR Data from an Accredited Data Recipient (A1) (who, after receiving CDR Data, will also become an Accredited Data Recipient) (**Accredited Data Recipient Request**).

4.2 The concept of an Accredited Data Recipient request, as described in paragraph 4.1.2, is a new concept included in the proposed amendments to the CDR Rules, and is linked to the new concept of Disclosure Consent, as specified above in paragraph 3.7.

4.3 To accommodate the new concept of Accredited Data Recipient Requests, the proposed amendments to the CDR Rules have broadened the language used in relation to Consumer Data Requests to include collection of CDR Data from Accredited Data Recipients (as well as Data Holders). Accordingly, a number of the proposed amendments to the CDR Rules relate to expanding the language from collecting CDR Data from a Data Holder, to collecting CDR Data from CDR Participants (which, as noted above, includes Data Holders and Accredited Data Recipients of the CDR Data).

Valid Consumer Data Request

4.4 The CDR Rules in relation to valid Consumer Data Requests have been amended to reflect that division of the concept of 'consent' into Collection Consent, Use Consent, and Disclosure Consent. This includes specifying that an Accredited Person may ask a CDR Consumer to give the following consents, in order to provide goods and services to the CDR Consumer:

4.4.1 a Collection Consent for the Accredited Person to collect their CDR Data from the CDR Participant[15]; and

4.4.2 a Use Consent for the Accredited Person to use that CDR Data.

Data Holder Request

4.5 The proposed amendments to the CDR Rules do contain some changes to the Rules in relation to Data Holder Requests, however a majority of these amendments are clarification of language (i.e. to reflect that 'consent to collect and use CDR Data' is now, under the proposed amendments, Collection Consent and Use Consent). Given these changes are not substantive, but more clarification of language, we have not discussed them in this PIA Update report.

4.6 The only substantive change to Data Holder Requests is the fact that an Accredited Person may send a Data Holder Request if, among other things, the request is valid (noting the language previously used was 'the consent is current').

Accredited Data Recipient Request and AP Disclosure Consent

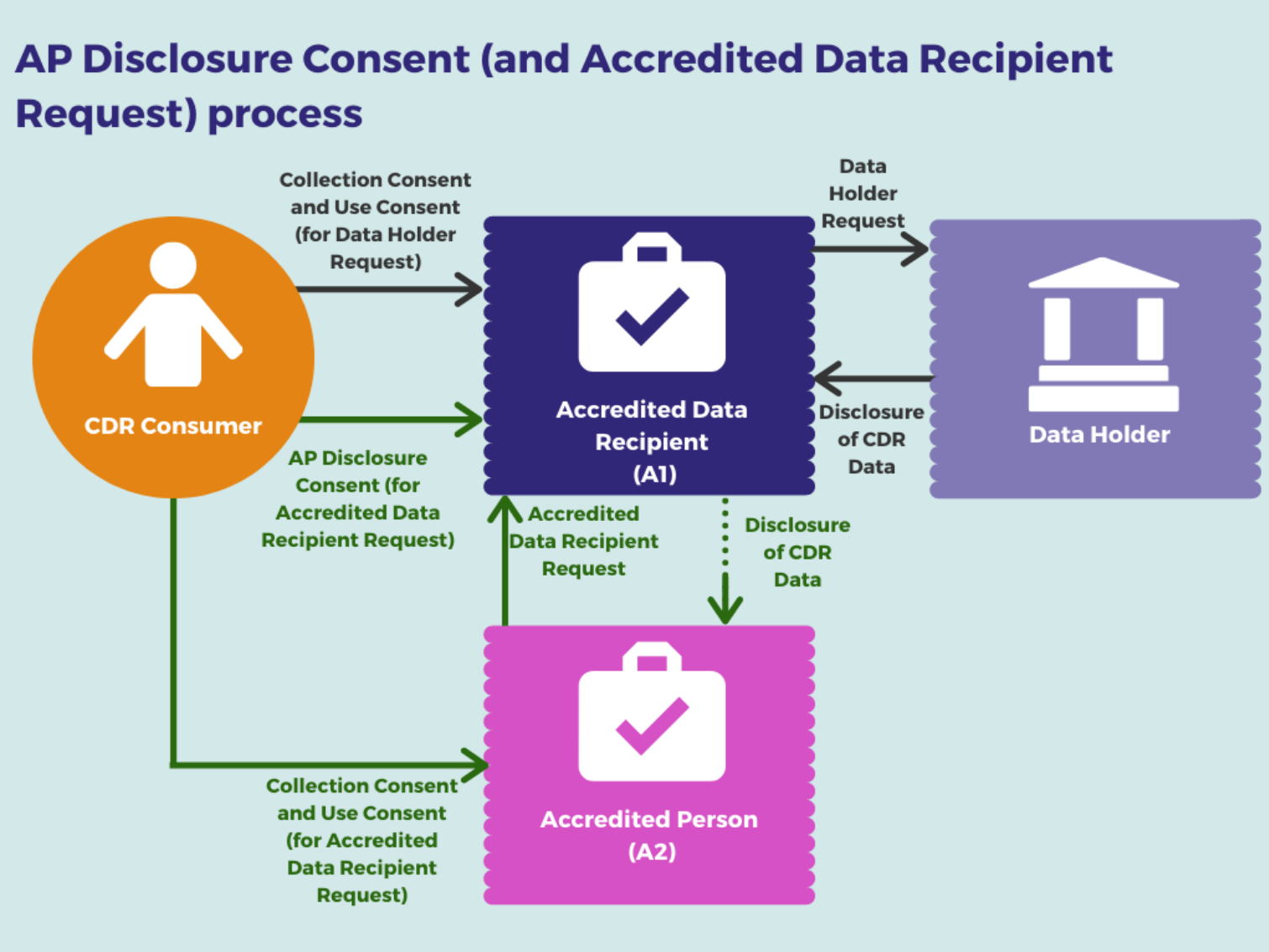
4.7 The proposed amendments to the CDR Rules introduce a concept of Accredited Data Recipient Requests, which are requests made by an Accredited Person (**A2**) to an Accredited Data Recipient (**A1**). For clarity, the Accredited Person is not an Accredited Data Recipient until they collect the CDR Consumer's CDR Data from either:

4.7.1 a Data Holder under a Data Holder Request; or

4.7.2 an Accredited Data Recipient under an Accredited Data Recipient Request.

4.8 Given the complexities of the AP Disclosure Consent process (and the Accredited Data Recipient Request process), we have set out below a diagram illustrating this new information flow, together with a description of each stage in the process.

[15] The Data Holder for a Data Holder Request, or Accredited Data Recipient for an Accredited Data Recipient Request (as relevant).


AP Disclosure Consent (and Accredited Data Recipient Request) process
Collection Consent and Use Consent (for Data Holder Request)
Data Holder Request
CDR Consumer
Accredited Data Recipient (A1)
Data Holder
Disclosure of CDR Data
AP Disclosure Consent (for Accredited Data Recipient Request)
Accredited Data Recipient Request
Disclosure of CDR Data
Collection Consent and Use Consent (for Accredited Data Recipient Request)
Accredited Person (A2)

CDR Consumer provides AP Disclosure Consent to Accredited Person (A1) when providing Collection Consent and Use Consent for Data Holder Request (optional)

4.9 In addition to a CDR Consumer providing their Collection Consent and Use Consent to an Accredited Person (A1) for a Data Holder Request, the CDR Consumer may also provide an AP Disclosure Consent to the Accredited Person (A1).

4.10 As discussed in paragraph 3.12 of this **Part B [Project Description]**, the CDR Consumer will be able to make several choices when providing their AP Disclosure Consent.

4.11 If a CDR Consumer provides an AP Disclosure Consent at this stage, the CDR Consumer will be able to select the Accredited Person (A2) to whom the Accredited Data Recipient (A1) may disclose their CDR Data.

4.12 If the Accredited Data Recipient (A1) intends to charge the CDR Consumer a fee for the disclosure, the Accredited Data Recipient (A1) must provide the information specified in paragraphs 3.13 to 3.14 of this **Part B [Project Description]** to the CDR Consumer.

CDR Consumer provides Collection Consent and Use Consent to Accredited Person (A2) for Accredited Data Recipient Request

4.13 The CDR Consumer has the opportunity to, similar to a Data Holder Request, provide a Collection Consent and Use Consent to the Accredited Person (A2) for the Accredited Person (A2) to collect CDR Data from an Accredited Data Recipient (A1), and for the Accredited Person (A2) to use that CDR Data. As is the case when seeking consent for the purposes of a Data Holder Request, the Accredited Person (A2) has to provide the CDR Consumer with a range of information in relation to their Collection Consent and Use Consent.

4.14 The proposed amendments to the CDR Rules also broaden the concept of charging for the collection of CDR Data to apply to Accredited Data Recipient Requests, specifying that if the Accredited Data Recipient (A1) charges a fee for disclosure of CDR Data to the Accredited Person (A2), and the Accredited Person (A2) intends to pass that fee onto the CDR Consumer, the Accredited Person (A2) must, when asking for the CDR Consumer's consent:

4.14.1 clearly distinguish between the CDR Data (if any) for which a fee will be passed on and the CDR Data (if any) for which a fee will not be passed on; and

4.14.2 allow the CDR Consumer to actively select or otherwise clearly indicate whether they consent to the disclosure of the CDR Data (if any) for which a fee will be passed on.

4.15 In addition, if the Accredited Person (A2) intends to pass on a fee to the CDR Consumer, the Accredited Person (A2) must specify the amount of the fee, and the consequences if the CDR Consumer does not consent to the collection of that data.

4.16 The proposed amendments to the CDR Rules provide that an Accredited Person's processes for asking a CDR Consumer to give and amend their Collection Consent for the purposes of an Accredited Data Recipient Request is not required to accord with the Data Standards.

Accredited Person (A2) makes Accredited Data Recipient Request to Accredited Data Recipient (A1)

4.17 The Accredited Person (A2) may make an Accredited Data Recipient Request to an Accredited Data Recipient (A1) for the Accredited Data Recipient (A1) to disclose some or all of the CDR Data that:

4.17.1 is the subject to the relevant Collection Consent and Use Consent provided to the Accredited Person (A1); and

4.17.2 it is able to collect and use in accordance with the data minimisation principle.

Accredited Data Recipient (A1) asks CDR Consumer for AP Disclosure Consent (if the Disclosure Consent is not already provided) (optional)

4.18 An Accredited Data Recipient (A1) may ask a CDR Consumer for an AP Disclosure Consent in relation to an Accredited Person (A2) (in accordance with the relevant CDR Rules), if:

4.18.1 the Accredited Data Recipient (A1) receives an Accredited Data Recipient Request from an Accredited Person (A2);

4.18.2 the Accredited Data Recipient (A1) does not have a current AP Disclosure Consent from the CDR Consumer to disclose the CDR Consumer's CDR Data to that Accredited Person (A2) (i.e. the CDR Consumer did not provide an AP Disclosure Consent at the stage specified in paragraphs 4.9 to 4.12 of this **Part B [Project Description]**); and

4.18.3 the Accredited Data Recipient (A1) reasonably believes that the Accredited Data Recipient Request was made by an Accredited Person on behalf an eligible CDR Consumer.

Accredited Data Recipient (A1) discloses CDR Data to Accredited Person (A2) (optional)

4.19 If the CDR Consumer provides their AP Disclosure Consent, the Accredited Data Recipient (A1) is authorised, but is not required to, disclose the CDR Consumer's CDR Data to the Accredited Person (A2).

4.20 In summary, the Accredited Data Recipient (A1) can disclose the CDR Data to the Accredited Person (A2) if the CDR Consumer has given:

4.20.1 the Accredited Person (A2):

(a) a Collection Consent to collect the CDR Data from the Accredited Data Recipient (A1); and

(b) a Use Consent; and

4.20.2 the Accredited Data Recipient (A1) an AP Disclosure Consent to disclose the CDR Data to the Accredited Person (A2).

4.21 At this stage, Accredited Person (A2) will become an Accredited Data Recipient under the legislative framework, as the Accredited Person (A2) will meet the definition of an Accredited Data Recipient.

Withdrawal of AP Disclosure Consent

4.22 As is the case in relation to Data Holder Requests, a CDR Consumer can also withdraw the Collection Consent and Use Consent (given to the Accredited Person (A2)) and the AP Disclosure Consent (given to the Accredited Data Recipient (A1)) at any time. In addition to the requirements of the current CDR Rules[16], if the CDR Consumer withdraws their AP Disclosure Consent, the Accredited Data Recipient (A1) must notify the Accredited Person (A2) of the withdrawal.

Expiry of Collection Consent and AP Disclosure Consent

4.23 If:

4.23.1 an Accredited Person (A2) has a Collection Consent to collect particular CDR Data from a particular Accredited Data Recipient (A1); and

4.23.2 the Accredited Data Recipient (A1) has an AP Disclosure Consent to disclose that CDR Data to that Accredited Person (A2),

and one of those consents expires, the other consent expires at the same time.

Notification if Collection Consent or AP Disclosure Consent expires for Accredited Data Recipient Request[17]

4.24 If the Collection Consent an Accredited Person (A2) holds in relation to an Accredited Data Recipient Request expires, they must notify the Accredited Data Recipient (A1) of this expiry.

4.25 If the AP Disclosure Consent an Accredited Data Recipient (A1) holds in relation to an Accredited Data Recipient Request expires, they must notify the Accredited Person (A2) of this expiry.

5. TA Disclosure Consent

5.1 As discussed above, CDR Consumers will be able to provide a TA Disclosure Consent to the disclosure of their CDR Data from an Accredited Person to a Trusted Adviser.

5.2 The following classes of person will be eligible to become Trusted Advisers:

5.2.1 accountants;

5.2.2 lawyers;

5.2.3 tax agents;

5.2.4 BAS agents;

5.2.5 financial advisors;

5.2.6 financial counsellors;

5.2.7 mortgage brokers; and

[16] See paragraphs 15.26 to 15.29 of **Part D [Project Description]** in the Original CDR PIA report for further information.

[17] We note that in the proposed amendments, this Rule is titled "*Notification of collection consent or use consent expires*", however we understand the intention is for the Rule to refer to situations where AP Disclosure Consents expire, rather than Use Consents.

5.2.8 any other class as approved by the ACCC.

5.3 Trusted Advisers will not be Accredited Persons.

5.4 Relevantly, the Accredited Person must not make the following a condition for the supply of the goods or services requested by the CDR Consumer:

5.4.1 the nomination of a Trusted Adviser;

5.4.2 the nomination of a particular person as a Trusted Adviser; or

5.4.3 the giving of a TA Disclosure Consent in respect of a Trusted Adviser.

5.5 However, Accredited Persons may charge CDR Consumers a fee for disclosing their CDR Data to a Trusted Adviser.

5.6 For completeness, we note that the CDR Rules will not regulate:

5.6.1 how CDR Data must be transferred to a Trusted Adviser; or

5.6.2 how a Trusted Adviser must handle that CDR Data.

6. Insight Disclosure Consent

6.1 The proposed amendments to the CDR Rules will allow CDR Consumers to provide an Insight Disclosure Consent to the disclosure of a CDR Insight by an Accredited Data Recipient to a person (**Insight Recipient**).

6.2 The CDR Rules will not seek to limit who can be an Insight Recipient (i.e. anyone can be an Insight Recipient).

6.3 The proposed amendments provide that a CDR Insight, in relation to the CDR Data of a CDR Consumer, means a set of data that:

6.3.1 is derived from the CDR Data;

6.3.2 has an identifier that associates it with the CDR Consumer; and

6.3.3 without that identifier, would be considered to be de-identified for the purposes of the CDR Rules.

6.4 It is intended that CDR Consumers will be able to request, from the Accredited Person, a copy of the CDR Insight about them. It is also possible that CDR Consumers may be able to see the CDR Insight before it is disclosed by the Accredited Person to the Insight Recipient.

7. New levels and kinds of accreditation

General

7.1 Under the current CDR Rules, there is only one level of accreditation (the 'unrestricted level'). However, section 56BH of the CCA Act allows the CDR Rules to provide that accreditations may be granted at different levels corresponding to different risks, including risks associated with specified classes of CDR Data, classes of activities or classes of applicants for accreditation.

7.2 The proposed amendments to the CDR Rules will introduce two new levels of accreditation, being the:

7.2.1 unrestricted level; and

7.2.2 the restricted level.

7.3 There will also be three different kinds of restricted accreditation, being:

7.3.1 data enclave accreditation;

7.3.2 limited data accreditation; and

7.3.3 affiliate accreditation.

7.4 For all applications for accreditation, an applicant will still be required to apply to the Data Recipient Accreditor, and to provide all of the information that is required by the CDR Rules. The Data Recipient Accreditor will still consider the application in accordance with the accreditation criteria specified in the CDR Rules (although different criteria will apply, depending on the relevant level and kind of accreditation).

Data enclave accreditation

7.5 We understand that:

7.5.1 the ACCC's stakeholder consultations have revealed that the cost of demonstrating compliance with the ICT and other systems requirements for handling CDR Data is one of the most significant barriers to a person seeking to be an Accredited Person; and

7.5.2 the proposed amendments are intended to address this barrier by allowing the Data Recipient Accreditor to accredit a person (the **Data Enclave Accredited Person**) to access and use CDR Data by leveraging the ICT and data environment of another person already accredited at the unrestricted level (the **Unrestricted Accredited Person**) whose environment will comply with the requirements of the CDR regime.

Applying for data enclave accreditation

7.6 The accreditation criteria for the data enclave accreditation will remain the same as for an unrestricted level applicant – that is, that the person would, if accredited, be able to comply with the obligations in Rule 5.12. Rule 5.12 will remain substantially the same as is currently the case for unrestricted level applicants, but amended so that the accredited person must:

7.6.1 take all reasonable steps to ensure that it is licensed or otherwise authorised to use any CDR logo as required by the Data Standards;

7.6.2 having regard to the fit and proper person criteria, be a fit and proper person to be accredited "*at the relevant level and kind"*; and

7.6.3 have adequate insurance, or a comparable guarantee, "*appropriate to the level and kind".*[18]

7.7 A person applying for data enclave accreditation will need to specify a proposed '**enclave provider**' in their application and continue to have an enclave provider after being accredited (Rule 5.1B(1)).

7.8 An enclave provider must:

7.8.1 have unrestricted accreditation (i.e., they must be an Unrestricted Accredited Person);

7.8.2 be the provider in a '**CAP arrangement**' with the Data Enclave Accredited Person. A CAP arrangement (short for combined accredited person arrangement) is between two accredited persons, a '**principal'** and a '**provider'**, under which the provider will perform functions on behalf of the principal. In a data enclave CAP arrangement, the Unrestricted Accredited Person will be the provider, who will make consumer data requests for CDR Data and hold the collected CDR Data on behalf of the Data Enclave Accredited Person. The CAP arrangement may also provide for the Unrestricted Accredited Person (the provider) to use or disclose CDR Data on behalf of the Data Enclave Accredited Person (the principal); and

7.8.3 be recorded on the Accreditation Register as the enclave provider of the principal.

7.9 The Data Recipient Accreditor must, if they decide to grant data enclave accreditation, notify the applicant of the name and accreditation number of the enclave provider. The enclave provider must also be entered on the Accreditation Register.

After accreditation

7.10 After accreditation, the Data Enclave Accredited Person, when asking for consent, will be required to tell the CDR Consumer that:

7.10.1 their CDR Data may be, or will be, collected by the provider under a CAP arrangement, and:

7.10.2 the provider's name;

7.10.3 the provider's accreditation number; and

7.10.4 a link to the provider's CDR Policy, with a statement that the CDR Consumer can obtain further information about such collections or disclosures from the CDR policy if desired.

7.11 It appears from the proposed amendments that the Data Enclave Accredited Person will be able to ask the CDR Consumer for consent directly, or by another person acting on behalf of the Data Enclave Accredited Person under a CAP agreement. We understand that the new Rule 4.11(4) is intended to clarify that in both cases the consent is taken to have been requested by, and given to, the Data Enclave Accredited Person.

7.12 A Data Enclave Accredited Person will only be able to make a request for CDR Data, or hold any collected CDR Data (or any data derived from that CDR Data), *"through the enclave provider acting on its behalf under the CAP arrangement"*.

[18] We understand that guidance will be issued about these requirements.

7.13 A Data Enclave Accredited Person's CDR Policy will need to include a list of other Accredited Persons with whom they have a CAP arrangement, the name of the Unrestricted Accredited Person who is the enclave provider, and the nature of the services provided by that provider.

7.14 Disclosing a CDR Consumer's CDR Data to another party to a CAP arrangement (i.e., between the provider and the principal) will be a 'permitted use or disclosure' of the CDR Data, if this is reasonably needed for other permitted uses or disclosures.

7.15 If CDR Data may be collected by a provider under a CAP arrangement, the proposed amendments will require an Accredited Person to ensure that their consumer dashboard includes the provider's name and accreditation number. This means that the consumer dashboard provided by a Data Enclave Accredited Person must contain the name and accreditation number of the Unrestricted Accredited Person (who is the enclave provider).

7.16 Under Privacy Safeguard 5, for the banking sector, an Accredited Person who has collected CDR Data must update their consumer dashboard. The proposed amendments will mean that this Rule will only apply to the provider under the CAP arrangement (i.e., the Unrestricted Accredited Person). The proposed amendments mean that the Unrestricted Accredited Person must indicate on the CDR Consumer's consumer dashboard that their CDR Data was collected *"by an accredited person [i.e., the Unrestricted Accredited Person] on behalf of the accredited person [i.e., the Data Enclave Accredited Person] under a CAP arrangement*".

7.17 Similarly, in relation to Privacy Safeguard 10, the current CDR Rules contain requirements for a Data Holder to update a CDR Consumer's consumer dashboard if they disclose CDR Data to an Accredited Data Recipient. The proposed amendments clarify that if the Data Holder discloses CDR Data to an Accredited Data Recipient (i.e., the Data Enclave Accredited Person) "*through another accredited person action on its behalf under a CAP arrangement"* (i.e. Unrestricted Accredited Person as the enclave provider), only the enclave provider should be listed on the consumer dashboard.

7.18 Under Privacy Safeguard 11, a Data Holder is required to identify to the CDR Consumer the Accredited Person to whom the CDR Data was disclosed. The effect of the proposed amendments is that this requirement only relates to the provider (i.e., the Unrestricted Accredited Person).

7.19 For Privacy Safeguard 12 in relation to redundant data, the current CDR Rules set out steps that must be taken if (among other things) the Accredited Person thinks it appropriate in the circumstances to de-identify rather than delete CDR Data. The proposed amendments will clarify that such a decision must be taken by the principal of a CAP arrangement (i.e., the Data Enclave Accredited Person), who must give certain directions to any provider under the CAP arrangement that *"has been provided with a copy of the redundant data"*.

7.20 An Accredited Data Recipient is required to keep and maintain certain records. The proposed amendments will extend these requirements to include *"any CAP arrangement … in which the accredited data recipient is the principal, including how the provider will use or manage any CDR data shared with it"*.

7.21 There are also some changes to the application of Schedule 2, including a new provision in relation to Part 2.2(7) about implementation and maintenance of a third–party management framework (discussed below in paragraph 7.44 below). The enclave provider (Unrestricted Accredited Person) and the Data Enclave Accredited Person will be required to comply with different requirements of Schedule 2, as indicated in the table below:

Schedule 2 requirement	Unrestricted Accredited Person (also an enclave provider)		Data Enclave Accredited Person must comply
1.1 (Purpose of Part) **and 1.2** (interpretation)	✓		
1.3 (Step 1—Define and implement security governance in relation to CDR data)	✓		✓
1.4 (Step 2—Define the boundaries of the CDR data environment)	✓		✓
1.5 (Step 3—Have and maintain an information security capability)	✓		✓
1.6 (Step 4—Implement a formal controls assessment program)	✓		✓
1.7 (Step 5—Manage and report security incidents)	✓		Paragraphs 1.7(b) and (c) only
	In respect of itself	**In respect of the enclave**	
2.1 (Purpose of Part)	✓		
2.2 (1) (a) to (i) (An accredited data recipient must have processes in place to limit the risk of inappropriate or unauthorised access to its CDR data environment)	✓	✓	✓
2.2 (2) (a) to (e) (An accredited data recipient of CDR data must take steps to secure their network and	✓	Paragraph (d) only (re hardening of end-user devices)	✓

Schedule 2 requirement	Unrestricted Accredited Person (also an enclave provider)		Data Enclave Accredited Person must comply
systems within the CDR data environment).			
2.2 (3) (a) to (c) (An accredited data recipient must securely manage information assets within the CDR data environment over their lifecycle)	✓	✓	
2.2 (4) (a) to (c) (An accredited data recipient must implement a formal vulnerability management program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner)	✓	✓	In relation to the devices the person uses to access the data enclave, or host the network from which it accesses the data enclave
2.2 (5) (a) to (c) (An accredited data recipient must take steps to limit prevent, detect and remove malware in regards to their CDR data environment)	✓	✓	In relation to the devices the person uses to access the data enclave
2.6 (a) to (c) (An accredited data recipient must implement a formal information security training and awareness program for all personnel interacting with CDR data)	✓		✓
2.7 (a) (Third party management)	✓		

7.22 We understand that the changes to Schedule 2 have been developed in accordance with cybersecurity advice obtained by the ACCC.

7.23 A Data Enclave Accredited Person is required to provide annual assurance assessments and attestation reports to the Data Recipient Accreditor, which are less onerous than the similar reports required to be provided by an Unrestricted Accredited Person. The enclave provider (i.e., the Unrestricted Accredited Person) must also provide regular enclave

attestation reports to the Data Recipient Accreditor about the Data Enclave Accredited Person's compliance with Schedule 2.

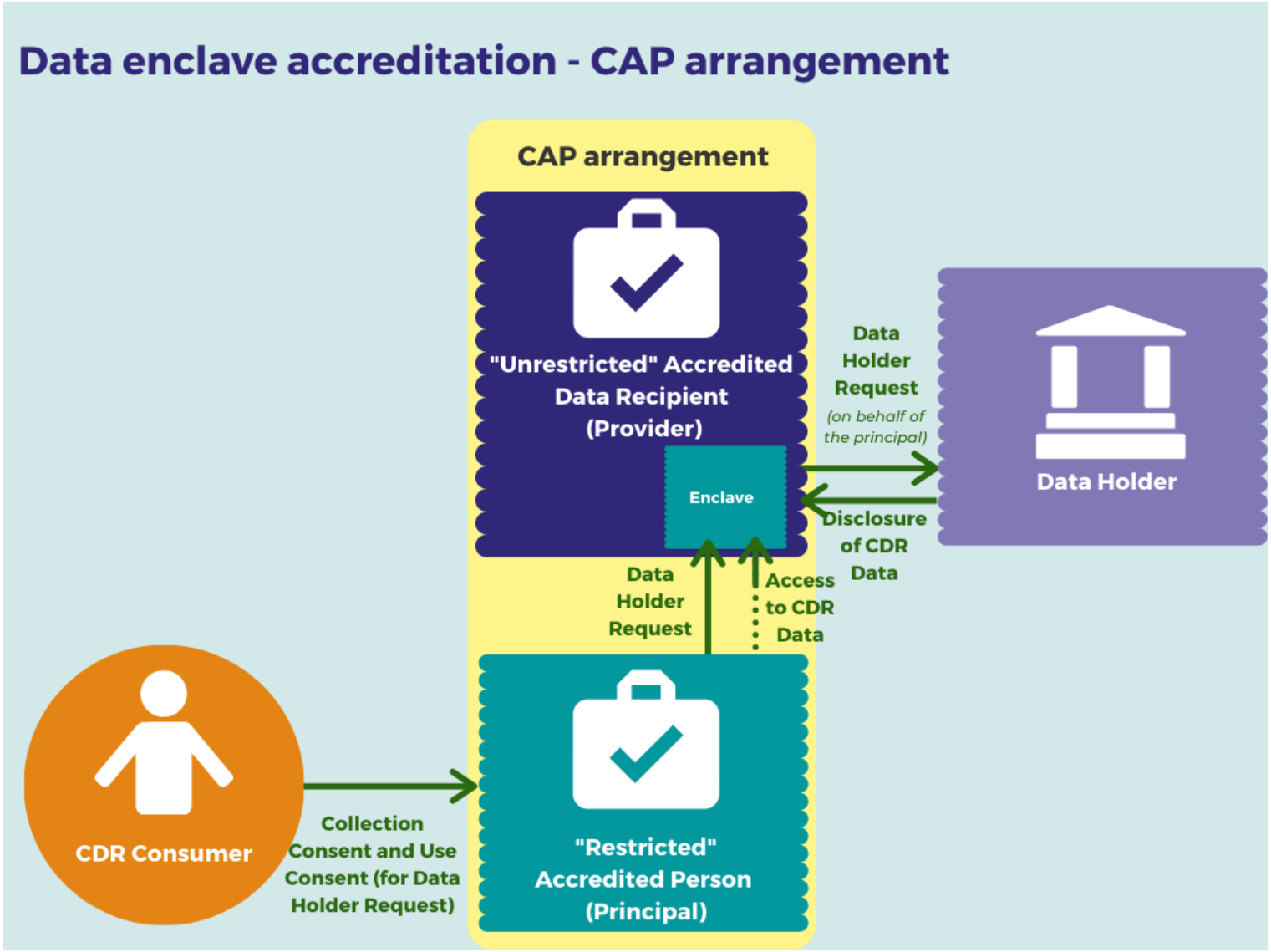
Revocation and suspension of accreditation

7.24 In addition to existing situations for revocation, suspension or surrender of accreditation, an Accredited Person's data enclave accreditation may be suspended or revoked by the Data Recipient Accreditor if the accreditation of the provider in the CAP arrangement (i.e., the Unrestricted Accredited Person) is suspended or revoked.

7.25 Before any revocation, the Data Recipient Accreditor must also notify the enclave provider if the principal's accreditation is being revoked, or the principal if the enclave provider's accreditation is being revoked.

Summary of enclave accreditation process

7.26 To assist with understanding this new process, we have set out below an information flow diagram.


Data enclave accreditation - CAP arrangement
CAP arrangement
"Unrestricted" Accredited Data Recipient (Provider)
Enclave
Data Holder Request (on behalf of the principal)
Disclosure of CDR Data
Data Holder
Data Holder Request
Access to CDR Data
CDR Consumer
Collection Consent and Use Consent (for Data Holder Request)
"Restricted" Accredited Person (Principal)

Limited data accreditation

7.27 As for data enclave accreditation, the criterion for limited data accreditation will be the same as that currently applicable for an unrestricted level applicant. That is, that the person would, if accredited, be able to comply with the obligations in Rule 5.12 (as discussed in paragraph 7.6 above).

7.28 A person with limited data accreditation (**Limited Data Accredited Person**) will only be permitted to collect CDR data of a kind specified in a Schedule to the CDR Rules.

7.29 For the banking sector, the CDR Rules will specify the following kinds of CDR Data as data may be collected by a Limited Data Accredited Person:

7.29.1 "Basic Bank Account Data";

7.29.2 "Basic Customer Data";

7.29.3 "Detailed Bank Account Data";

7.29.4 "Bank Payee Data"; and

7.29.5 "Bank Regular Payments",

with these terms having the same meaning as in the Data Standards. We understand that these categories of CDR Data have been identified as representing 'low' to 'medium' risk categories by the ACCC's ICT security advisers.

7.30 A Limited Data Accredited Person will have substantially the same obligations in relation to the CDR Data environment protections in Schedule 2 of the CDR Rules as an Unrestricted Accredited Person. A Limited Data Accredited Person will only be required to comply with:

7.30.1 all requirements in Part 1 of Schedule 2 (i.e., except for the interpretation clauses in 1.1 and 1.2); and

7.30.2 all requirements in Part 2 of Schedule 2 (except the new Part 2.2(7) in relation to third party management, which is discussed further below in paragraph 7.44).

7.31 After accreditation, the types of CDR Data that a Limited Data Accredited Person will be permitted to handle will be restricted, but a Limited Data Accredited Person will have the same obligations as an Unrestricted Accredited Person in relation to the collection, use and disclosure that CDR Data.

Affiliate accreditation

7.32 The third new kind of restricted accreditation is affiliate accreditation.

Applying for affiliate accreditation

7.33 The proposed amendments introduce new criterion for affiliate accreditation, being that:

7.33.1 the applicant has a '**sponsor**' (as described in paragraph 7.36 below); and

7.33.2 the sponsor certifies that the applicant meets the accreditation criteria (which are the same as for an unrestricted level applicant – as discussed in paragraph 7.6 above).

7.34 This means that there is no requirement for the applicant to demonstrate to the Data Recipient Accreditor that they meet the requirements in Rule 5.12 (including that they are a 'fit and proper person' and have appropriate internal and external dispute resolution processes).

7.35 A person applying for affiliate accreditation must specify a proposed sponsor in their application and, once accredited, must continue to be an affiliate of a sponsor.

7.36 A person applying for affiliate accreditation must specify a proposed sponsor in their application.

7.37 To be a sponsor of an affiliate, a person must:

7.37.1 have unrestricted accreditation (i.e. they must be an Unrestricted Accredited Person);

7.37.2 be recorded on the Accreditation Register as the sponsor of the affiliate; and

7.37.3 agree to take reasonable steps to ensure that the affiliate complies with its obligations as an Accredited Person,

and the affiliate must undertake to provide the sponsor with information and access to its operations as is needed for the sponsor to fulfil its obligations as sponsor.

7.38 Under the proposed amendments to the CDR Rules, sponsors (i.e. the Unrestricted Accredited Person) and affiliates (i.e. the Restricted Accredited Person), will be able to make Consumer Data Requests, and handle CDR Data, in accordance with two different arrangements:

7.38.1 through the process described in paragraph 4 of this **Part B [Project Description]**, in which:

(a) the affiliate receives a Collection Consent and Use Consent from a CDR Consumer for an Accredited Data Recipient Request;

(b) the sponsor receives an AP Disclosure Consent from the CDR Consumer; and

(c) the sponsor then discloses the CDR Data that it holds to the affiliate;

7.38.2 under a CAP arrangement (as described in paragraph 7.8.2 of this this **Part B [Project Description]**), in which:

(a) the affiliate is the principal and the sponsor is the provider;

(b) the sponsor (provider) will do either or both of:

(i) making consumer data requests on behalf of the affiliate; or

(ii) disclosing CDR Data that it holds as an Accredited Data Recipient to the affiliate in response to a consumer data request; and

(c) the sponsor (provider) may also use or disclose CDR Data on behalf of the principal.

7.39 If accreditation is granted to the affiliate, the Data Recipient Accreditor must notify the applicant of the name and accreditation number of the sponsor. It must also ensure the sponsor is included on the Accreditation Register.

After accreditation

7.40 After accreditation, a person with affiliate accreditation (**affiliate**) may only make a consumer data request:

7.40.1 *"through the sponsor acting on its behalf under a CAP arrangement"*; or

7.40.2 to the sponsor (where the sponsor is an Accredited Data Recipient of the CDR Data).

7.41 A sponsor will be required take reasonable steps to ensure that the affiliate complies with its obligations as an Accredited Person.

7.42 As for data enclave arrangements, for affiliate arrangements involving a CAP arrangement:

7.42.1 the affiliate must ensure that their CDR policy contains information in relation to their CAP arrangement with the sponsor, and the sponsor will also be required to include similar information in relation to their CAP arrangement with the affiliate (as described in paragraph 7.13 above);

7.42.2 the Rules in relation to Privacy Safeguard 5 (about updating the consumer dashboard) only apply to the sponsor, who must update their consumer dashboard to show that the CDR Data was collected by the sponsor on behalf of the affiliate under a CAP arrangement (as described in paragraph 7.16 above);

7.42.3 the Rules in relation Privacy Safeguard 10 only apply to the sponsor, and the sponsor should not be listed on the Data Holder's consumer dashboard as the entity to whom the CDR Data has been disclosed (as described in paragraph 7.17 above);

7.42.4 under Privacy Safeguard 11, a Data Holder will only be required to identify to the CDR Consumer the sponsor to whom the CDR Data was disclosed; and

7.42.5 for the purposes of Privacy Safeguard 12 in relation to redundant data, it is the affiliate (i.e., the principal under the CAP arrangement) who must think it appropriate in the circumstances to de-identify rather than delete CDR Data. The affiliate must give certain directions to any sponsor that has been provided with a copy of the redundant data.

7.43 Disclosing a CDR Consumer's CDR Data to another party to a CAP arrangement (i.e., between the sponsor and the affiliate) is a 'permitted use or disclosure' of the CDR Data, if this is reasonably needed for other permitted uses or disclosures.

7.44 Some changes to the requirements in Schedule 2 are also proposed for affiliate accreditation.

7.45 An Unrestricted Accredited Person, who is also a sponsor, must comply with all requirements of Schedule 2. This includes new requirements in Part 2.2(7) about implementation and maintenance of a third–party management framework. This requires management of third parties, including affiliates, in line with a defined third-party management framework (which should include due diligence before establishing new relationships or contracts, contractual arrangements which are reflective of responsibilities for the CDR data and data environment, annual review and assurance activities, reporting requirements and post-contract requirements).

7.46 The requirements to comply with Schedule 2 are summarised in the table below:

Schedule 2 requirement	Unrestricted Accredited Person (also a sponsor)		Affiliate
1.1 (Purpose of Part) **and** 1.2 (interpretation)	✓		✓
1.3 (Step 1—Define and implement security governance in relation to CDR data)	✓		✓
1.4 (Step 2—Define the boundaries of the CDR data environment)	✓		✓
1.5 (Step 3—Have and maintain an information security capability)	✓		✓
1.6 (Step 4—Implement a formal controls assessment program)	✓		✓
1.7 (Step 5—Manage and report security incidents)	✓		✓
	In respect of itself	**In respect of the affiliate**	
2.1 (Purpose of Part)	✓		✓
2.2 (1) (a) to (i) (An accredited data recipient must have processes in place to limit the risk of inappropriate or unauthorised access to its CDR data environment)	✓	Paragraph (i) only (encryption in transit)	✓
2.2 (2) (a) to (e) (An accredited data recipient of CDR data must take steps to secure their network and systems within the CDR data environment).	✓	Paragraph (d) only (re hardening of end-user devices)	✓

Schedule 2 requirement	Unrestricted Accredited Person (also a sponsor)		Affiliate
2.2 (3) (a) to (c) (An accredited data recipient must securely manage information assets within the CDR data environment over their lifecycle)	✓		✓
2.2 (4) (a) to (c) (An accredited data recipient must implement a formal vulnerability management program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner)	✓		✓
2.2 (5) (a) to (c) (An accredited data recipient must take steps to limit prevent, detect and remove malware in regard to their CDR data environment)	✓		✓
2.6 (a) to (c) (An accredited data recipient must implement a formal information security training and awareness program for all personnel interacting with CDR data)	✓		✓
2.7 (a) (Third party management)	✓	✓	

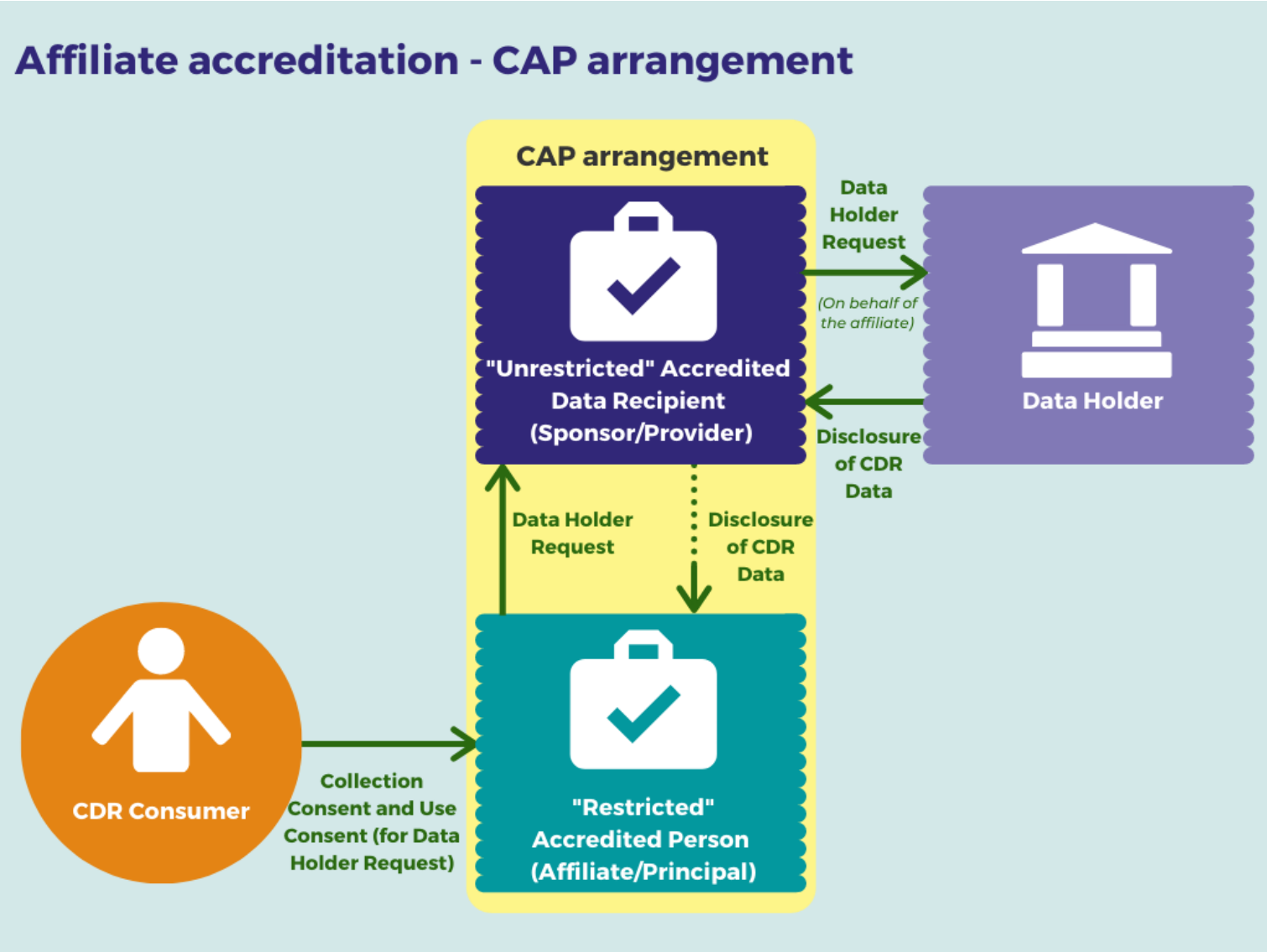
Revocation and suspension of accreditation

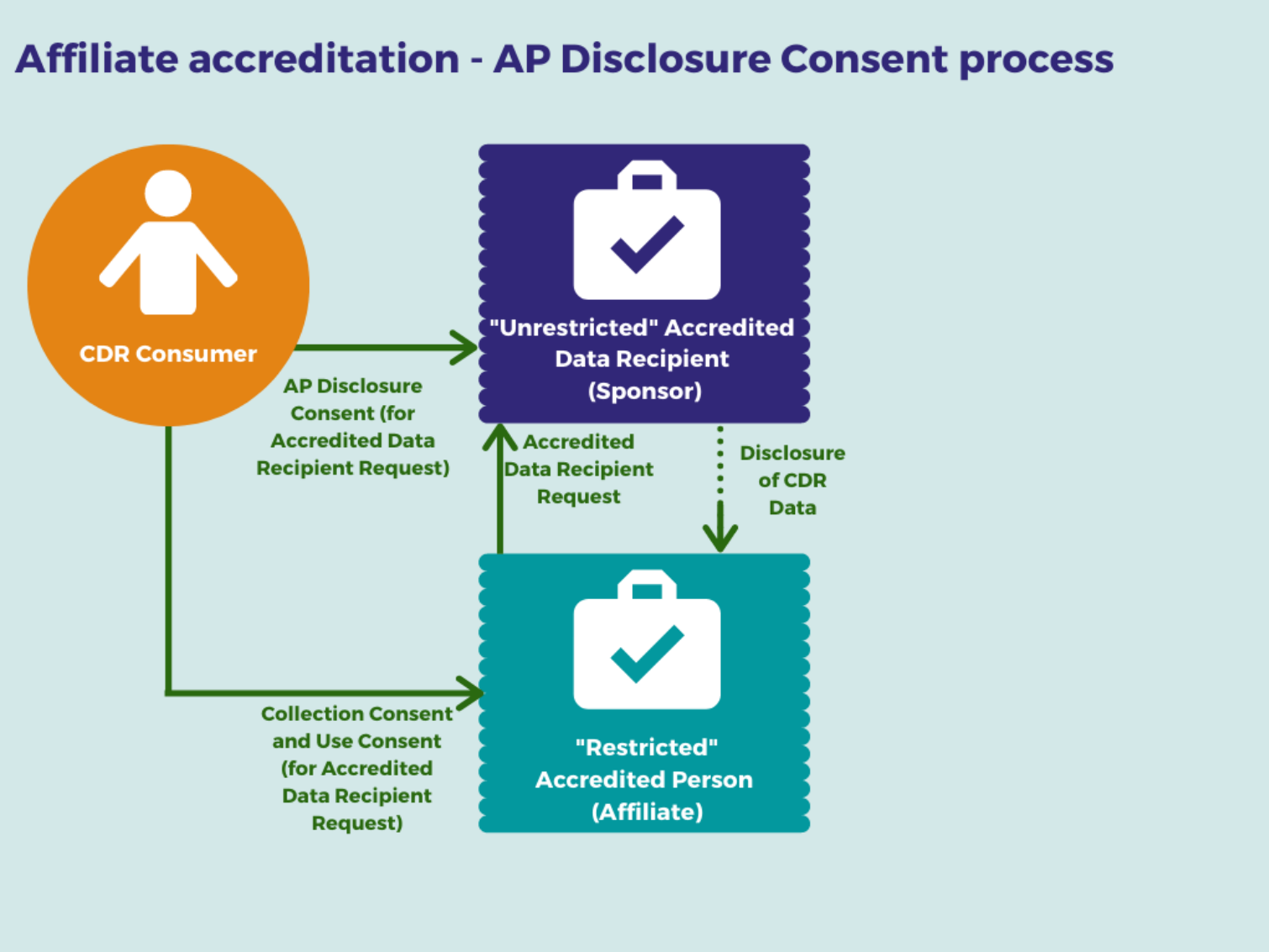
7.47 In addition to existing situations for revocation, suspension or surrender of accreditation, affiliate accreditation may be suspended or revoked by the Data Recipient Accreditor if the accreditation of the Accredited Person's sponsor is suspended or revoked.

7.48 Before any revocation of the sponsor's accreditation, the Data Recipient Accreditor must also notify the affiliate. Similarly, before any revocation of the affiliate's accreditation, the Data Recipient Accreditor must notify the sponsor.

Summary of affiliate accreditation process

7.49 To assist with understanding this new process, we have set out below information flow diagrams (one for where there is a CAP arrangement, and one involving AP Disclosure Consents).


Affiliate accreditation - CAP arrangement
CAP arrangement
"Unrestricted" Accredited Data Recipient (Sponsor/Provider)
Data Holder Request
(On behalf of the affiliate)
Disclosure of CDR Data
Data Holder
Data Holder Request
Disclosure of CDR Data
CDR Consumer
Collection Consent and Use Consent (for Data Holder Request)
"Restricted" Accredited Person (Affiliate/Principal)


Affiliate accreditation - AP Disclosure Consent process
CDR Consumer
"Unrestricted" Accredited Data Recipient (Sponsor)
AP Disclosure Consent (for Accredited Data Recipient Request)
Accredited Data Recipient Request
Disclosure of CDR Data
Collection Consent and Use Consent (for Accredited Data Recipient Request)
"Restricted" Accredited Person (Affiliate)

8. Joint Account Holders

8.1 The current CDR Rules include provisions relating to joint accounts. Importantly, the current CDR Rules provide that a Data Holder who could be required to disclose CDR Data that relates to a joint account must provide a Joint Account Management Service (**JAMS**), to be delivered in accordance with the Data Standards. JAMS must be provided online, and if there is a Data Holder Dashboard for the joint account, may be included in the dashboard. JAMS may also, but need not, be provided offline.

8.2 JAMS can be used by CDR Consumers who are Joint Account Holders (**JAHs**) to indicate the disclosure option they would like to apply to their joint account/s (i.e. a disclosure option must be selected to apply to an account, through JAMS, prior to that account appearing in the authorisation process). JAMS must give effect to a disclosure option applying, or no longer applying, as soon as practicable after a JAH has selected a disclosure option in JAMS.

8.3 No information is currently provided during the authorisation process to explain to CDR Consumers how to select a disclosure option in JAMS.

8.4 To ensure that CDR Consumers are provided with sufficient guidance regarding joint accounts and selecting a disclosure option in JAMS, such that they can make informed decisions about their joint accounts, a number of amendments to the CDR Rules have been proposed. These proposed amendments to the joint account mechanisms in the CDR regime are discussed below.

Selecting a disclosure option in JAMS to occur during the authorisation process

8.5 The proposed amendments to the CDR Rules will include the ability for CDR Consumers who are JAHs to select a disclosure option in JAMS during the authorisation process. CDR Consumers will be permitted to select a disclosure option in JAMS during the authorisation process, however it will not be mandatory. CDR Consumers will still be able to select a disclosure option in JAMS at other times, and through other processes, in accordance with the CDR Rules.

8.6 Whilst going through the authorisation process, the first JAH (**JAH A**) will be able to select a disclosure option in JAMS. When JAH A selects a disclosure option, it will trigger a notification to the second JAH (**JAH B**), inviting them to select a corresponding disclosure option in JAMS. Importantly, the proposed amendments to the CDR Rules will allow there to be multiple holders of a joint account (i.e. more than two people will be permitted to be joint account holders). As such, all references in this Consultation Document to JAH B refer to one or more JAH Bs, unless expressly noted otherwise.

8.7 Irrespective of whether JAH A selects a disclosure option in JAMS, the relevant Data Holder will be able to share CDR Data with the Accredited Data Recipient on JAH A's non-joint accounts, and JAH A will receive the relevant goods or services for those accounts. However, the Data Holder will require both JAH A and JAH B to select the same disclosure option in JAMS before JAH A can receive goods or services in relation to the joint account/s from the Accredited Data Recipient (i.e. no CDR Data on the joint account/s can be shared until the same disclosure option in JAMS is selected by JAH B).

8.8 The only instance in which CDR Data on a joint account can be shared without the approval of JAH B, is if the Data Holder considers it is necessary to avoid seeking the approval of JAH B in order to prevent physical or financial harm or abuse to JAH A.

Notifications to JAH B and instructions for how to select a disclosure option in JAMS

8.9 As discussed above, the proposed amendments to the CDR Rules mean that once JAH A has selected a disclosure option in JAMS, the Data Holder must notify JAH B that JAH A has selected a disclosure option and invite JAH B to select a corresponding disclosure option in JAMS. The notification to JAH B must be made through the Data Holder's ordinary methods for contacting JAH B (e.g. in person or via an email). This notification must:

8.9.1 provide an outline of what the consumer data right is;

8.9.2 inform JAH B of the disclosure option that JAH A has selected, or otherwise inform JAH B that JAH A has indicated that they would not like any disclosure option to apply to the relevant joint account;

8.9.3 inform JAH B that, at present, no disclosure option applies to the account;

8.9.4 explain to JAH B that no disclosure option will apply to the account unless both JAH A and JAH B have selected the same disclosure option to apply;

8.9.5 invite JAH B to make the same disclosure option as JAH A in respect of the relevant joint account; and

8.9.6 if JAH A did select a disclosure option, identify the relevant accredited person to whom JAH A would like to disclose CDR Data in respect of the relevant joint account.

Additional requirements on JAMS to ensure informed decisions are made

8.10 The proposed amendments to the CDR Rules will require Data Holders to include further information on JAMS to assist CDR Consumers who are JAHs to make informed decisions about disclosure options. Data Holders will be required to ensure that JAMS includes information about:

8.10.1 the difference between the 'pre-approval' option and 'co-approval' option (including the impact of each decision), if the Data Holder offers both 'pre-approval' and 'co-approval' disclosure options. We understand that:

(a) the 'pre-approval' option means, if both JAH A and JAH B select the 'pre-approval' option, a Data Holder will be able to disclose CDR Data to an Accredited Data Recipient in relation to the relevant joint account if only one JAH has authorised that disclosure (i.e. the other JAH will not need to also authorise that disclosure); and

(b) the 'co-approval' option means that, if both JAH A and JAH B select the 'co-approval' option, both JAH A and JAH B will be required to authorise the Data Holder to disclose CDR Data in respect of a relevant joint account to an Accredited Data Recipient;

8.10.2 the impact of a disclosure option if the Data Holder offers, and both JAH A and JAH B select in JAMS, the 'pre-approval' or the 'co-approval' option;

8.10.3 that if JAH A and JAH B do not select the same disclosure option to apply to the joint account, disclosure of joint account data relating to the account will ordinarily not be allowed under the CDR Rules;

8.10.4 the fact that both JAH A and JAH B can remove their disclosure option selection in JAMS at any time (independently of each other), the process for removing the selection, and the impact of this withdrawal; and

8.10.5 the fact that when the CDR Data on the joint account is disclosed by a Data Holder to an Accredited Data Recipient, both JAH A and JAH B will ordinarily be able to see information about the authorisation on their Data Holder Consumer Dashboard (as is required by the CDR Rules), for both disclosure options (subject to the discussion below).

8.11 We understand that the CDR Rules will require Data Holders to offer the pre-approval option on joint accounts, but Data Holders may also choose to offer the co-approval option.

Selecting a disclosure option for Consumer Data Requests to Data Holders

8.12 If a Data Holder asks JAH A to authorise disclosure following receipt of a Consumer Data Request, and JAH A has not previously selected a disclosure option to apply to the account, the Data Holder must ask JAH A to select a disclosure option in JAMS, in accordance with the Data Standards.

8.13 If JAH A selects a disclosure option in JAMS, the Data Holder must, through its ordinary methods for contacting JAH B:

8.13.1 notify JAH B that an Accredited Person has made a Consumer Data Request, on behalf of JAH A, that relates to the relevant joint account;

8.13.2 explain to JAH B that JAH A has authorised the disclosure of the joint account data, and that a co-approval option applies to the joint account;

8.13.3 notify JAH B of:

(a) the name of the Accredited Person that made the request;

(b) the period of time to which the CDR Data that is the subject of the request relates;

(c) the types of CDR Data for which the Data Holder is seeking an authorisation to disclose;

(d) whether the authorisation is being sought for the disclosure of CDR Data on a single occasion, or over a period of time of not more than 12 months; and

(e) if the disclosure is over a period of time, what that period of time is,

insofar as these matters relate to the relevant Consumer Data Request;

8.13.4 ask JAH B whether they approve of the joint account data being disclosed;

8.13.5 advise JAH B the time by which the Data Holder needs JAH B to provide this approval;

8.13.6 inform JAH B that they may, at any time, remove the approval;

8.13.7 provide JAH B with instructions for how to remove their approval; and

8.13.8 explain to JAH B the consequence of removing the approval.

8.14 Relevantly, JAH B may remove their approval at any time, regardless of whether that approval was expressly given under a co-approval option, or whether a pre-approval option applies.

8.15 The Data Holder may only disclose joint account data if JAH A has authorised the Data Holder to disclose the relevant CDR Data and:

8.15.1 a pre-approval option applies to the joint account, and JAH B has not removed this approval via their Consumer Dashboard; or

8.15.2 a co-approval option applies to the joint account, and:

(a) JAH B has approved the disclosure of the CDR Data within the relevant timeframe, and JAH B has not removed this approval via their Consumer Dashboard; or

(b) the Data Holder considers it necessary to avoid seeking the approval of JAH B in order to prevent physical or financial harm or abuse to JAH A; or

8.15.3 no disclosure option applies to the joint account and the Data Holder considers it necessary to avoid inviting JAH B to choose a disclosure option in order to prevent physical or financial harm or abuse to JAH A.

8.16 For completeness, the proposed amendments to the CDR Rules will also require Data Holders to notify JAHs in a number of circumstances relating to Consumer Data Requests. The Data Holder must:

8.16.1 notify JAH A, and any other JAH B, through its ordinary means of contacting JAH A, if:

(a) JAH B gives, amends or removes a particular approval through their Consumer Dashboard; or

(b) JAH B does not provide an approval within the relevant timeframe;

8.16.2 notify JAH B, through its ordinary means of contacting JAH B, if JAH A gives, amends or removes a particular authorisation through their Consumer Dashboard; and

8.16.3 if JAH A amends an authorisation relating to a particular approval notify JAH B (through its ordinary methods for contacting JAH B) of:

(a) the nature of the amendments; and

(b) how JAH B may remove an approval to prevent further CDR data relating to the joint account being disclosed.

8.17 However, these notifications are not required if the Data Holder considers it necessary to avoid making the notification to a JAH to prevent physical or financial harm or abuse to another JAH.

Data Holder Consumer Dashboard

8.18 Currently, the CDR Rules require Data Holders to provide Consumer Dashboards for CDR Consumers. The current CDR Rules prescribe that a Data Holder's Consumer Dashboard must contain particular functionalities and information. Importantly, a Data Holder's Consumer Dashboard is currently required to include the details of each authorisation to disclose CDR Data (i.e., details of the Accredited Data Recipient receiving the CDR Data from the Data Holder) and of the types of CDR Data that have been authorised to be disclosed to that Accredited Data Recipient.

8.19 In the proposed amendments to the CDR Rules, if JAH A is authorising a Data Holder to disclose CDR Data that is customer data in relation to a joint account, details of that CDR Data are not required to be included in the equivalent Data Holder Consumer Dashboard for JAH B.[19] For example, JAHs will not be able to see the personal information (i.e. name and address) of another JAH.

8.20 If the JAHs have selected the 'pre-approval' option in relation to a joint account, JAH A can withdraw their authorisation through normal processes provided for in the CDR regime. This includes through the Data Holder Consumer Dashboard (noting that this must allow JAH A to withdraw their authorisation at any time, and notify them of the impact of such a withdrawal). If JAH A withdraws their authorisation, the Data Holder will no longer be able to disclose the CDR Data in relation to the joint account, and the corresponding consent provided to the Accredited Data Recipient will expire at the same time as when JAH A withdraws their authorisation.

8.21 The effect of a 'pre-approval' selection is that JAH B will not be able to withdraw their authorisation (as it will have been provided by JAH A), but JAH B will be able to withdraw their disclosure option selection, effectively withdrawing their permission to the sharing of information in relation to their joint account with JAH A. This will result in the Data Holder no longer being able to disclose the CDR Data in relation to the joint account. The proposed amendments to the CDR Rules will accordingly require the equivalent Data Holder Consumer Dashboard for JAH B to outline the process for JAH B to withdraw their JAMS election, and the impact of such a withdrawal.

Remove restrictions on showing joint accounts during the authorisation process

8.22 The proposed amendments to the CDR Rules will remove the current restriction on Data Holders which requires them not to show any joint account during the authorisation process unless a prior disclosure option has been selected. As such, Data Holders will be able to show joint accounts during the authorisation process, even if a disclosure option has not yet been selected by both JAHs.

Restriction on amendments to JAMS

8.23 The proposed amendments to the CDR Rules, in respect of JAMS, will prohibit Data Holders from:

8.23.1 adding anything to the JAMS process beyond those requirements specified in the CDR Rules and the Data Standards;

8.23.2 offering additional or alternative services as part of the process;

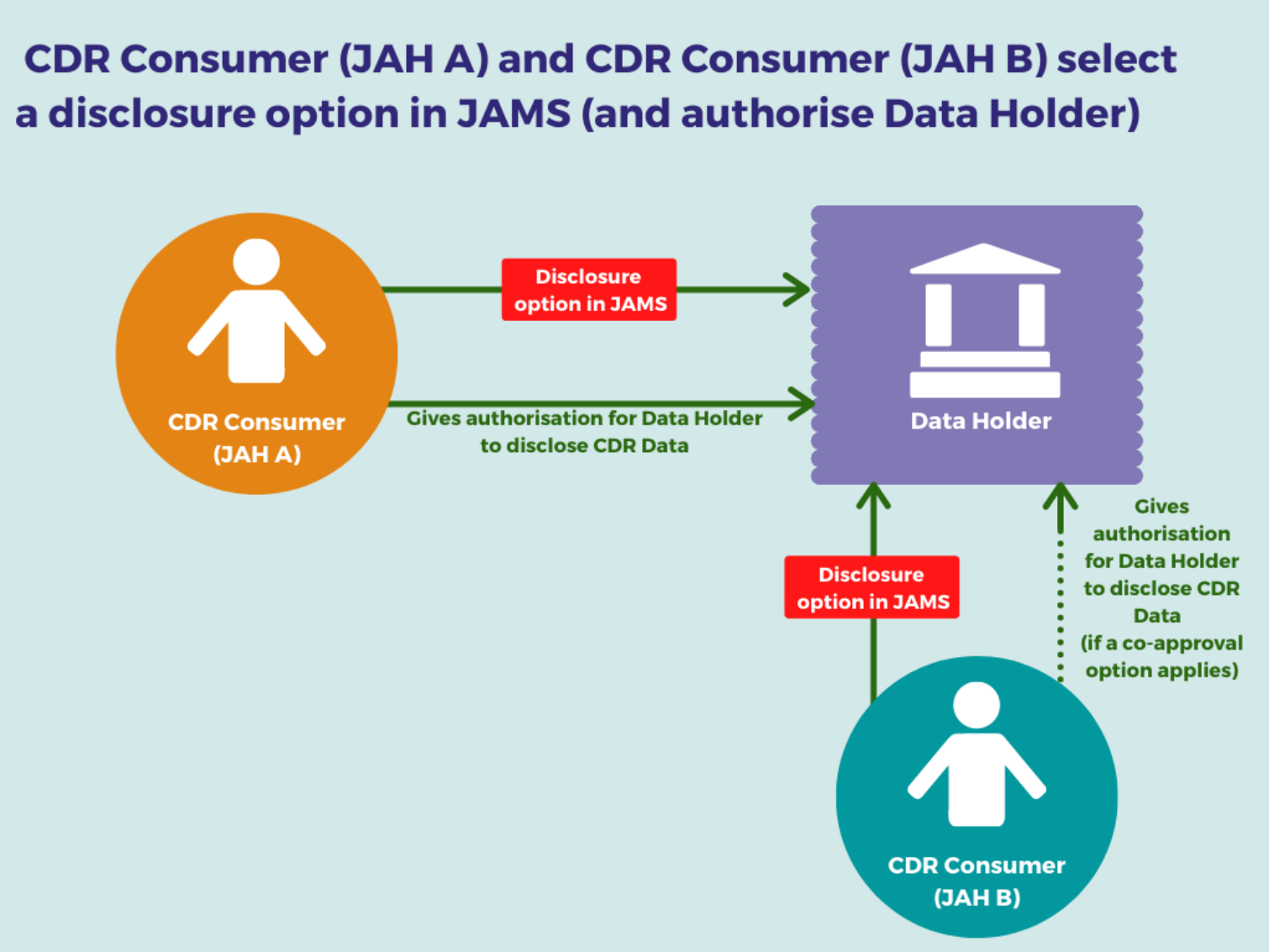
8.23.3 including or referring to other documents, or providing any other information, so as to reduce comprehensibility; or

8.23.4 offering any pre-selected disclosure options.

Summary of JAMs

8.24 To assist with understanding this new process, we have set out below an information flow diagram.

[19] We understand that the Data Standards will also prohibit the personal information of another individual being shown on a CDR Consumer's Data Holder Consumer Dashboard.


CDR Consumer (JAH A) and CDR Consumer (JAH B) select a disclosure option in JAMS (and authorise Data Holder)
CDR Consumer (JAH A)
Disclosure option in JAMS
Gives authorisation for Data Holder to disclose CDR Data
Data Holder
Disclosure option in JAMS
Gives authorisation for Data Holder to disclose CDR Data (if a co-approval option applies)
CDR Consumer (JAH B)

Part C Analysis of Risks

9. Overview

9.1 This **Part C** contains our preliminary analysis of the risks that we have identified as a result of the proposed amendments to the CDR Rules.

9.2 For convenience, we have grouped the following information flows and concepts[20], which may involve new or changed privacy considerations in addition to those identified in the Original CDR PIA report:

9.2.1 general risks that are relevant to all of the information flows and concepts;

9.2.2 changes to consents;

9.2.3 the disclosure of CDR Data to Accredited Persons (through AP Disclosure Consents and Accredited Data Recipient Requests);

9.2.4 the disclosure of information relating to CDR Consumers to non-accredited persons (through TA Disclosure Consents and Insight Disclosure Consents);

9.2.5 the introduction of new levels and kinds of accreditation; and

9.2.6 changes to joint accounts.

9.3 We have described and considered the privacy risks associated with these information flows and concepts in the tables below. We have also identified some of the key existing mitigation strategies that have been included in the legislative framework underpinning the CDR regime, or are intended to be included in the proposed amendments to the CDR Rules, together with our preliminary analysis of, and proposed recommendations to mitigate, any identified gaps.

[20] Please see **Part D [Project Description]** for further information on each of the information flows/concepts.

10. General risks

GENERAL RISKS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**Complexity of the proposed amendments** The proposed amendments will significantly add to the already complex legislative framework underpinning the CDR regime. The proposed amendments will introduce a number of new definitions, concepts, and information flows, all at the same time. There are several inconsistencies and incomplete provisions in the proposed amendments, which may make it difficult to understand the application and intention of those amendments.		The complexities of the proposed amendments raise privacy risks associated with: • entities participating in the CDR regime (such as Data Holders, Accredited Persons and Accredited Data Recipients) not understanding, or taking steps to implement, their obligations under the legislative framework; • the protections for CDR Consumers (built into the legislative framework) not being appropriately applied to CDR data, the result being that any risk of mishandling of CDR Data is not proactively managed. Instead breaches of the framework will need to be reactively managed by the regulator(s) after the CDR Consumer has been exposed to harm (which is likely to involve additional time and resources for the regulators); and • CDR Consumers not understanding the operation of the legislative framework, meaning that they may: o not be properly informed before giving relevant consents; and

GENERAL RISKS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			○ be unlikely to know whether a particular action by an entity breaches their privacy rights. The complexities are particularly concerning in relation to the ability of entities to seek restricted accreditation, noting that such entities are less likely to be sophisticated providers of services who are familiar with handling important personal information and complying with complex legislative frameworks. ***Note to Stakeholders**: We are considering recommending that the ACCC:* • *continue to refine the drafting of the CDR Rules;* • *issue detailed, comprehensive, and clear guidance about the intended application and operation of the CDR Rules, as amended by the proposed changes. We are considering suggesting that different forms of guidance could be developed and specifically tailored to assist:* ○ *CDR Consumers;* ○ *applicants for accreditation;* ○ *Data Holders;*

GENERAL RISKS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			○ *Accredited Persons for each level of accreditation; and* ○ *enclave providers and sponsors.*
2.	**Lack of clarity around collection, use, holding and disclosure of CDR Data** There is a risk that an entity will not understand their obligations under the legislative framework underpinning the CDR regime as it is unclear whether they have collected, are holding, or have disclosed, CDR Data at various stages in the proposed new information flows.		As we previously raised in relation to PIA Update 1, we have found it difficult to determine from the proposed amendments which entity or entities will be considered to have 'collected' CDR data in the context of a CAP arrangement, and when that entity or those entities will be considered to be 'holding' CDR data. In particular, we have found refences to collection by a provider 'on behalf of the principal' to be somewhat ambiguous. This clarity is important because it affects whether the provider is considered to be an 'accredited person' or an 'accredited data recipient' at various stages, which then affects other legislative obligations (including the application of the privacy safeguards). ***Note to Stakeholders:*** *Please see our proposed recommendation in* ***Item 1*** *above, which we consider will assist in mitigating the identified risk.*

GENERAL RISKS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
3.	**CDR Consumers will not understand the consents they are providing, and will experience "information overload"** Given the increased number of different types of consents that can/are required to be requested from a CDR Consumer, a CDR Consumer may find this confusing and potentially overwhelming (noting that each of the proposed amendments to the CDR Rules contains additional requirements for what information is to be provided at this stage). This may result in a CDR Consumer experiencing "information overload", meaning they may not give an Accredited Person properly informed consent.	Rule 4.10(1) (including the proposed amendments) provides that an Accredited Person's processes for asking a CDR Consumer to give and amend consent must: • accord with any consumer experience Data Standards; • be as easy to understand as practicable, including by use of concise language and, where appropriate, visual aids (having regard to any consumer experience guidelines); and • if the consent is not a Collection Consent for the purposes of an Accredited Data Recipient Request, or a Disclosure Consent, accord with any other Data Standards.	***Note to Stakeholders**: We are considering recommending that the ACCC consider whether it would be appropriate to continue, in consultation with the Data Standards Body, conducting consumer research on what is the best way to present a CDR Consumer with all of the different types of consents, to ensure that CDR Consumers are provided with an adequate amount of information before providing their consent, but balancing this against the risk of "information overload" for the CDR Consumer.*

11. Risks associated with changes to consents

CHANGES TO CONSENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
4.	**CDR Participants, and Accredited Persons, will not understand the amendments to the CDR Rules (including the impact on their obligations when collecting, using, and disclosing, CDR Data)** As discussed in ***Item 1***, the complexities of the drafting of the proposed amendments may mean that an Accredited Person does not fully understand their obligations in relation to the type of consent they are seeking (noting there are several obligations relating to the various types, including the introduction of 'categories', of Collection Consents, Use Consents, and Disclosure Consents).		The proposed amendments increase the amount of information an Accredited Person must provide a CDR Consumer, and introduces a new concept of 'categories' of consents. ***Note to Stakeholders:*** *We are considering recommending that the ACCC consider:* • *the need for this new concept of 'categories' as it adds further complexities to an already-complex to understand consent process; and* • *providing Accredited Persons with very clear guidance on how the process in Rule 4.11 is intended to operate, so as to ensure that CDR Consumers are provided with the right type of information and choices before providing their consent.*

CHANGES TO CONSENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
5.	**When CDR Consumer provides Use Consent for Accredited Data Recipient to use CDR Data for general research purposes, the CDR Consumer will not understand what they are consenting to** There may be very little information contained in the CDR Policy, and it is unlikely to contain information about the specific research projects that will be undertaken using that CDR Consumer's CDR Data. There is also a risk that CDR Consumers are unlikely to actually access, and then consider, the CDR Policy when providing their Use Consent.	The proposed amendments provide that when a CDR Consumer is asked to provide a Use Consent for the purposes of general research, they must be provided a link to the description in the Accredited Data Recipient's CDR Policy, which specifies the research to be conducted, and any additional benefit to the CDR Consumer for consenting to the use of their CDR Data.	***Note to Stakeholders:*** *We are considering recommending that the ACCC consider:* • *requiring an Accredited Person to clearly specify, when seeking a Use Consent for the purposes of general research, which specific research projects the Accredited Person will use the CDR Consumer's CDR Data for; or* • *alternatively, whether the information an Accredited Person will use for research should be de-identified, so that no identifiable information of a CDR Consumer will be used by the Accredited Person.*

CHANGES TO CONSENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
6.	**CDR Consumer unaware their CDR Data can be sold** The proposed amendments remove the restriction on asking a CDR Consumer for their consent to sell their CDR Data, and instead introduce a new restriction, limiting the Accredited Person to only seeking consent that falls within a category of consents. This means that an Accredited Person is not prohibited from asking a CDR Consumer for consent to sell their CDR Data when asking for any consent that falls into a category of consents.	If the Accredited Person sells a CDR Consumer's CDR Data when disclosing the CDR Data to another Accredited Person, the recipient of that CDR Data will be required to comply with the relevant requirements and obligations in the CDR Rules, and will also be "accredited".	There is no clear prohibition on an Accredited Person asking a CDR Consumer for consent to sell their CDR Data, but note that this is also not expressly permitted (unless it falls into the category of consent that refers to "selling" CDR Data). Further, there are no requirements in the proposed amendments for the CDR Consumer to be informed, or be able to choose whether they consent to, the selling of their CDR Data. ***Note to Stakeholders:*** *We are considering recommending that the ACCC consider:* • *including requirements around the selling of CDR Data (e.g. requirements for the Accredited Person to seek a CDR Consumer's express consent for the selling of their CDR Data); and* • *including a requirement for the Accredited Person to provide the CDR Consumer with a clear option to not consent to the selling of their CDR Data.*

CHANGES TO CONSENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
7.	**Timing of notifications** The proposed amendments requires CDR Consumers to be told certain things at certain points in information flows, but there is no timing for the requirements.		As examples of the identified risk, the proposed amendments provide the following notification obligations without any timing requirements on those obligations: • in the case of amending a consent, an Accredited Person must give the CDR Consumer statements in relation to the amendment of the consent, however there is no timing for when the CDR Consumer needs to receive this information; and • if the CDR Consumer's Collection Consent expires, but the Use Consent is current, the Accredited Person must notify the CDR Consumer that they can withdraw the Use Consent and make an election to delete redundant data. ***Note to Stakeholders:*** *Given the importance of notifying CDR Consumers about information relating to their consents (such as in relation to the withdrawal or amendment of a consent), we are considering recommending that the ACCC consider including requirements for the Accredited Person to provide the relevant information within a certain timeframe (to ensure that for example, an Accredited Person provides a CDR Consumer with the relevant information* ***before*** *they amend their consent).*

CHANGES TO CONSENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
8.	**Information provided to CDR Consumer when they amend their consent** There is a risk that CDR Consumer's will be provided with too much, or too little, information when amending their consent.	Rule 4.12C(3) provides that when a CDR Consumer amends their consent, the Accredited Person must give the CDR Consumer: • a statement that indicates the consequences of amending the consent; and • a statement that the Accredited Person will be able to continue to use any CDR Data that has already been disclosed to it to the extent allowed by the amended consent.	We consider that providing this information to CDR Consumers is privacy enhancing, especially notifying them that the Accredited Person will be able to continue to use any CDR Data already to disclosed to it. ***Note to Stakeholders:*** *We are considering recommending that the ACCC consider whether it would be appropriate to give the CDR Consumer the opportunity, to at this stage, withdraw their Use Consent if they do not want the Accredited Person to continue using any already-collected CDR Data.* The drafting in Rule 4.12C(3) is unclear as to whether the ACCC intends for all of the information required in Rule 4.11(3) to: • be provided to a CDR Consumer every time the CDR Consumer amends their consent (noting Rule 4.11(3) specifies what information an Accredited Person must give a CDR Consumer when asking a CDR Consumer to ***give*** consent); or • only be provided once when the CDR Consumer gives their original consent (and therefore the only information a CDR Consumer will receive when amending their consent is that specified in new Rule 4.12C(3).

CHANGES TO CONSENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			Note to Stakeholders: *We are considering recommending that the ACCC clarify this requirement, and also consider whether the CDR Consumer should only be provided the information in Rule 4.11(3) if the information has changed since the last time the CDR Consumer gave/amended their consent. This will assist in ensuring a CDR Consumer is provide with adequate information before amending their consent, but does not experience "information overload".*
9.	**If an Accredited Data Recipient becomes a Data Holder, a CDR Consumer's Disclosure Consent does not expire** There is a risk that when an Accredited Data Recipient becomes a Data Holder, the CDR Consumer's Disclosure Consents do not expire, meaning that the CDR Consumer's CDR Data can continue to be disclosed (and potentially sold).		***Note to Stakeholders:*** *Similar to the expiry of Collection Consents and Use Consents, we are considering recommending that the ACCC consider whether it should expressly specify that if an Accredited Data Recipient becomes a Data Holder of CDR Data, any Disclosure Consents that relate to that CDR Data expire (or otherwise explain it is appropriate why those Disclosure Consents continue).*

CHANGES TO CONSENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
10.	**CDR Consumer wishes to amend one aspect of their consent**	The current CDR regime does not facilitate a CDR Consumer amending their consent, however this concept will be introduced in the proposed amendments to the CDR Rules. The proposed amendments will also mean that CDR Consumers will have control over their Collection Consents, Use Consents and Disclosure Consents (rather than simply over their "consent"). This additional level of granularity will mean that it will be easier for the CDR Consumer to amend certain things like extending the validity period of a consent, without amending this period for each consent.	We support the proposed amendments to the CDR Rules as a privacy enhancing step, as they will provide CDR Consumers with greater control of their consents, and increase their engagement with the CDR regime as it will be more "user-friendly".
11.	**Consequence of withdrawing a Collection Consent** There is a risk that a CDR Consumer will not understand what happens with their CDR Data and any Use Consents if they withdraw a Collection Consent.	The proposed amendments to the CDR Rules will mean that if a CDR Consumer's Collection Consent expires (including because the CDR Consumer withdraws that consent), an Accredited Person must notify the CDR Consumer that they may: • withdraw the Use Consent; and • make the election to delete redundant data in respect of that CDR Data.	We consider that notifying CDR Consumers is a privacy enhancing feature, as it will assist in ensuring that they are aware that the expiry of a Collection Consent does not mean that an Accredited Person is prevented from continuing to use that CDR Data (and will give the CDR Consumer to withdraw their Use Consent and make an election to delete any redundant data).

CHANGES TO CONSENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**

12.	**Accredited Person pressures CDR Consumer to amend their consent**
	
	There is a risk that an Accredited Person may coerce a CDR Consumer to amend their consent (e.g. to add additional uses, collect additional CDR Data, or extend the validity period of a consent).
		The proposed amendments to the CDR Rules permit an Accredited Person to invite a CDR Consumer to amend their consent if:
		
		• the amendment would better enable the Accredited Person to provide the goods or services requested by the CDR Consumer; or
		
		• the amendment would:
		
		  ○ be consequential to an agreement between the Accredited Person and the CDR Consumer to modify those requested goods or services; and
		
		  ○ enable the Accredited Person to provide the modified goods or services.
		
		Further, if the Accredited Person invites a CDR Consumer to amend the validity period of their current consent, they must not give:
		
		• the invitation more than a reasonable period before the current consent is expected to expire; or
		
		• more than a reasonable number of such invitations within this period.
			We consider that the requirements for limiting how often, and when, an Accredited Person can invite a CDR Consumer to amend the validity period of a consent are privacy enhancing.
			
			Note to Stakeholders: *We are considering recommending that the ACCC consider including similar limitations on how often, and when, the Accredited Person can invite a CDR Consumer to amend their consent in general (because if a CDR Consumer is constantly inundated with invitations to amend their consent, they may feel pressured to do so, meaning the amendments to their consents may not be given voluntarily).*
			
			Note to Stakeholders: *We are also considering recommending the ACCC continue to investigate the appropriateness of presenting pre-selected options to a CDR Consumer with details of their current consent (and ensure the requirements around permitting pre-selected options are limited to **only** details of the CDR Consumer's current consent), as this information may assist in informing a CDR Consumer which aspects of their consent they would like to amend (as they will be able to view what they previously selected, such as their election to delete redundant data).*

CHANGES TO CONSENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		In addition, the Accredited Person may present the CDR Consumer with pre-selected options in relation to their current consent.	
13.	**CDR Consumer will not understand they can amend their consent** There is a risk that the CDR Consumer will not understand that when they provide their Collection Consent, Use Consent, and Disclosure Consent, they can, at a later point, amend that consent		***Note to Stakeholders:*** *We are considering recommending, to enhance the privacy protections in the CDR Rules, that the ACCC consider including, as part of the information required to be provided as part of Rule 4.11, a requirement for Accredited Persons to notify CDR Consumers when asking for their consent that they can, at a later stage, amend that consent through the Accredited Person's Consumer Dashboard (e.g. to vary the validity period of the consent, or to change the type of CDR Data the Accredited Person collects from a Data Holder).*

CHANGES TO CONSENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
14.	**CDR Consumer will not remember amendments made to the authorisations provided to the Data Holder** Unlike the requirements for when a CDR Consumer amends their consent, the CDR Consumer may amend, or be prompted by the Data Holder to amend, their authorisation, however, will not be able to see these amendments on their Data Holder Consumer Dashboard.		***Note to Stakeholders:*** *We are considering recommending that the ACCC consider whether it should include, similar to the proposed amendments to the requirements of an Accredited Person's Consumer Dashboard, requirements for the Data Holder's Dashboard to contain details of each amendment that has been made to each authorisation.*

12. Risks associated with the disclosure of CDR Data to Accredited Persons (through AP Disclosure Consents and Accredited Data Recipient Requests)

AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
15.	**CDR Participants, and Accredited Persons, will not understand the amendments to the CDR Rules** This new information flow (i.e. disclosure of CDR Data from an Accredited Data Recipient to an Accredited Person) is difficult to track through in the proposed amendments. There is a risk that, given the complexity of the drafting, the obligations of the various parties at each stage will not be understood (especially considering that an 'Accredited Person' who receives the CDR Data from an 'Accredited Data Recipient' will them themselves become an 'Accredited Data Recipient' of that CDR Data).		***Note to Stakeholders:*** *Given the importance of each party understanding their obligations (especially as the CDR Rules contains certain obligations on Accredited Persons, and certain obligations on Accredited Data Recipients), we are considering recommending that the ACCC consider clearly setting out this new information flow (including clarifying the fact that an Accredited Person (A2) becomes an Accredited Data Recipient after receipt of CDR Data and therefore must comply with any obligations relevant to Accredited Data Recipients)).*

AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
16.	**Unclear when Collection Consent, or AP Disclosure Consent, expires** There is a risk that it is not clear when, if one consent (such as the Collection Consent) expires, the other associated consent (such as the AP Disclosure Consent) expires.	The proposed amendments to the CDR Rules provide that if: • an Accredited Person (A2) has a Collection Consent to collect particular CDR Data from a particular Accredited Data Recipient (A1); and • the Accredited Data Recipient (A1) has an AP Disclosure Consent to disclose that CDR Data to that Accredited Person (A2), and one of those consents expires, the other consent expires at the same time (Rule 4.14(1B)).	It is not clear to what is intended by "the other consent expires at the same time", and if this is intended to mean that an associated consent expires: • automatically when the other consent expires; or • when that party is notified by the other party of the expiry of the other consent. ***Note to Stakeholders:*** *We are considering recommending that the ACCC consider whether it would be appropriate to clearly specify when, if one consent expires, the other consent expires. For example, this could include clarifying whether the expiry one a consent is contingent on one party notifying the other of the expiry of the associated consent, or whether the associated consent automatically expires.*
17.	**Accredited Data Recipient (A1) discloses CDR Data to Accredited Person (A2) without checking their accreditation ADR** There is a risk, as the CDR Rules do not require the Accredited Data Recipient (A1) to check the Accredited	We understand that the identified risk may be mitigated by the technical implementation of the ACCC's CDR ICT system, rather than relying on legislative protections in the proposed amendments to the CDR Rules. how the technical implementation will address the privacy risks. CDR Data is required to be encrypted in transit in accordance with Schedule 2.	It is unclear from the proposed amendments to the CDR Rules whether the Accredited Data Recipient (A1) will be required to check the credentials of the Accredited Person (A2) (such as through the ACCC CDR ICT system and Accreditation Register) before disclosing CDR Data to that Accredited Person (A2). This is especially important as the Accredited Person (A2) may have for example, been previously accredited when the Accredited Data Recipient

AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	Person's (A2) accreditation before disclosing CDR Data, that the Accredited Data Recipient (A1) discloses CDR Data to a person who is not indeed "accredited".		(A1) disclosed CDR Data for another CDR Consumer to that Accredited Person (A2), but since that disclosure, the Accredited Person's (A2) has been suspended, revoked, or surrendered. Further, the proposed amendments do not specify the process for disclosing CDR Data in response to an Accredited Data Recipient Request (noting that currently the CDR Rules (Rule 4.6) impose requirements on the disclosure of CDR Data from a Data Holder to an Accredited Data Recipient). This means there are no requirements for the disclosure to be, for example, in accordance with the Data Standards. We query whether it would be more appropriate for (some of) these issues to be addressed in the CDR Rules, or at least further explanation given to entities participating in the CDR regime. ***Note to Stakeholders:*** *Given the importance of ensuring that CDR Data is only disclosed to an "accredited" person, we are considering recommending that the ACCC consider including obligations on:* • *the Accredited Data Recipient (A1) to check the credentials of the Accredited Person (A2) before any CDR Data is disclosed (similar to the obligations on Data Holders); and*

AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			• *each party to notify the other if their accreditation gets suspended, revoked, or surrendered.*
18.	**CDR Consumer unaware of status of Accredited Data Recipient Request** Under the proposed amendments to the CDR Rules, an Accredited Data Recipient (A1) is not obliged to seek an AP Disclosure Consent from a CDR Consumer, even if the CDR Consumer has provided a Collection Consent to the relevant Accredited Person (A2). In addition, even if the CDR Consumer has provided an AP Disclosure Consent to the Accredited Data Recipient (A1), that Accredited Data Recipient (A1) is not obliged to provide the CDR Data to the nominated Accredited Person (A2). Accordingly, there is a risk that a CDR Consumer will not receive an appropriate level of control or oversight		We understand that these proposed amendments reflect that, unlike Data Holders, an Accredited Data Recipient cannot be required to disclose CDR Data. However, we consider that CDR Consumers should be provided with transparency around the progress of their Accredited Data Recipient Request. ***Note to Stakeholders:*** *To ensure the CDR Consumer retains control over their CDR Data (and oversight over any Accredited Data Recipient Requests), we are considering recommending that the ACCC consider whether the CDR Consumer should be informed about:* • *the refusal to progress their Accredited Data Recipient Request (including by refusing to provide the CDR Data to the Accredited Person (A2)); and* • *the reasons for the refusal.*

AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	over the status of their Accredited Data Recipient Request, or their CDR Data.		
19.	**CDR Consumer amends the Collection Consent with the Accredited Person (A2) and not the associated Disclosure Consent with the Accredited Data Recipient (A1)** There is a risk that that the CDR Consumer amends the Collection Consent with the Accredited Person (A2) but not the associated Disclosure Consent with the Accredited Data Recipient (A1).		***Note to Stakeholders:*** *We are considering recommending that the ACCC consider whether it would be appropriate to include requirements for the Accredited Data Recipient (A1) to invite the CDR Consumer to amend their Disclosure Consent if the Accredited Data Recipient (A1) is notified by the Accredited Person (A2) that the CDR Consumer has amended their Collection Consent. This requirement could be drafted in a similar way to the proposed amendments in relation to a Data Holder inviting a CDR Consumer to amend their authorisation if the Data Holder is notified that they have amended their associated Collection Consent with the Accredited Data Recipient (see Rule 4.22A).*
20.	**Accredited Data Recipient (A1) unaware that CDR Consumer has withdrawn their Collection Consent provided to Accredited Person (A2)** There is a risk that an Accredited Data Recipient (A1) continues to disclose CDR Data to an Accredited Person	The proposed amendments require the Accredited Person (A2) to notify the Accredited Data Recipient (A1) if a Collection Consent expires (Rule 4.18B). Withdrawal of a consent is one way that a consent can expire (see Rule 4.14).	***Note to Stakeholders:*** *To ensure that an Accredited Data Recipient (A1) does not continue to disclose CDR Data if the associated Collection Consent given to an Accredited Person (A2) has been withdrawn, we are considering recommending that the ACCC consider including clarifying the obligations on an Accredited Person to notify an Accredited Data Recipient if a Collection Consent for the purposes of an Accredited Data Recipient*

AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	(A2) after the CDR Recipient has withdrawn their Collection Consent given to the Accredited Person (A2).		*Request is **withdrawn**, similar to the requirements specified in Rule 4.13(2)(b).*
21.	**Transparency around Use Consents and Disclosure Consents for direct marketing purposes** There is a risk that before providing the relevant Use Consents and Disclosure Consents for the purposes of direct marketing, a CDR Consumer will not have transparency around what arrangements are in place between Accredited Persons when being recommended certain goods or services (which may mean that vulnerable consumers are taken advantage of).	The proposed amendments (Rule 7.5(3)(a)(iv)) specify that the Accredited Data Recipient may provide this information about another Accredited Person's goods and services if the Accredited Data Recipient: • reasonably believes that the CDR Consumer might benefit from those other goods or services; and • sends such information to the CDR Consumer on no more than a reasonable number of occasions. Further, the proposed amendments also specify that the Accredited Data Recipient can disclose CDR Data to that Accredited Person if the CDR Consumer has given the relevant Collection Consent and Use Consent to the Accredited Person, and AP Disclosure Consent to the Accredited Data Recipient.	***Note to Stakeholders:** Given that this may be used to exploit vulnerable CDR Consumers, we are considering recommending that the ACCC consider whether CDR Consumers should receive greater transparency, before providing Use Consents and Disclosure Consents for direct marketing, about what is "in it" for an Accredited Data Recipient if they recommend/provide information about another Accredited Person (e.g. information about any arrangements/monetary benefits the Accredited Data Recipient receives if they recommend that Accredited Person).*

AP DISCLOSURE CONSENT (AND ACCREDITED DATA RECIPIENT REQUESTS)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
22.	The Original CDR PIA report discusses the risks associated with the disclosure of CDR Data to an Accredited Data Recipient (See ***Step 6 in the Original CDR PIA report***), which will also apply to situations where the Accredited Data Recipient discloses CDR Data to an Accredited Person.	*See Original CDR PIA report.*	*See Original CDR PIA report.*

13. Risks associated with the disclosure of information relating to CDR Consumers to non-accredited persons (through TA Disclosure Consents and Insight Disclosure Consents)

DISCLOSURE TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
23.	**CDR Consumers do not understand the implications of consenting to disclosure of CDR Data, or a CDR Insight, to a recipient outside of the CDR** As discussed above, the proposed amendments will make it easier for CDR Data or CDR Insights to be disclosed outside of the CDR Regime, where the data will have less privacy protections (or potentially no privacy protections) than the same data will have when within the CDR Regime.		We note that the proposed amendments will allow the disclosure of CDR Data and CDR Insights to recipients who are not Data Holders or Accredited Persons (and do not have any obligations under the CDR legislative framework). These recipients may not even have any obligations under other privacy legislation (i.e. the recipient does not need to be an APP entity for the purposes of the Privacy Act, or have otherwise agreed to comply with the APPs). It is important that CDR Consumers understand that if their CDR Data, or a CDR Insight, is disclosed to a Trusted Adviser or an Insight Recipient, that information will be disclosed *outside* the CDR regime. This means that the information, once disclosed, will not be afforded the protections offered by the CDR Rules (and, in particular, the Privacy Safeguards). Additionally, it is important that CDR Consumers understand that CDR Data and CDR Insights may be disclosed to recipients that do not have obligations under any privacy legislation.

DISCLOSURE TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			Note to Stakeholders: *We are considering recommending that the ACCC consider only allowing CDR Data and CDR Insights to be disclosed outside of the CDR Regime to APP entities, or to entities who agree to comply with the APPs as if they were an APP entity.*
24.	**Consent from vulnerable CDR Consumers** There is a risk that an Insight Disclosure Consent from a vulnerable CDR Consumer may not be free and fully-informed.		We note that there is a risk that an Insight Disclosure Consent from a vulnerable CDR Consumer may not be free and fully-informed, particularly in circumstances where the CDR Consumer: • may not understand the negative consequences that may flow from giving their Insight Disclosure Consent (i.e. that the disclosure of the CDR Insight to another person may result in the CDR Consumer being refused access to goods or services); or • may be pressured into providing their Insight Disclosure Consent by a potential provider of goods or services. ***Note to Stakeholders:*** *We are considering recommending that the ACCC consider:* • *whether it is appropriate for CDR Insights to be part of the CDR Regime in circumstances where there is a significant risk that vulnerable CDR Consumers may be pressured into providing an Insight Disclosure Consent, or may otherwise not fully understand*

DISCLOSURE TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			the potential negative consequences that their consent may have; or • *if the ACCC determines that it is appropriate for CDR Insights to remain within the scope of the CDR Regime, implementing mechanisms to ensure that vulnerable CDR Consumers are giving free and fully-informed Insight Disclosure Consents.*
25.	**CDR Insights may be more invasive than sharing raw CDR Data** There is a risk that sharing a CDR Insight about a CDR Consumer may be as, or more, invasive than sharing a CDR Consumer's raw CDR Data.		We note that CDR Insights contain the results of the analysis of raw CDR Data. Therefore, CDR Insights contain information that is more sensitive than raw CDR Data alone. ***Note to Stakeholders:*** *We are considering recommending that the ACCC consider whether it is appropriate for CDR Insights to be generated and disclosed as part of the CDR Regime. This is because of the inherent risks associated with the disclosure of the results of the analysis of raw CDR Data.*

DISCLOSURE TO NON-ACCREDITED PERSONS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
26.	**Risk relating to the transfer of CDR Data and CDR Insights to Trusted Advisers and Insight Recipients** We note that in transferring CDR Data or CDR Insights to a Trusted Adviser or an Insight Recipient, an Accredited Person does not need to comply with the CDR Rules or Data Standards in relation to such transfers. In our view, this may increase the risks of loss or unauthorised access and disclosure during that transfer.		We note that it is important that CDR Data or CDR Insights that are disclosed to a Trusted Adviser or Insight Recipient are appropriately protected during the transfer of information. ***Note to Stakeholders:*** *We are considering recommending that the ACCC consider implementing measures to ensure that CDR Data and CDR Insights are appropriately protected during the transfer between an Accredited Person and a Trusted Adviser or Insight Recipient.*

14. Risks associated with the introduction of new levels and kinds of accreditation

NEW LEVELS AND KINDS OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
27.	**Complexity of the CDR Rules** We note that there is a risk that greater numbers of less sophisticated entities, who may not be experienced in handling personal information, may apply for an unrestricted level of accreditation.		As discussed above (***Item 1***), the proposed amendments to the CDR Rules are very complex to navigate, and this is particularly the case for the new kinds of accreditation. For example, the same entity may be described several different ways in different clauses of the CDR Rules (for example, a Data Enclave Accredited Person may be described in different rules as 'a person with data enclave accreditation or as an 'accredited person', or as 'the principal', or as the 'accredited data recipient'; and an Unrestricted Accredited Person may be described as 'a person [having] unrestricted accreditation', or as an 'accredited person', or as 'the provider', or as 'the enclave provider', or an 'accredited data recipient'). This means that it is often somewhat difficult to work through which rules will apply to the different parties to a CAP arrangement, for the different information flows. In addition, it is unclear which party or parties to a CAP arrangement will be considered to have 'collected', and/or 'disclosed' CDR Data, or be 'holding' CDR Data. This risk is generally discussed above (see ***Item 2***) but is particularly applicable for CAP arrangements in connection with data enclave accreditation and affiliate accreditation. For example, it is not immediately apparent from the proposed amendments whether an enclave provider or sponsor who

NEW LEVELS AND KINDS OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			'collects CDR data on behalf of the principal' under a CAP arrangement, will be considered to have 'collected' the CDR Data and therefore be an Accredited Data Recipient, or whether only the principal is intended to be the Accredited Data Recipient in such a situation. It is also not clear who the CDR Data will have been 'disclosed' to the principal and/or the provider; or whether a data enclave provider will be considered to be 'holding' the CDR Data. This makes it somewhat difficult to apply the definition of 'accredited data recipient' in s56AK of the CC Act. If it is intended that only the principal is considered to have collected the CDR Data (i.e., only it, and not the provider, is considered to be an Accredited Data Recipient), then it is also not clear *when* the principal will be considered to have become an Accredited Data Recipient. While we believe that it is likely to be intended that this will be the time that the CDR Data is transferred into the enclave or otherwise received by the sponsor, rather than when the CDR Data is accessed by the provider, this is not entirely clear from the drafting of the proposed amendments. It is foreseeable that further complexity will arise where an entity undertakes transactions in multiple capacities. For example, an Unrestricted Accredited Person may have an appropriate consent from a CDR Consumer to collect CDR Data from a Data Holder; may then

NEW LEVELS AND KINDS OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			agree to be an enclave provider and collect the same CDR Data on behalf of a Data Enclave Accredited Person; and may also potentially collect the same CDR Data on behalf of another affiliate in its capacity as a sponsor. It may be difficult for that person (or the ACCC and/or OAIC at a later date) to determine the capacity in which they are collecting and/or holding CDR Data at any point in time, making it difficult to determine which obligation(s) in the CDR Rules apply. For example, Schedule 2 currently provides important protections for CDR Consumers in relation to the storage and handling of CDR Data. We suggest that it may be difficult for an Unrestricted Accredited Person who is also a sponsor and/or enclave provider for one or more other Accredited Persons (and perhaps also an outsourced service provider for these or other entities), and/or for the ACCC or OAIC, to establish compliance with the relevant requirements of Schedule 2 in respect of any transaction, because their obligations will differ depending on the capacity in which they are acting. Clarity is important to ensure that the obligations of both the Unrestricted Accredited Person and the Data Enclave Accredited Person can be ascertained and understood by these entities. In our view, the further complexity of the CDR Rules as a result of the proposed amendments increases risks of non-compliance, particularly

NEW LEVELS AND KINDS OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			by restricted Accredited Persons, with the important privacy protections contained in the legislative framework. This in turn may increase reliance on the regulators to take additional investigatory and/or legal action for noncompliance. ***Note to Stakeholders:*** *We are considering recommending that the CDR Rules be further clarified (e.g. further expansion of Rule 1.7(v), which only relates to outsourced service arrangements), and/or clear and simple guidance provided by the ACCC, to assist entities understand their privacy obligations.* *We are interested in whether other options should also be recommended, for example whether an Accredited Person must complete mandatory training and demonstrate an understanding of their privacy obligations before accreditation will be granted for particular levels or kinds of accreditation.*

NEW LEVELS AND KINDS OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
28.	**Incentive on sponsor to ensure compliance by affiliate** We query whether the obligations on a 'sponsor' in connection with their affiliate's accreditation are sufficiently robust.	In order for an affiliate accreditation to be granted, the sponsor must certify that the affiliate complies with the relevant requirements of the CDR Rules. The sponsor must also take 'reasonable steps' to ensure ongoing compliance by the affiliate (Rule 5.5A). An affiliate may only make consumer data requests through the sponsor acting on its behalf under a CAP arrangement (Rule 5.1D(2). The ACCC and/or OAIC may take action against an affiliate for non-compliance with the legislative framework, or a sponsor who does not take reasonable steps as described above (noting the amendments to the civil penalty provisions in the CDR Rules).	The accreditation requirements are important in ensuring CDR Consumers can have confidence that the recipients of their CDR Data have been appropriately 'vetted' as suitable entities to handle CDR Data. We query whether the current amendments provide a sponsor with enough incentive for it to actively monitor and otherwise ensure that the affiliate complies with their obligations as an Accredited Person. We also query whether there may be uncertainty about what will be required for a sponsor to have taken 'reasonable steps'. For example, it is not clear whether a sponsor would satisfy the test by simply including an obligation in the CAP agreement which requires the affiliate to comply with the CC Act and the CDR Rules. If this would be sufficient, we suggest that it may provide little protection for a CDR Consumer if a restricted level Accredited Person does not meet its contractual requirements, noting that there is no obligation on a sponsor to enforce the CAP arrangement. ***Note to Stakeholders:*** *We are considering whether the CDR Rules should specify that a sponsor should be liable for the actions of their affiliates and their compliance with the legislative framework (similar to the position for an Accredited Person's outsourced service providers).*

NEW LEVELS AND KINDS OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
29.	**The CDR Rules do not deal with a situation where the relevant CAP agreement is terminated, or suspended, or expires**	An affiliate must have a sponsor (Rule 5.1D(1)), and a Data Enclave Accredited Person must have an enclave provider (Rule 5.1B(1)). In order to be a sponsor or enclave provider, the Unrestricted Accredited Person must be a provider in a CAP arrangement. An Accredited Person has an obligation to notify the Data Recipient Accreditor of any certain matters that might affect the decision to grant accreditation (Rule 5.14).	We note that the CDR Rules will provide that on suspension or revocation of the accreditation of a sponsor or enclave provider, the Data Recipient Accreditor may suspend or revoke the accreditation of the affiliate or Data Enclave Accredited Person (as applicable) (Rule 5.17(1), Items 11 and 12 of the table). We consider that this is appropriate and enhances the protection for CDR Consumers. However, if the relevant CAP arrangement between the principal and the provider is suspended, terminated or expires, the Unrestricted Accredited Person will no longer be a 'enclave provider' or a 'sponsor', but there does not appear to be mechanism for the lower level accreditation to end. ***Note to Stakeholders:*** *We are considering whether there should be a requirement in the CDR Rules (or perhaps a condition of accreditation) to notify the Data Recipient Accreditor if the relevant CAP arrangement is suspended or terminated or expires, and for the Data Recipient Accreditor to have the ability to suspend or revoke the restricted accreditation in such a situation.* It is also not clear what mechanisms would be used if a restricted level Accredited Person wishes to 'switch' enclave provider or sponsor after accreditation (e.g. whether they must

NEW LEVELS AND KINDS OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			surrender their existing accreditation and seek a new accreditation in relation to the new sponsor/enclave provider). ***Note to Stakeholders:*** *We are considering recommending that this be clarified.*
30.	Risk that CDR Consumer does not know that a provider under a CAP arrangement has been used to collect their CDR Data	The CDR Consumer will be informed that a specific provider will collect their CDR Data when they are asked to provide their consent (Rule 4.11(3)(i)). Rule 7.2(4) will mean that the affiliate or Data Enclave Accredited Person's CDR policy must contain information about their relationship with the Unrestricted Accredited Person (either an enclave provider or sponsor) If CDR Data may be collected by a provider under a CAP arrangement, the proposed amendments will require an Accredited Person to ensure that their consumer dashboard includes the provider's name and accreditation number (Rule 1.14(3)(i)).	We consider that the requirements to inform the CDR Consumer of the specific provider that will be collecting (and/or storing) their CDR Data on behalf of the restricted level Accredited Person to be a privacy-enhancing feature of the proposed amendments.

NEW LEVELS AND KINDS OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
31.	**Deletion of redundant data** There is a risk that a provider under a CAP arrangement may not comply with a direction by the principal to delete redundant data.	Rule 7.12(2)(b) will mean that the principal to a CAP arrangement must give directions to the provider in relation to deletion of redundant data.	It is not clear whether Rule 7.12(2)(b) will apply to a CAP arrangement for data enclave accreditation arrangements, or for affiliate accreditation arrangements, since the rule will only apply if the principal has been 'provided with a copy' of the redundant data. Although the provider will have collected the CDR Data on behalf of the restricted level Accredited Person (and in the case of an enclave provider, the CDR Data will be stored on its ICT infrastructure), it is difficult to see how they will have been 'provided with a copy' of that CDR Data. In addition, there does not appear to be any legislative requirement for the provider to comply with a direction by the principal in respect of redundant data. Unlike contractual arrangements for outsourced service providers, the CDR Rules are silent about the matters that must be contained in a CAP arrangement. For example, there is no requirement that it must include provisions which will require the provider to comply with any directions by the principal about deletion or de-identification of redundant data. Without this clarity, there is a risk that a CDR Consumer's CDR Data will continue to be inappropriately held in an identified form after it becomes redundant.

NEW LEVELS AND KINDS OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			Note to Stakeholders: *We are considering recommending that this be further clarified by the CDR Rules.*
32.	**Risk of overlap or inconsistency between contractual CAP arrangements and legislative liability** There may be a risk that a Data Enclave Accredited Person is not aware that, despite the terms of a CAP agreement, they will have responsibilities and liabilities under the legislative framework.		As discussed above (***Item 31***), the proposed amendments do not specify any requirements for a CAP arrangement, but leave it to the parties to reach a suitable agreement on all matters. For example, a Data Enclave Accredited Person may negotiate a CAP arrangement which clearly allocates all liability for a failure of the relevant ICT environment to adequately protect CDR Data stored in the data enclave to the enclave provider. The Data Enclave Accredited Person may therefore not appreciate that it may still bear responsibility or liability under the legislative requirements as an Accredited Data Recipient, and as a consequence may not take appropriate action to ensure compliance with those requirements, therefore exposing the CDR Consumer to the risk of harm. ***Note to Stakeholders:*** *As for* ***Item 1****, we suggest that further guidance is required, to ensure all entities participating in the CDR regime understand their obligations.*

NEW LEVELS AND KINDS OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
33.	**Maintenance of records** As currently drafted only the principal (restricted level Accredited Persons) will be required to keep records about the CAP arrangement.	Rule 9.3(2)(i) will require an 'accredited data recipient' to keep and maintain records of any CAP arrangement in which the accredited data recipient is the principal, including how the provider will use and manage any CDR data shared with it".	We consider that it may be critical for the ACCC and/or the OAIC to have access to all information about the CAP arrangement and its operation, in order to take action to effectively enforce compliance with privacy obligations in the legislative framework. There may be instances in which the principal has failed to keep the relevant records, or those records are otherwise no longer available. ***Note to Stakeholders:*** *We are considering that the ACCC consider whether there would be benefits in broadening Rule 9.3(2)(i) to apply to providers in a CAP arrangement.*
34.	**Risk that the CDR Data that a Limited Data Accredited Person can handle is inherently sensitive, or may be if analysed together with CDR Data obtained in relation to other sectors.**	ACCC has received advice from cyber-security experts about the risks associated with the types of CDR Data that may be held for the banking sector. A Limited Data Accredited Person will be required to comply with all protections in CDR legislation for the types of CDR Data that it is permitted to handle.	Although we understand that the risks of the CDR Data types included in Schedule 3 have been comprehensively considered from a security perspective (i.e. the risks of the data being of a nature which would be unlikely to be the subject of a cyber security threat), we note that any banking transactions data is likely to be inherently sensitive and could potentially still expose CDR Consumers to risk if it is mishandled, even if there is little security risk in relation to that CDR Data. ***Note to Stakeholders:*** *We are considering recommending that the ACCC ensure that it is satisfied that the types of CDR Data that may be*

NEW LEVELS AND KINDS OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			handled by Limited Data Accredited Persons is appropriate, including through considering feedback from stakeholders as part of this consultation process. This is particularly important once other sectors are introduced, and the CDR Data may (if appropriate consent is obtained) be analysed together with other information about the CDR Consumer.
35.	**Risk that a Limited Data Accredited Person will seek to collect CDR Data that does not fall within one of the permitted types of data**	Rule 5.1C expressly prohibits such collection. We understand that the technical implementation will mean that a Limited Data Accredited Person will technically only be able to use the ACCC CDR ICT system to request data of a type that falls within Schedule 3.	There is currently little information about how a Data Holder, or an Accredited Data Recipient, who receives a request for CDR Data will know that the request is from, and/or made on behalf of, a Limited Data Accredited Person, and that the request is for the permitted types of CDR Data, before disclosure. ***Note to Stakeholders:*** *We are considering whether the ACCC should clarify this, to provide assurance that the Data Holder/Accredited Data Recipient will not mistakenly disclosure more types of CDR Data than the Limited Data Accredited Person is permitted to handle.*

15. Risks associated with the changes to joint accounts

JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
36.	**JAMS only applies to the disclosure of CDR Data by a Data Holder to an Accredited Data Recipient** The CDR Rules only allow for disclosure options to be selected in JAMS, being a service offered by Data Holders. Therefore, JAMS is only relevant to the disclosure of CDR Data by a Data Holder to an Accredited Data Recipient.		The CDR Rules are currently silent on whether disclosure options must be selected (or confirmed) before an Accredited Data Recipient (or Accredited Person) may disclose CDR Data on a joint account to another Accredited Person, a Trusted Advisor or an Insight Recipient (noting that this would be a CDR Insight based on raw CDR Data relating to a joint account). In other words, there is currently no mechanisms for JAHs to consent to the disclosure of joint account data once it is held by the Accredited Data Recipient. This means that JAHs have no control over their joint account data at this stage. ***Note to Stakeholders:*** *We are considering recommending that the ACCC consider ensuring that the CDR Rules prescribe how JAHs can have control over their joint account data once it is held by an Accredited Data Recipient.*
37.	**CDR Consumers do not understand the mechanism for selecting a disclosure option in JAMS** There is a risk that CDR Consumers who are JAHs will not understand why and how	The proposed amendments to the CDR Rules will assist to ensure that JAHs make informed decisions about disclosure options. Data Holders will be required to ensure that JAMS includes information about: • the difference between a 'pre-approval' disclosure option and a 'co-approval' option	We support the additional requirements to notify JAHs of certain information about the process of selecting a disclosure option in JAMS. From a privacy perspective, we believe that provision of additional information will help CDR Consumers understand the operation of CDR regime, so that informed consent can be obtained from both JAHs, is a positive privacy step.

JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	they have to select a disclosure option in JAMS (and subsequently authorise the Data Holder to disclose data in respect of the joint account to the Accredited Data Recipient without understanding the implications of the disclosure).	(including the impact of each decision), if the Data Holder offers both 'pre-approval' and 'co-approval' options; • the impact of the disclosure options if the Data Holder offers, and both JAH A and JAH B select in JAMS, the pre-approval' or 'co-approval' option; • the fact that both JAH A and JAH B can remove their disclosure option selection in JAMS at any time (independently of each other), and the impact of this withdrawal; and • the fact that when the CDR Data on the joint account is disclosed by a Data Holder to an Accredited Data Recipient, both JAH A and JAH B will be able to see information about the authorisation on their Data Holder Consumer Dashboard (as is required by the CDR Rules), for both 'pre-approval' and 'co-approval options' (subject to the particular exemptions). Additionally, when a Data Holder sends a notification to a JAH B, inviting them to make a corresponding JAMS election, that notification must contain particular information. The notification must: • provide an outline of what the CDR is;	

JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		• inform JAH B of the disclosure option that JAH A has selected, or otherwise inform JAH B that JAH A has indicated that they would not like any disclosure option to apply to the relevant joint account; • inform JAH B that, at present, no disclosure option applies to the account; • explain to JAH B that no disclosure option will apply to the account unless both JAH A and JAH B have selected the same disclosure option to apply; • invite JAH B to select the same disclosure option as JAH A in respect of the relevant joint account; and • if JAH A did select a disclosure option, identify the relevant Accredited Person to whom JAH A would like to disclose CDR Data in respect of the relevant joint account.	

JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
38.	**Inconsistency between JAMS and the 'offline' version of JAMS** Noting that there will be an ability for CDR consumers to select a disclosure option in an 'offline' version of JAMS, there is a lack of clarity about how data holders will be required to ensure that they accurately and promptly reflect the offline selection in their online version of JAMS. This raises the privacy risk that a disclosure option selected in the offline version will not be properly implemented in the online version of JAMS, which is relied upon for processing disclosures of joint account CDR Data.		We note that it is important that the online version of JAMS displays the correct disclosure option selected by a JAH at any point in time. This is because the processing of disclosures of CDR Data on joint accounts relies upon the disclosure options recorded in JAMS. ***Note to Stakeholders:*** *We are considering recommending that the ACCC consider requiring Data Holders to promptly input any disclosure option selected in an offline version of JAMS into the online version of JAMS.* *We are also considering recommending that the ACCC consider implementing measures to ensure that the disclosure option selected in the offline version of JAMS is correctly reflected in the online version of JAMS.*

JOINT ACCOUNTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
39.	**Vulnerable CDR Consumers** The risks discussed in the CDR PIA report in relation to vulnerable CDR Consumer have been, to an extent, mitigated through the proposed amendments to the CDR Rules.	*As discussed in Step 1B in the Original CDR PIA report*. However, the proposed amendments to the CDR Rules will allow a Data Holder to disclose CDR Data relating to a joint account with *only* JAH A having selected a disclosure option, if the Data Holder considers that asking JAH B to make a disclosure option (or alerting JAH B to the fact that JAH A has selected a disclosure option) may result in financial or physical abuse to JAH A by JAH B. Further, as an additional mitigation strategy to protect vulnerable CDR Consumers, the proposed amendments to the CDR Rules will prohibit Data Holders from displaying CDR Data that comprises of personal information (i.e. name and address) on the Data Holder Consumer Dashboard of another CDR Consumer. This will mean, in effect, that JAHs will not be able to see the personal information of another JAH on their joint account via their Data Holder Consumer Dashboard. We understand that this proposed amendment to the CDR Rules reflects extensive consumer experience testing and research, which suggested that being able to see the personal information of another JAH could trigger fear and anxiety in a JAH.	We note that the proposed amendments to the CDR Rules will provide further clarity around joint accounts and, if implemented, will afford JAHs further privacy protections and ensure that JAHs cannot see the personal information of another JAH. Additionally, important amendments have been introduced that will allow Data Holders to disclose joint account data *without* a disclosure option having been selected by both JAHS, if the Data Holder considers that asking JAH B to make a disclosure option (or alerting JAH B to the fact that JAH A has selected a disclosure option) may result in financial or physical abuse to JAH A by JAH B. These are privacy-enhancing steps. However, we note that the proposed amendments to the CDR Rules do not oblige the Data Holder to require a particular, clear and standardised level of evidence, if an exception to the JAMS election process is to apply. ***Note to Stakeholders:*** *We are considering recommending that the ACCC consider ensuring that the CDR Rules prescribe the level of evidence that a Data Holder must be satisfied of before determining that an exception to the disclosure option process in JAMS is to apply (or that a notification need not be given).*

Attachment 1 Glossary

Term	Meaning
ACCC	means the Australian Competition and Consumer Commission.
Accreditation Register	means the register to be established in accordance with subsection 56CE(1) of the CC Act.
Accredited Data Recipient (ADR)	has the meaning given by section 56AK of the CC Act.
Accredited Person	means a person who holds an accreditation under section 56CA(1) of the CC Act.
Australian Privacy Principles (APPs)	means the Australian Privacy Principles at Schedule 1 to the Privacy Act.
CC Act	means the *Competition and Consumer Act 2010* (Cth).
CDR Consumer(s)	has the meaning given by subsection 56AI(3) of the CC Act.
CDR Data	has the meaning given by subsection 56AI(1) of the CC Act.
CDR Participant	has the meaning given by subsection 56AL(1) of the CC Act.
CDR Policy	means a policy that a CDR entity must have and maintain in compliance with subsection 56ED(3) of the CC Act.
Consumer Dashboard	(a) in relation to an accredited person, has the meaning given by Rule 1.13 of the *Competition and Consumer (Consumer Data) Rules 2019.* (b) in relation to a Data Holder, has the meaning given by Rule 1.14 of the *Competition and Consumer (Consumer Data) Rules 2019*.
Consumer Experience Guidelines (CX Guidelines)	means the guidelines of that name, as published by Data61.
Data Holder	has the meaning given by subsection 56AJ of the CC Act.
Data Recipient Accreditor	means the person appointed to the role of Data Recipient Accreditor in accordance with subsection 56CG of the CC Act.
Data Standards Body	means the body holding an appointment under subsection 56FJ(1) of the CC Act.
Data Standards	means the data standards made under subsection 56FA of the CC Act.
CDR Rules	means the *Competition and Consumer (Consumer Data Right) Rules 2020*.
OAIC	means the Office of the Australian Information Commissioner.

Open Banking Designation	means the *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (Cth).
Privacy Act	means the *Privacy Act 1988* (Cth).
Privacy Safeguards (PSs)	means the provisions in Subdivision B to F of Division 5 of Part IVD of the CC Act.