Maddocks

Australian Competition and Consumer Commission

CONSUMER DATA RIGHT REGIME

Update 1 to Privacy Impact Assessment

Analysis undertaken as at 4 September 2020

Report finalised on 6 October 2020

Contents

Part A Introduction

1. Overview

1.1 Maddocks was engaged to undertake this updated privacy impact assessment report (**PIA Update 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 for the Consumer Data Right Regime (**Original CDR PIA report**), together with the responses to the recommendations made in that report.[1]

1.3 As the Original 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**), the 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[2].

1.4 The ACCC is responsible for making the CDR Rules, including continually reviewing, considering and revising those CDR Rules as required. The CDR Rules commenced on 6 February 2020. Since that time, the ACCC has undertaken an extensive process of consultation with stakeholders about the operation of the CDR Rules within the broader legislative framework. The ACCC has formulated a number of amendments to the CDR Rules.

1.5 In accordance with the recommendation in the Original CDR PIA report, the ACCC has engaged Maddocks to undertake an assessment of the privacy impacts of some of the proposed amendments to the CDR Rules. We have based our discussion and analysis in this PIA Update report on a version of the CDR Rules provided to us on 4 September 2020.[3] These proposed amendments to the CDR Rules relate to the ability for Accredited Data Recipients to, under an outsourcing arrangement (**CDR Outsourcing Arrangement**) with another accredited person (who will be an "outsourced service provider" (**OSP**) of the Accredited Data Recipient), arrange for CDR Data to be collected by the OSP directly from the Data Holder (the current CDR Rules contemplate an OSP only being permitted to *use* CDR Data on behalf of the Accredited Data Recipient after the Accredited Data Recipient has received the CDR Data from the Data Holder).

1.6 This PIA Update report is intended to complement the Original CDR PIA report. It does not seek to repeat existing privacy risks or mitigation strategies that were discussed in the Original CDR PIA report. Rather, it focuses on the privacy implications of the proposed amendments to the CDR Rules, and whether or not there are privacy safeguards in place or that could be implemented to ensure that individuals are not unnecessarily exposed to risks of harm.

[1] The Original CDR PIA report, and the responses made to the recommendations in that report, are available at: https://treasury.gov.au/publication/p2019-41016.
[2] Recommendation 1 in the Original CDR PIA report.
[3] We understand that the version of the CDR Rules we received on 4 September 2020 was further reviewed and refined by the ACCC after this date, and before being made on 1 October 2020.

2. Structure of this PIA Update report

2.1 This PIA Update report is comprised of the following sections :

2.1.1 **Part B – Executive Summary**: This section contains a summary of the privacy risks we have identified, together with a list of all recommendations we have made as a result of our analysis.

2.1.2 **Part C - Methodology:** This section details how we are undertook this PIA Update report, and includes information about the scope of this PIA Update report.

2.1.3 **Part D - Project Description:** This section contains a summary of the proposed changes to the CDR Rules, describes the applicable legislative framework, and discusses the various relationships and information flows involved in the CDR regime.

2.1.4 **Part E - Analysis of Risks:** We conducted an analysis of the potential privacy risks that we identified as being associated with the proposed changes to the CDR Rules, based on the information available to us. We identified the current mitigation strategies, and conducted a gap analysis to identify any areas of concern.

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

2.1.6 **Attachment 2 – Summary of Original Steps in the CDR PIA**: This section sets out the diagrams of the original steps of the Original CDR PIA report.

Part B Executive Summary

3. Introduction

3.1 In this **Part B [Executive Summary]**, we have provided a summary of the privacy risks we have identified in the proposed changes to the CDR Rules, as well as a consolidated list of all of the recommendations we have made as a result of our analysis and the associated privacy risks we have identified during that analysis.

3.2 We understand that the ACCC, in consultation with other Commonwealth agency stakeholders as required, will separately develop a response to our recommendations.

4. Summary of findings

4.1 We have identified several privacy risks related to the proposed amendments to the CDR Rules. These include privacy risks associated with:

4.1.1 a lack of clarity in relation to when a Provider collects CDR Data from a Data Holder on behalf of a Principal;

4.1.2 the need for the parties to the CDR Outsourcing Arrangement to effectively communicate information in relation to a CDR Consumer's consent;

4.1.3 the need for further guidance about the liability of the parties to the CDR Outsourcing Arrangement, including in relation to the collection of CDR Data and compliance with various obligations on Accredited Data Recipients (and/or accredited persons) in the CDR Rules;

4.1.4 a potential lack of clarity for CDR Consumers in relation to the specific Provider that will be collecting their CDR Data; and

4.1.5 a potential for continued collection, use, or disclosure, of CDR Data by a Provider, after:

(a) the CDR Consumer has withdrawn their consent, or their consent has expired; or

(b) the Principal's or Provider's accreditation has been surrendered, suspended or revoked.

4.2 However, we believe that these risks may be mitigated if the ACCC considers, and implements (in required), the Recommendations in paragraph 5 of this **Part B [Executive Summary]**.

5. Recommendations

5.1 We have made the following recommendations in this PIA report. These are summarised below, but should be read in connection with the relevant Parts of this PIA Update report.

Recommendation 1 Clarification in relation to CDR Outsourcing Arrangements

We **recommend** that the ACCC clarify:

- whether the Provider is liable for its collection of CDR Data from the Data Holder (not the Principal on whose behalf it is making that collection);
- which obligations in the CDR Rules apply to the Principal and/or the Provider (noting that both will be accredited persons); and
- the intention of the proposed amendments to Rule 7.6(2)(b)(ii), and specify whether it is intended to apply to further CDR Outsourcing Arrangements of the Provider in relation to that CDR Consumer, or additional CDR Outsourcing Arrangements of the Provider for other CDR Consumers.

Recommendation 2 CDR Outsourcing Arrangements

We **recommend** that the CDR Outsourcing Arrangements be expressly required to contain an obligation:

- upon the Principal to accurately communicate the CDR Consumer's consent to the Provider;
- upon the Provider to collect CDR Data from the Data Holder in accordance with the consent provided by the CDR Consumer, and communicated by the Principal; and
- upon the Principal to notify the Provider if a CDR Consumer withdraws their consent or authorisation, so that the Provider does not inadvertently continue to use or disclose CDR Data without an appropriate consent and authorisation.

Further, we **recommend** that the ACCC should consider whether the legislative framework should contain specific technical requirements for any communications that occur between the Principal and the Provider for information that is not CDR Data (such as information about a CDR Consumer's consent, or their contact information). These requirements could be specified in the proposed amendments to the CDR Rules regarding the content of CDR Outsourcing Arrangements. This would further assist to ensure that the information is appropriately protected.

Recommendation 3 Obligations in relation to communicating consent

As an alternative to **Recommendation 2** in relation to containing an obligation in the CDR Outsourcing Arrangements for communication of consent, we **recommend** the ACCC consider whether the CDR Rules could be amended to include an express obligation on the Principal to the CDR Outsourcing Arrangement to notify the Provider of the withdrawal or expiry of a consent. This would strengthen the privacy protections by not simply relying on the Accredited Data Recipients complying with, and enforcing, contractual obligations.

Recommendation 4 Consideration of information provided to CDR Consumer when asking for consent

We **recommend** that:

- the ACCC clarify whether the references to 'the accredited person's CDR Policy' in Rule 4.11(3)(f)(ii) and (iii) are meant to refer to the Principal, the Provider if they are an accredited person, or both;
- Rule 4.11(3)(f)(iii) is amended to specify that the CDR Consumer can obtain further information about the specific Provider's *collections, uses* and disclosures from the Principal's CDR Policy; and
- the CDR Consumer is informed that their CDR Data may be collected by, disclosed to, or *used by*, the specific Provider.

Recommendation 5 Information provided on Principal's Consumer Dashboard

We **recommend** that the ACCC consider whether, through the Principal's Consumer Dashboard, CDR Consumers should be provided with more granular information (e.g. Provider "X" will be used to collect CDR Data from Data Holder "X").

Recommendation 6 Use of Principal's credentials

If use of the Principal's ICT credentials (i.e., ICT security certificates) by the Provider is to be permitted, we **recommend** that the ACCC consider amending the CDR Rules to require CDR Outsourcing Arrangements to contain strict obligations in relation to the use of the Principal's credentials by the Provider. If it is not intended that the Provider can use the Principal's credentials, we **recommend** that the CDR Rules expressly prohibit this use.

Recommendation 7 Data Holder's obligations

We **recommend** that the ACCC consider whether Data Holders should know whether the Accredited Data Recipient is acting in the role of a Provider or a Principal.

The Data Holder could then be required to:

- check the accreditation for both the Provider and the Principal, including whether each accreditation has been surrendered, suspended or revoked; and
- notify the Principal and the Provider if the CDR Consumer's authorisation is withdrawn or expires.

Recommendation 8 Steps before Provider discloses CDR Data to the Principal

We **recommend** that the ACCC consider whether it would be appropriate for the CDR Rules to contain requirements for the Provider, before disclosing any CDR Data, to check:

- the accreditation of the Principal; and
- that the technical details it is going to use for the disclosure of the CDR Data match up with the Principal on whose behalf it collected the CDR Data from the Data Holder, or the Principal who disclosed the CDR Data to it.

Recommendation 9 Notification of suspension, revocation, or surrender, of accreditation

We **recommend** that the ACCC consider whether the CDR Rules should clearly provide further protections for CDR Consumers, which could include:

- requiring, if either the Principal's, or the Provider's, accreditation is suspended, revoked or surrendered (previously-accredited data recipient):
    - the previously-accredited data recipient must notify the other Accredited Data Recipient (i.e. the Principal or the Provider, as relevant) of the fact that it is no longer accredited; and
    - the CDR Consumer must be notified of that fact by either:
        - the previously-accredited data recipient; or
        - the other Accredited Data Recipient,

      as agreed in the CDR Outsourcing Arrangement; and
- broadening the obligations in the CDR Rules so that, if a party to a CDR Outsourcing Arrangement is notified regarding the other party (i.e. the previously-accredited data recipient is no longer accredited), they must not continue to collect or use CDR Data and clarifying the requirements to treat that CDR Data as redundant data.

If the ACCC intends to implement systems (e.g. through the ACCC CDR ICT system), which will ensure anyone using the Principal's credentials (including a Provider) is notified of a suspension, revocation or surrender of the Principal's accreditation, this functionality should be clearly communicated to CDR Consumers.

Recommendation 10 Further clarifications

We **recommend** that the ACCC consider whether it should explicitly clarify that, if the Principal uses a Provider to collect CDR Data from a Data Holder on its behalf, the Principal only collects the CDR Data when the Provider discloses that CDR Data to the Principal (rather than when the Provider collects that CDR Data from the Data Holder).

We also **recommend** that the ACCC consider:

- providing additional guidance for CDR participants about the distinction between CDR Data and service data, and how the CDR Rules apply to each category; and
- ensuring there are no overlaps or gaps that occur in the application of the CDR Rules to CDR Data and service data.

Part C Methodology

6. Our methodology

6.1 We conducted our PIA Update broadly in accordance with the Office of the Australian Information Commissioner's *Guide to undertaking privacy impact assessments*. This involved the following steps:

Stage	Description of steps
1.	**Plan for the PIA Update:** We were provided with initial instructions about the proposed amendments to the CDR Rules, including in an initial workshop with the ACCC. We were provided with a draft of the proposed amendments to the CDR Rules, to assist us to gain an understanding of the ACCC's intentions for the proposed amendments to the CDR Rules. We also agreed on the scope of this PIA Update report (discussed further in this **Part C [Methodology]** below), the approach to undertaking a broader stakeholder consultation process, and the timeframes for the necessary activities involved in conducting this PIA Update report.
2.	**Project description and information flows:** We prepared an initial draft Project Description for the proposed amendments to the CDR Rules, which was provided to the ACCC for review to ensure that it was complete and correct. The initial draft was refined following feedback from the ACCC.
3.	**Privacy impact analysis and compliance check:** In this stage, we worked to identify and critically analyse how the proposed amendments to the CDR Rules will impact upon privacy, both positively and negatively. For the reasons elaborated in the Original CDR PIA report, we took the same approach to risk assessment which was adopted in the original CDR regime analysis, and did not endeavour to quantify or label the level of risk associated with each of the identified privacy risks.
4.	**Privacy management and addressing risks:** We worked to consider potential mitigation strategies which could further address any additional negative privacy impacts identified during the privacy impact analysis stage.
5.	**Stakeholder consultation**: A draft of a stakeholder consultation document that we prepared as a result of the above steps was published by the ACCC, together with a draft of the proposed legislative instrument to amend the CDR Rules, with an invitation to members of the public to provide written submissions in respect of either or both documents. The ACCC provided us with relevant submissions, from which we identified and considered further valuable insights.
6.	**Refinement of proposed amendments to the CDR Rules:** As a result of the feedback received from stakeholders, and the privacy risks identified in our stakeholder consultation document, the ACCC further refined its approach to amending the CDR Rules, and provided us with a further draft of the proposed amendments (with the final version being as at 4 September 2020).

Stage	Description of steps
7.	**Privacy impact analysis and compliance check, and privacy management and addressing risks:** We prepared a further Project Description to reflect the updated approach to amending the CDR Rules. We then identified and critically analysed how those proposed amendments will impact upon the privacy of individuals, both positively and negatively. We then further refined the potential mitigation strategies which could further address any additional negative privacy impacts identified during the privacy impact analysis stage.
8.	**Recommendations:** From the steps referred to above, we prepared recommendations to remove or reduce identified avoidable privacy risks.
9.	**Report:** We finalised this PIA Update report.
10.	**Respond and review:** We understand that the ACCC will review this PIA Update report, in consultation with other stakeholders as required, to respond to our recommendations.

7. Scope of this PIA Update report

7.1 The scope of this PIA Update report is limited to the proposed changes to the CDR Rules as described in **Part D [Project Description]**. As was the case with the Original CDR PIA report, this document does not include consideration of:

7.1.1 the application of the CDR regime other than its initial implementation in the banking Sector; or

7.1.2 any possible future versions of the CC Act, the Open Banking Designation, the CDR Rules or the Data Standards.

7.2 Our analysis in this document has been undertaken on the basis of our understanding of the proposed amendments to the CDR Rules, and the current "point in time" status of the CC Act, CDR Rules, Data Standards and the Open Banking Designation, as at 4 September 2020.

Part D Project Description

9. Background to the development of the changes to the CDR regime

9.1 As discussed in **Part A [Introduction]**, this Update 1 to the Original CDR PIA (**PIA Update**) is intended to complement the Original CDR PIA report published by the Department of the Treasury (**Treasury**) on 11 December 2019 (available here).

9.2 As discussed in the Original CDR PIA report[4], the ACCC is responsible for developing and administering the CDR Rules made under the CC Act.

9.3 Since the finalisation of the Original CDR PIA report, there have been several developments to CDR Rules. These include the commencement of:

9.3.1 the CDR Rules on 6 February 2020; and

9.3.2 a range of amendments to the CDR Rules on 18 June 2020, including to improve alignment between the CDR Rules and the Data Standards, and to clarify the operation of specific Rules.[5]

9.4 Whilst it was not considered necessary to update the Original CDR PIA in respect of the above changes, the ACCC (together with other agency stakeholders) has been undertaking consultations with various stakeholder groups in relation to the application of the CDR regime to the banking Sector, to further enhance and refine the CDR Rules. This has resulted in the ACCC now considering amendments to the CDR Rules, to expand the role of OSPs. The amendments will permit Accredited Data Recipients to arrange for another accredited person (who will be the Accredited Data Recipient's OSP) to collect CDR Data directly from the Data Holder on behalf of the Accredited Data Recipient.[6] The current CDR Rules contemplate an OSP only being permitted to *use* CDR Data on behalf of the Accredited Data Recipient, after the Accredited Data Recipient has received the CDR Data from the Data Holder.

9.5 The ACCC considers that these amendments may require additional consideration about any potential privacy impacts for CDR Consumers, and accordingly the ACCC commissioned this PIA Update report in order to analyse the privacy impacts of the proposed amendments to the CDR Rules.

[4] Paragraphs 9.4 and 12 of **Part D [Project Description]** of the Original CDR PIA report.
[5] The *Competition and Consumer (Consumer Data Right) Amendment Rules (No.1) 2020* are available at https://www.legislation.gov.au/Details/F2020L00757.
[6] As was the case with the Original CDR PIA report, for convenience, we have (unless specified otherwise) used "Accredited Data Recipient" in this PIA Update report to refer to an accredited person who either has, or may, receive CDR Data under the CDR regime.

10. Overview of amendments to CDR Outsourcing Arrangements

10.1 Currently, the CDR Rules specify the requirements for a CDR Outsourcing Arrangement (which is the written contract between a person (the ***discloser***) and another person to which the discloser discloses CDR Data (the ***recipient***)).[7]

10.2 The proposed amendments to the CDR Rules:

10.2.1 remove references to "disclosers" and "recipients", and instead specify that a CDR Outsourcing Arrangement is a written contract between a person (the ***Principal***) and another person (the ***Provider***)[8];

10.2.2 specify that the Provider is an OSP of the Principal;

10.2.3 introduces a concept of service data[9], which consists of any CDR Data that:

(a) was collected by the Provider from a Data Holder or the Principal in accordance with a CDR Outsourcing Arrangement; or

(b) was disclosed to the Provider in the CDR Outsourcing Arrangement for the purposes of the CDR Outsourcing Arrangement; or

(c) directly or indirectly derives from such CDR data;

10.2.4 expand the application of CDR Outsourcing Arrangements to apply to situations where the Provider (if they are an accredited person) collects CDR Data on behalf of the Principal, clarifying that a Provider may (if they are an accredited person);

(a) collect CDR Data on behalf of the Principal; and/or

(b) provide goods or services to the Principal using CDR Data disclosed to it by the Principal;

10.2.5 clarify that under a CDR Outsourcing Arrangement, a Provider may (irrespective of whether or not they are an accredited person) provide goods or services to the Principal using CDR Data disclosed to it by the Principal;

10.2.6 clarify that a Principal is taken to have disclosed CDR Data to the Provider if:

(a) the Provider is engaged under a CDR Outsourcing Arrangement to collect CDR Data on behalf of, and provide goods or services to, a Principal; and

(b) the Principal gives permission for the Provider to access or use the CDR Data;

10.2.7 expand on the requirements that a Provider is required to comply with in relation to any CDR Data, including to:

(a) require the Provider to, if directed by the Principal, provide the Principal with access to any CDR Data that it holds; and

[7] As currently drafted, the CDR Rules requires a CDR Outsourcing Agreement between any outsourced service provider and the Accredited Data Recipient, or between an outsourced service provider and its outsourced service providers.

[8] As this change is not substantive, we have not considered this further in this PIA Update report. Instead, we have focused on the effect of the more substantive changes to the CDR Rules (such as the ability for a Provider to collect CDR Data on behalf of the Principal).

[9] For the purposes of this PIA Update report, any references to 'CDR Data' include 'service data', unless expressly stated otherwise.

(b) prohibit the Provider from outsourcing the collection of CDR Data from a Data Holder; and

10.2.8 require a Principal to ensure that the Provider to the CDR Outsourcing Arrangement complies with its requirements under the CDR Outsourcing Arrangement.

10.3 In addition, the CDR Rules will expressly provide that any use or disclosure of CDR Data by a Provider under a CDR Outsourcing Arrangement is taken to have been a use or disclosure by the Principal, irrespective of whether the use or disclosure:

10.3.1 is in accordance with the CDR Outsourcing Arrangement;

10.3.2 is taken to have been by the Provider (by virtue of the fact that the Provider is in fact the Principal in another CDR Outsourcing Arrangement)[10].

10.4 For the purposes of outlining how the proposed amendments operate in the CDR regime, we have set out below a description of each stage at which the changes that are proposed to the CDR regime amend the information flows specified in the Original CDR PIA report.

11. Collection of CDR Consumer's consent

11.1 When the Principal collects the CDR Consumer's consent, the CDR Consumer must be provided with the following information:

11.1.1 a statement of the fact that the CDR Consumer's CDR Data may be collected by, or disclosed to (as relevant), an OSP;

11.1.2 a link to the accredited person's CDR policy; and

11.1.3 a statement that the CDR Consumer can obtain further information about such disclosures from the accredited person's CDR policy.[11]

12. Obtaining of Data Holder's information from ACCC CDR ICT system, sending of request to Data Holder, and redirection of CDR Consumer

12.1 Depending on the arrangements in place, and which party is to make a request to the Data Holder, the Principal or the Provider will use the ACCC CDR ICT system, so that it can obtain the technical information required to send the CDR Consumer's request to the Data Holder.

12.2 Once the technical information is obtained, either the Principal or the Provider (on behalf of the Principal) will send the consumer data request to the Data Holder. If the Provider sends the request, we understand that it may notify the Principal that the request has been made.

12.3 The Principal, or the Provider (using the information provided to it by the Principal), will redirect the CDR Consumer to the Data Holder's systems. In accordance with the information flows in the Original CDR PIA, at this stage the CDR Consumer will use a one-time password and their usual banking credentials in the Data Holder's systems.

[10] The proposed new Rule 7.6(2)(b)(ii) refers to "another CDR outsourcing arrangement". The intention of this wording is somewhat unclear – please see our analysis in **Item 2** of **Part E [Analysis of Risks]**.
[11] The wording in Rule 4.11(3)(f) refers to "the accredited person's CDR policy". Again, the intention of this wording is somewhat unclear in the circumstances where both the Principal and the Provider will be accredited persons – please see our analysis in **Item 5** of **Part E [Analysis of Risks]**.

13. Data Holder uses the ACCC CDR ICT system to check credentials of, the Principal, Provider, or both (as relevant)

13.1 From the proposed amendments to the CDR Rules, it is not clear to us whether the Data Holder will check the credentials (that is, the ICT security certificates) of the Principal (if the Provider is using the Principal's software product), the Provider (if the Provider is using its own software product), or both (including which entities the Data Holder will check to ensure that their accreditation has not been surrendered, suspended or revoked). We understand that the ACCC intends that this will be addressed through the technical implementation of the ACCC CDR ICT system.

13.2 However, in all cases, the Data Holder will obtain the technical information required to communicate with the Provider (who will be acting on behalf of the Principal), using the ACCC CDR ICT system (and Accreditation Register).

14. Data Holder discloses CDR Data

14.1 The Data Holder will then technically send the CDR Data to the Provider, and that Provider will accordingly collect that CDR Data, on behalf of the Principal. From the Data Holder's perspective, if the Provider uses the credentials of the Principal, the Data Holder will not necessarily be aware that it is sending the CDR Data to the Provider, rather than the Principal.

Provider collects CDR Data from the Data Holder

14.2 Depending on the CDR Outsourcing Arrangement, as discussed in paragraph 10.2.4 of this **Part D [Project Description]**:

14.2.1 the Provider may simply collect the CDR Data (on behalf of the Principal) from the Data Holder and then disclose that CDR Data to the Principal; or

14.2.2 the Provider may collect the CDR Data (on behalf of the Principal) from the Data Holder, and the Principal may give permission to the Provider to access or use the CDR Data, in order for the Provider to provide goods or services to the Principal.

Provider uses CDR Data

14.3 If the Provider has received permission from the Provider to access or use the CDR Data it has collected on behalf of the Principal, then, before the Provider discloses the CDR Data to the Principal (and the Principal collects that CDR Data), the Provider may, in accordance with its CDR Outsourcing Arrangement with the Principal:

14.3.1 use the CDR Data to provide the goods or services to the Principal;

14.3.2 disclose the CDR Data to its outsourced service providers under CDR Outsourcing Arrangements; and

14.3.3 disclose de-identified data to third parties.

Provider discloses CDR Data to the Principal

14.4 In accordance with the CDR Outsourcing Arrangement, the Provider will disclose the CDR Data to the Principal, either:

14.4.1 after collecting the CDR Data (on behalf of the Principal) from the Data Holder; or

14.4.2 after collecting the CDR Data (on behalf of the Principal) from the Data Holder, and if it receives permission from the Principal, after accessing or using the CDR Data.

14.5 The proposed amendments to the CDR Rules will require:

14.5.1 transfer of CDR Data between the Provider and Principal to be encrypted;

14.5.2 the Provider to ensure that any CDR Data it stores or hosts for a Principal is segregated,

in accordance with the requirements specified in Schedule 2 to the CDR Rules.

15. Withdrawal or expiry of CDR Consumer's consent

15.1 There are no changes proposed to the CDR Rules about withdrawal or expiry of consent. The CDR Consumer may withdraw their consent at any time by communicating the withdrawal to the Principal or by using the Principal's Consumer Dashboard.

15.2 It is not clear to us whether the proposed amendments to the CDR Rules require CDR Outsourcing Arrangements to specify the mechanisms by which each party will be made aware of any withdrawal or expiry of a CDR Consumer's consent.

16. Withdrawal or expiry of CDR Consumer's authorisation

16.1 There are no changes proposed to the CDR Rules about withdrawal or expiry of authorisation. The CDR Consumer may withdraw their authorisation by communicating the withdrawal to the Data Holder or by using the Data Holder's Consumer Dashboard.

17. Suspension, revocation or surrender of accreditation

17.1 There are no changes proposed to the CDR Rules about the suspension, revocation or surrender of accreditation.

18. Additional changes to the CDR Rules

18.1 The Privacy Safeguards in the CDR Rules will also be changed as follows:

18.1.1 **Privacy Safeguard 1 (open and transparent management of CDR Data)** will be changed to clarify that the Principal's and the Provider's CDR Policy must include a list of their OSPs (whether based in Australia or based overseas, and whether or not any is an accredited person).

18.1.2 **Privacy Safeguard 5 (notifying of the collection of CDR Data)** will only apply to a Principal, if the Provider collects CDR Data (on behalf of the Principal) from a Data Holder under a CDR Outsourcing Arrangement.

18.1.3 **Privacy Safeguard 10 (notifying of the disclosure of CDR Data)** will only apply to a Principal, if the Provider collects CDR Data (on behalf of the Principal) from a Data Holder under a CDR Outsourcing Arrangement.

18.2 The proposed amendments also expand certain requirements in the CDR Rules, such as:

18.2.1 expanding a step in the CDR Data deletion process to apply to Providers who have collected CDR Data on behalf of the Principal; and

18.2.2 requiring the Principal and Provider to keep and maintain records that record and explain any arrangements that may result in CDR Data being collected by, or disclosed to, OSPs, including copies of agreements with the OSPs.

Part E Analysis of Risks

19. Introduction

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

19.2 For convenience, we have grouped the following information flows and concepts[12], which may involve new or changed privacy considerations in addition to those identified in the Original CDR PIA report:

19.2.1 CDR Outsourcing Arrangements;

19.2.2 collection of CDR Consumer's consent;

19.2.3 obtaining of Data Holder's information from ACCC CDR ICT system, sending of request to Data Holder, and redirection of CDR Consumer;

19.2.4 Data Holder uses the ACCC CDR ICT system to check credentials of the Principal, the Provider, or both (as relevant);

19.2.5 Data Holder discloses CDR Data to Provider, and Provider collects that CDR Data;

19.2.6 Provider discloses CDR Data to Principal;

19.2.7 withdrawal or expiry of CDR Consumer's consent;

19.2.8 withdrawal or expiry of CDR Consumer's authorisation;

19.2.9 suspension, revocation or surrender of accreditation; and

19.2.10 additional changes to the CDR Rules, and other identified risks.

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

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

CDR Outsourcing Arrangements

CDR OUTSOURCING ARRANGEMENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**Confusion over liability regime in CDR Rules, and which obligations apply to either the Principal, the Provider, or both** Despite the amendments to Rule 7.6(2), it is still unclear which obligations in the CDR regime apply to the Principal and/or the Provider (noting both will be accredited persons), including in relation to the collection of CDR Data by the Provider (on behalf of the Principal). Further, there may be confusion about liability of a Provider's OSPs, and whether the Principal or the Provider is responsible.	The proposed amendments to the CDR Rules (Rule 7.6(2)) will expressly provide that any use or disclosure of CDR Data by a Provider under a CDR Outsourcing Arrangement is taken to have been a use or disclosure by the Principal, irrespective of whether the use or disclosure: • is in accordance with the CDR Outsourcing Arrangement (Rule 7.6(2)(b)(i)); and • is taken to have been by the Provider (by virtue of the fact that the Provider is in fact the Principal in another CDR Outsourcing Arrangement) (Rule 7.6(2)(b)(ii)). In relation to situations where the Provider collects CDR Data from the Data Holder (on behalf of the Principal), the following mitigations will apply: • the Provider will be accredited in accordance with the CDR Rules;	Although the proposed amendments set out that the Principal is responsible for any use or disclosure of the Provider, it does not clearly specify that the Provider is liable for its collection of the CDR Data from the Data Holder (on behalf of the Principal). Further, it is difficult to ascertain from the proposed amendments which obligations in the CDR Rules apply to the Principal and/or the Provider (as they will both be accredited persons). In addition, the proposed wording in Rule 7.6(2)(b)(ii) is confusing, as it is unclear whether "another CDR Outsourcing Arrangement" is intended to refer to another CDR Outsourcing Arrangement between the Provider and its OSPs related to the same CDR Consumer/consent process (i.e. a further subcontracting arrangement), or if this intended to refer to any other CDR Outsourcing Arrangement the Provider may have in its right as an Accredited Data Recipient (i.e. in relation to other CDR Consumers). Accordingly, we **recommend** that the ACCC clarify: • whether the Provider is liable for its collection of CDR Data from the Data Holder (not the Principal on whose behalf it is making that collection);

	Stakeholder discussion on related issues Some stakeholders expressed that the ACCC should consider ensuring that the CDR Rules clearly apportion liability between the Provider and the Principal. One stakeholder commented "*[t]he Principal should not be responsible for trying to negotiate into a [CDR Outsourcing Arrangement] a liability package that appropriately and proportionally allocates liability...*" (The Australian Banking Association). However, some other stakeholders submitted that the apportionment of liability should be dealt with in the individual contractual arrangements between the Provider and the Principal (i.e. the CDR Outsourcing Arrangements) rather than specifying requirements for those contracts in the CDR Rules. One stakeholder submitted "*the CDR Rules need to allow for a flexible approach to allow Providers and Principals to contractually determine the obligations and liabilities each of them should*	• the Provider will be obliged to comply with Schedule 2 to the CDR Rules; and • the Provider cannot further outsource the collection of the CDR Data from the Data Holder (Rule 1.10(2)(b)(iv)). The proposed amendments to the CDR Rules will also require the Principal to ensure that the Provider complies with its requirements under the CDR Outsourcing Arrangement (Rule 1.16(1)), which must include a requirement that the Provider: • can only disclose CDR Data under further CDR Outsourcing Arrangements with its OSPs; and • must ensure those OSPs comply with the requirements of those arrangements.	• which obligations in the CDR Rules apply to the Principal and/or the Provider (noting that both will be accredited persons); and • the intention of the proposed amendments to Rule 7.6(2)(b)(ii), and specify whether it is intended to apply to further CDR Outsourcing Arrangements of the Provider in relation to that CDR Consumer, or additional CDR Outsourcing Arrangements of the Provider for other CDR Consumers. (**Recommendation 1**)

CDR OUTSOURCING ARRANGEMENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	bear according to the arrangement" (Intuit).		
2.	**The CDR Rules do not expressly require CDR Outsourcing Arrangements to deal with communication between the Principal and the Provider about a CDR Consumer's consent** The CDR Rules contain requirements for what should be contained in CDR Outsourced Arrangements, but do not specify any mandatory provisions relating to communication of information about a CDR Consumer's consent or withdrawal of their consent.	Both parties to CDR Outsourcing Arrangements are already Accredited Data Recipients in their own right and are therefore already subject to a range of obligations under the CDR regime, including in relation to a CDR Consumer's consent. The penalties for a breach by an Accredited Data Recipient will be an incentive for the Principal and Provider to ensure that their CDR Outsourcing Arrangement contains all necessary requirements to ensure compliance with their legislative obligations.	Given the importance of effectively and accurately communicating the CDR Consumer's consent (and the role of their consent in the CDR regime), we **recommend** that CDR Outsourcing Arrangements be expressly required to contain an obligation: • upon the Principal to accurately communicate the CDR Consumer's consent to the Provider; • upon the Provider to collect CDR Data from the Data Holder in accordance with the consent provided by the CDR Consumer, and communicated by the Principal; and • upon the Principal to notify the Provider if the Principal becomes aware that the CDR Consumer has withdrawn their consent or authorisation, so that the Provider does not inadvertently continue to use or disclose CDR Data without an appropriate consent and authorisation. (**Recommendation 2**)

Collection of CDR Consumer's consent

COLLECTION OF CDR CONSUMER'S CONSENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
3.	**Security of the communication pathway between the Principal and the Provider for non-CDR Data about the CDR Consumer** There is a risk that the communication pathway between the Principal and Provider is not secure, or is compromised, when the CDR Consumer's consent and, if relevant, the CDR Consumer's contact information, is communicated between the parties.	As this information will not be considered to be CDR Data, the protections of the CDR Rules do not apply. If the Principal and the Provider are APP entities, then the APPs (including APP 11) will apply to the personal information (such as the contact information of the CDR Consumer). Further, section 79 in the Privacy Act applies the Privacy Act to small business operators (once they become accredited under the CDR regime) as if they were an 'organisation' under the Privacy Act, in relation to any personal information that is not CDR Data. The proposed amendments will include high level obligations in Schedule 2, which the Principal and the Provider must comply with in relation to CDR Data. These obligations include requiring the implementation of robust network security controls to help protect data in transit, including encrypting that data.	It is not entirely clear whether the parties to a CDR Outsourcing Arrangement are required to ensure that additional protections contained in the proposed amendments in Schedule 2 will also be used by the parties to transfer non-CDR Data. This is important because any non-CDR Data in transit (such as the CDR Consumer's contact information, or their consent) is not CDR Data and is therefore not afforded the protections in Schedule 2. We **recommend** that the ACCC should consider whether the legislative framework should contain specific technical requirements for any communications that occur between the Principal and the Provider for information that is not CDR Data (such as information about a CDR Consumer's consent, or their contact information). These requirements could be specified in the proposed amendments to the CDR Rules regarding the content of CDR Outsourcing Arrangements. This would further assist to ensure that the information is appropriately protected (**Recommendation 2**). ***Stakeholder discussion on related issues*** Stakeholders acknowledged that the CDR Rules, as currently drafted, contain gap regarding the security of the communication pathway. Additionally, the majority of stakeholder supported the inclusion for information to be encrypted in transit. Some stakeholders suggested that the CDR Rules should specify how data should be encrypted in

COLLECTION OF CDR CONSUMER'S CONSENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			transit, with one stakeholder expressing that "*Schedule 2 does not contain particulars about encryption of data in transit, allowing for interpretation in different ways by different participants*" (Xero Australia Pty Ltd). Another stakeholder noted that "*if the security controls [regarding encryption in transit] are left open to interpretation, it will also create potential auditing issues and leave decisions open to technical disputes*" (Australian Business Software Industry Association). Further, another stakeholder voiced that it is unclear whether the minimum controls apply data being transferred within its internal environment (RSM Australia Pty Ltd). One stakeholder noted that "*all data should ideally also be encrypted when at rest*" (Office of Victorian Information Commissioner). Stakeholders suggested that data segregation would act as a protection mechanism for non-CDR Data. One stakeholder provided data segregation would "*further enhance the privacy protection provided to non-CDR data – for example, by limiting the dissemination of that information, and by limiting the exposure of non-CDR data in the event of a breach*" (Office of Victorian Information Commissioner).

COLLECTION OF CDR CONSUMER'S CONSENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
4.	**Details of CDR Consumer's consent and contact information not accurately transferred from Principal to Provider** When the Principal collects the CDR Consumer's consent, it will need to transfer to the Provider the details of the CDR Consumer's consent and/or their contact information. There is a risk that the transmission of information about the CDR Consumer from the Principal (about the consent or their contact information) to the Provider is not accurate (so that the Provider seeks information about the 'wrong' Data Holder from the ACCC CDR ICT system).	See ***Item 3*** above.	See ***Item 3*** above.

COLLECTION OF CDR CONSUMER'S CONSENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
5.	**CDR Consumer unaware of that the Provider will be collecting their CDR Data, not the Principal (i.e. to whom they are providing their consent)** There is a risk that a CDR Consumer will not understand the role of the Provider in relation to the handling of their CDR Data.	If a Principal will be using a Provider under a CDR Outsourcing Arrangement, the proposed amendments to CDR Rules (Rule 4.11(3)(f)) require the CDR Consumer to be provided with the following information when providing their consent: • a statement of the fact that the CDR Consumer's CDR Data may be collected by, or disclosed to (as relevant), an OSP; • a link to the accredited person's CDR policy; and • a statement that the CDR Consumer can obtain further information about such disclosures from the accredited person's CDR policy. Further, the CDR Rules provide that an Accredited Data Recipient's CDR policy must list all Providers with which the Principal has a CDR Outsourcing Arrangement.	We consider that the requirements in relation to the information provided to a CDR Consumer when they give their consent are unclear. This is because it is not clear whether (for example) the Principal (when asking for consent) needs to provide a link to the Principal's CDR Policy, the Provider's CDR Policy, or both. It is also not clear whether the Principal needs to disclose the name of the Provider handling the CDR Consumer's CDR Data, or can simply provide a general statement that "an OSP" may be used (see Rule 4.11(3)(f)(i)). In addition, the CDR Consumer may be unaware that an OSP may use the CDR Data. Further, the information provided to a CDR Consumer will not ensure that they know which of the listed Providers will be handling their CDR Data, noting that the CDR Consumer may not remember which OSPs were listed when they gave their consent (given the amount of information they are provided at the time they provide their consent). We acknowledge the importance of avoiding "information overload", but note that this must be balanced against ensuring the CDR Consumers are fully informed about how their CDR Data will be handled. Accordingly, we **recommend** that: • the ACCC clarify whether the references to 'the accredited person's CDR Policy' in Rule 4.11(3)(f)(ii) and (iii) are meant to refer to the

COLLECTION OF CDR CONSUMER'S CONSENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			Principal, the Provider if they are an accredited person, or both; • Rule 4.11(3)(f)(iii) is amended to specify that the CDR Consumer can obtain further information about the specific Provider's *collections, uses* and disclosures from the Principal's CDR Policy; and • the CDR Consumer is informed that their CDR Data may be collected by, disclosed to, or *used by*, the specific Provider. (**Recommendation 4**) To ensure openness and transparency with the CDR Consumer, we **recommend** that the ACCC consider whether, through the Principal's Consumer Dashboard, CDR Consumers should be provided with more granular information (e.g. Provider "X" will be used to collect CDR Data from Data Holder "X") (**Recommendation 5**). ***Stakeholder discussion on related issues*** This recommendation is supported by some feedback from stakeholders, who emphasised the importance of openness and transparency. For example, one stakeholder stated that "*Rule 7.4 could be further bolstered, to the benefit of the consumer, by requiring the principal to specify in the consumer dashboard which provider collected the consumer's CDR data*" (Office of Victorian Information Commissioner).

COLLECTION OF CDR CONSUMER'S CONSENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			Several stakeholders expressed that a CDR Consumer could experience "information overload" if they received information about both the Principal and the Provider when providing their consent. These stakeholders suggested that this information overload could result in CDR Consumers not providing fully informed consent. For example, stakeholders stated that: • "*it would be a confusing experience for consumers to see the [provider] name along with the name of the financial institution, due to a [CDR Outsourcing Arrangement], when being asked to share their data. This has the potential to erode trust in Open Banking and discourage consumers from sharing their data*" (Data Action Pty Ltd); • "*…a significant amount of information needs to be disclosed in the consent flow and as a consequence, …consumers may not fully understand who they have consented to share their data with*" (NAB); • "*There is a significant volume of information which is mandated to be included in the consent flow via Rule 4.11(3)(i) which may make it complex for the consumer to comprehend and potentially impede the consumer's ability to provide informed consent*" (Australian Banking Association); and • "*the Provider should be mentioned, their accreditation number displayed, links to websites, privacy policy should be available to the Consumer but not in a way that clashes with the principal*" (SISS Data Services Pty Limited). One stakeholder suggested, as an alternative, that "*it may be more beneficial to present a statement that the principal*

COLLECTION OF CDR CONSUMER'S CONSENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			may use third parties to collect their CDR data and their names are disclosed in their Privacy Statements or Policies" (Cuscal Limited).
6.	The Original CDR PIA report discusses the risks associated with the collection of the CDR Consumer's consent (See ***Step 1B in the Original CDR PIA report***), which will also apply to situations where the Principal (as relevant) collects the CDR Consumer's consent.	*See Original CDR PIA report.*	*See Original CDR PIA report.*

Obtaining of Data Holder's information from ACCC CDR ICT system, sending of request to Data Holder, and redirection of CDR Consumer

OBTAINING OF DATA HOLDER'S INFORMATION FROM ACCC CDR ICT SYSTEM, SENDING OF REQUEST TO DATA HOLDER, AND REDIRECTION OF CDR CONSUMER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
7.	**Technical information does not match the CDR Consumer's consent** If, as discussed in ***Item 4*** above, the information about the CDR Consumer and their consent is not correctly transferred from the Principal to the Provider, there is a risk that the technical information obtained by the Provider does not match the requirements of the consent provided by the CDR Consumer to the Principal (so that the request received by the Data Holder does not match the consent provided by the CDR Consumer).	See ***Item 4***.	See ***Item 4***.

OBTAINING OF DATA HOLDER'S INFORMATION FROM ACCC CDR ICT SYSTEM, SENDING OF REQUEST TO DATA HOLDER, AND REDIRECTION OF CDR CONSUMER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
8.	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient using the ACCC CDR ICT system (see ***Step 2 in the Original CDR PIA report***), which will also apply to situations where the Principal or the Provider (as relevant) uses the ACCC CDR ICT system.	*See Original CDR PIA report.*	*See Original CDR PIA report.*
9.	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient sending the consumer data request to the Data Holder and redirecting the CDR Consumer (see ***Step 3 in the Original CDR PIA report***), which will also apply to situations where the Principal or the Provider (as relevant) sends the request and redirects the CDR Consumer.	*See Original CDR PIA report.*	*See Original CDR PIA report.*

Data Holder uses the ACCC CDR ICT system to check credentials of, the Principal, Provider, or both (as relevant)

DATA HOLDER USES THE ACCC CDR ICT SYSTEM TO CHECK CREDENTIALS OF, THE PRINCIPAL, PROVIDER, OR BOTH (AS RELEVANT)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
10.	**Data Holder sends CDR Data to an Accredited Data Recipient that is no longer accredited** It is not clear if the Data Holder will check both the Provider and Principal's credentials, including whether each accreditation has expired or been suspended or revoked.	Accredited Data Recipients may only disclose CDR Data to another entity that is an Accredited Data Recipient (therefore if a Provider discloses CDR Data to an entity that is not an Accredited Data Recipient they will have breached the requirements of the CDR legislation).	There are currently no obligations on the Provider to check the status of the Principal's accreditation. Although it would be a breach of the CDR legislation to disclose CDR Data to an entity that is not an Accredited Data Recipient, it would be preferable if the CDR regime had safeguards to prevent this disclosure in the first place. Accordingly, we **recommend** that the ACCC consider whether Data Holders should know whether the Accredited Data Recipient is acting in the role of a Provider or a Principal. The Data Holder could then be required to check the accreditation for both the Provider and the Principal, including whether each accreditation has been surrendered, suspended or revoked (**Recommendation 7**). Alternatively, the Provider could be required to check the accreditation of the Principal before it discloses any CDR Data to that Principal (**Recommendation 8**).

DATA HOLDER USES THE ACCC CDR ICT SYSTEM TO CHECK CREDENTIALS OF, THE PRINCIPAL, PROVIDER, OR BOTH (AS RELEVANT)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			Stakeholder discussion on related issues Some stakeholders emphasised that it was necessary "*to ensure that CDR data is not disclosed to an entity whose accreditation has been surrendered, suspended or revoked – particularly given a collection of CDR data by a provider is taken to be a collection by the Principal*" (Office of Victorian Information Commissioner).
11.	**Misuse of Principal's credentials by Provider** It is unclear whether there may be situations in which a Provider could use the credentials of a Principal (i.e. the "PKI certificate" for the ACCC CDR ICT system) for purposes outside of those in the CDR Outsourcing Arrangement.	If a Principal is to engage a Provider, there must be a CDR Outsourcing Arrangement between the parties. In addition, Accredited Data Recipients must accept terms and conditions before being permitted to use a PKI certificate for the ACCC CDR ICT system. We understand that these terms include obligations on the Accredited Data Recipient to ensure that the credential is kept securely and that measures are implemented to prevent unauthorised access.	The proposed CDR Rules do not currently expressly permit, or prohibit, the use of a Principal's credentials by a Provider. If such a use of the Principal's credentials is to be permitted, we **recommend** that the ACCC consider amending the CDR Rules to require CDR Outsourcing Arrangements to contain strict obligations in relation to the use of the Principal's credentials by the Provider. If it is not intended that the Provider can use the Principal's credentials, we **recommend** that the CDR Rules expressly prohibit this use (**Recommendation 6**).

DATA HOLDER USES THE ACCC CDR ICT SYSTEM TO CHECK CREDENTIALS OF, THE PRINCIPAL, PROVIDER, OR BOTH (AS RELEVANT)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
12.	The Original CDR PIA report discusses the risks associated with the Data Holder checking the credentials of the Accredited Data Recipient (see ***Step 5 in the Original CDR PIA report*****),** which will also apply to situations where the Provider is to collect the CDR Data from the Data Holder.	*See Original CDR PIA report.*	*See Original CDR PIA report.*

Data Holder discloses CDR Data to Provider, and Provider collects that CDR Data

DATA HOLDER DISCLOSES CDR DATA TO PROVIDER, AND PROVIDER COLLECTS THAT CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
13.	The Original CDR PIA report discusses the risks associated with the Data Holder disclosing CDR Data to Accredited Data Recipient (see ***Step 6 in the Original CDR PIA report***), which will also apply to situations where CDR Data is disclosed to the Provider.	*See Original CDR PIA report.*	*See Original CDR PIA report.*
14.	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient using CDR Data (see ***Step 7A in the Original CDR PIA report***), which will also apply to situations where the Provider uses the CDR Consumer's CDR Data after receiving it from the Data Holder or from the Principal (as relevant).	*See Original CDR PIA report.* In addition, the Provider must only use the CDR Data in accordance with its CDR Outsourcing Arrangement with the Principal. The proposed amendments to the CDR Rules mean that any use or disclosure of CDR Data by a Provider under a CDR Outsourcing Arrangement is taken to have been a use or disclosure by the Principal.	*See Original CDR PIA report.*

DATA HOLDER DISCLOSES CDR DATA TO PROVIDER, AND PROVIDER COLLECTS THAT CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
15.	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient disclosing CDR Data to its outsourced service providers (see ***Step 7C in the Original CDR PIA report***), which will also apply to situations where the Provider discloses CDR Data to its outsourced service providers.	*See Original CDR PIA report.* In addition, the Provider must only use the CDR Data in accordance with its CDR Outsourcing Arrangement with the Principal. The proposed amendments to the CDR Rules will also require the Principal to ensure that the Provider complies with its requirements under the CDR Outsourcing Arrangement (Rule 1.16(1)), which must include a requirement that the Provider: • can only disclose CDR Data under further CDR Outsourcing Arrangements with its OSPs; and • must ensure those OSPs comply with the requirements of those arrangements. Further, the proposed amendments to the CDR Rules mean that any use or disclosure of CDR Data by a Provider under a CDR Outsourcing Arrangement is taken to have been a use or disclosure by the Principal.	*See Original CDR PIA report.*

DATA HOLDER DISCLOSES CDR DATA TO PROVIDER, AND PROVIDER COLLECTS THAT CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
16.	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient disclosing de-identified data to third parties (see ***Step 7D in the Original CDR PIA report***), which will also apply to situations where the Provider discloses de-identified data to third parties.	*See Original CDR PIA report.* In addition, the Provider must only use the CDR Data in accordance with its CDR Outsourcing Arrangement with the Principal. The proposed amendments to the CDR Rules mean that any use or disclosure of CDR Data by a Provider under a CDR Outsourcing Arrangement is taken to have been a use or disclosure by the Principal.	*See Original CDR PIA report.*

Provider discloses CDR Data to Principal

PROVIDER DISCLOSES CDR DATA TO PRINCIPAL			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
17.	**Pathway security between the Provider and the Principal is compromised** There is a risk that the pathways used by the Provider to communicate with, and send CDR Data to, the Principal could be compromised.	The proposed amendments will include high level obligations in Schedule 2, which the Principal and the Provider must comply with in relation to CDR Data. These obligations include requiring the implementation of robust network security controls to help protect data in transit, including encrypting that data.	
18.	**Incorrect recipient of CDR Data** There is a risk that CDR Data is sent to the incorrect Accredited Data Recipient, particularly if the Provider is the Provider for several Principals (and therefore has multiple CDR Outsourcing Arrangements).	PS 4 requires an Accredited Data Recipient that receives unsolicited CDR Data to destroy it as soon as practicable (in the case that the Provider provides the CDR Data to the 'wrong' Accredited Data Recipient). The proposed amendments to the CDR Rules will require the Provider to ensure that any CDR Data it stores or hosts for a Principal is segregated in accordance with the requirements specified in Schedule 2 to the CDR Rules. This will include the Provider ensuring that the CDR Data:	We consider that the segregation of CDR Data by the Provider for CDR Data reduces the risks of CDR Data being sent to the incorrect Accredited Data Recipient. However, as an additional mitigation strategy, we **recommend** that the ACCC consider whether it would be appropriate for the CDR Rules to contain requirements for the Provider, before disclosing any CDR Data, to check that the technical details it is going to use for the disclosure of the CDR Data match up with the Principal on whose behalf it collected the CDR Data from the Data Holder, or the Principal who disclosed the CDR Data to it (**Recommendation 8**).

PROVIDER DISCLOSES CDR DATA TO PRINCIPAL			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		• is only accessible by the Principal to whom the CDR Consumer provided their consent; and • remains directly attributable to that Principal.	***Stakeholder discussion on related issues*** One stakeholder noted that "*Providers [should] check the credentials (status) of a Principal before providing data to the Principal…in order to maintain confidence in the CDR regime. As there can be time gaps between the provider collecting data to when it is sent to the principal this requirement ensures only ADRs with proper accreditation are in receipt of CDR data*" (SISS Data Services Pty Limited).

Withdrawal or expiry of CDR Consumer's consent

WITHDRAWAL OR EXPIRY OF CDR CONSUMER'S CONSENT			
a	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
19.	**Withdrawal or expiry of CDR Consumer's consent not communicated** There is a risk that the CDR Consumer only notifies the Principal that they have withdrawn their consent (or it has expired), and the Principal does not notify the Provider to inform them of the withdrawal or expiry of the CDR Consumer's consent. This could then result in the CDR Consumer's CDR Data being collected, used or disclosed after the CDR Consumer has withdrawn their consent, or it has expired.		The proposed amendments to the CDR Rules do not require the CDR Outsourcing Arrangements to contain an obligation on the Principal to notify the Provider if the CDR Consumer withdraws their consent, or their consent otherwise expires. Accordingly, as specified in ***Item 2,*** we **recommend** that the ACCC consider specifying in the proposed amendments to the CDR Rules the requirement for CDR Outsourcing Arrangements to include a mechanism or process to ensure the Principal notifies the Provider of the withdrawal or expiry of a CDR Consumer's consent (**Recommendation 2**). The CDR Rules could also be amended to include an express obligation on the Principal to the CDR Outsourcing Arrangement to notify the Provider of the withdrawal or expiry of a consent. This would strengthen the privacy protections by not simply relying on the Accredited Data Recipients complying with, and enforcing, contractual obligations (**Recommendation 3**). ***Stakeholder discussion on related issues*** One stakeholder noted the "*need for bespoke obligations pertaining to the management of customer consents as between the principal provider. At minimum, the CDR Rules should mandate that, where the provider collects or manages customer consents on behalf of the principal*

WITHDRAWAL OR EXPIRY OF CDR CONSUMER'S CONSENT			
a	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			under a [CDR Outsourcing Arrangement], the provider must keep the principal updated on any changes to those consents…There should be sufficient safeguards in the rules to ensure that the principal has accurate and complete consumer consent information…" (Prospa). That stakeholder also noted that "*the Rules should also clarify the processes for managing consent where the accreditation of either party has been suspended, including, for instance, that status of any changes to a particular customer's consent during the period of suspension."* For instance, where "*the consent is provided to the principal, the principal should be able to continue to rely on consent where the provider's accreditation is suspended. Conversely,…a provider cannot rely on a customer's consent where either party's accreditation has been suspended*".
20.	The Original CDR PIA report discusses the risks associated with the withdrawal or expiry of the CDR Consumer's consent (see ***Step 8 in the Original CDR PIA report***), which will also apply to situations where a Principal engages a Provider under a CDR Outsourcing Arrangement.	*See Original CDR PIA report.*	*See Original CDR PIA report.*

Withdrawal or expiry of CDR Consumer's authorisation

WITHDRAWAL OR EXPIRY OF CDR CONSUMER'S AUTHORISATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
21.	**Withdrawal or expiry of CDR Consumer's authorisation not communicated** There is a risk that one party to a CDR Outsourcing Arrangement does not notify the other party to inform them of the withdrawal or expiry of the CDR Consumer's authorisation. This could then result in the CDR Consumer's CDR Data being used or disclosed after they have withdrawn their authorisation, or it has expired.	See ***Item 19.***	See ***Item 19.*** Further, we understand that there is still uncertainty around whether the Data Holder will know whether it is providing CDR Data to an Accredited Data Recipient, or a Provider who is collecting CDR Data for a Principal under a CDR Outsourcing Arrangement, or whether it will know which Accredited Data Recipient is the Principal. If the Data Holder does not know that it is providing CDR Data to a Provider (and therefore does not know it is informing a Provider of the withdrawal or expiry of the CDR Consumer's authorisation), or know which Accredited Data Recipient is the Principal, there is a risk of disconnect, as the Provider may not notify the Principal of the authorisation ending, and the Data Holder has no ability to also notify the Principal of this fact. Accordingly, we **recommend** that the ACCC consider whether Data Holders should know whether the Accredited Data Recipient is acting in the role of a Provider or a Principal, and then accordingly be required to notify the Principal *and* the Provider if the CDR Consumer's authorisation is withdrawn or expires (**Recommendation 7**).

WITHDRAWAL OR EXPIRY OF CDR CONSUMER'S AUTHORISATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
22.	The Original CDR PIA report discusses the risks associated with the withdrawal or expiry of the CDR Consumer's authorisation (see ***Step 9 in the Original CDR PIA report***), which will also apply to situations where a Principal engages a Provider under a CDR Outsourcing Arrangement.	*See Original CDR PIA report.*	*See Original CDR PIA report.*

Suspension, revocation or surrender of accreditation

SUSPENSION, REVOCATION OR SURRENDER OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**

23.	**Continued use of CDR Data by, or disclosure to, previously-accredited data recipient (either Principal or Provider), after accreditation ends**
	
	There is a risk that a previously-accredited data recipient (either the Provider or the Principal) continues to use or disclose CDR Data received from a Data Holder, after the suspension, revocation or surrender of the accreditation of the other party to the CDR Outsourcing Arrangement (either the Principal or the Provider, as relevant).
		The ACCC intends that the technical implementation of the ACCC CDR ICT system will assist in mitigating the identified risk.
		
		Further, the CDR Rules provide that if an Accredited Data Recipient's accreditation has been surrendered or revoked, they must delete or de-identify the CDR Data by taking the steps specified in Rules 7.12 and 7.13. The proposed amendments to the CDR Rules require the Provider to delete CDR Data in accordance with the CDR Data deletion process, if directed by the Principal (Rule 7.12).
		
		We also note that the Data Recipient Accreditor must notify the Accreditation Registrar about information relating to accreditations of Accredited Data Recipients, including of any surrender, suspension or revocation (Rule 5.15). The Accreditation Registrar must then update the Accreditation Register to reflect these details (Rule 5.24).
			Noting the seriousness of this risk, we **recommend** that the ACCC consider whether the CDR Rules should clearly provide further protections for CDR Consumers, which could include:
			
			• requiring, if either the Principal's, or the Provider's, accreditation is suspended, revoked or surrendered (**previously-accredited data recipient**):
			  ○ the previously-accredited data recipient must notify the other Accredited Data Recipient (i.e. the Principal or the Provider, as relevant) of the fact that it is no longer accredited; and
			  ○ the CDR Consumer must be notified of that fact by either:
			  ▪ the previously-accredited data recipient; or
			  ▪ the other Accredited Data Recipient,
			  as agreed in the CDR Outsourcing Arrangement; and
			• broadening the obligations in the CDR Rules so that, if a party to a CDR Outsourcing Arrangement is notified regarding the other party (i.e. the previously-accredited data recipient is no longer accredited), they must not continue to collect or use CDR Data and clarifying the requirements to treat that CDR Data as redundant data.

SUSPENSION, REVOCATION OR SURRENDER OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			If the ACCC intends to implement systems (e.g. through the ACCC CDR ICT system), which will ensure anyone using the Principal's credentials (including a Provider) is notified of a suspension, revocation or surrender of the Principal's accreditation, this functionality should be clearly communicated to CDR Consumers. (**Recommendation 9**) ***Stakeholder discussion of related issues*** Stakeholders noted the importance of the CDR Rules requiring the parties to a CDR Outsourcing Arrangement to communicate their accreditation to each other. One stakeholder expressed that the CDR Rules (and related guidance) should include *"obligations of the principal or provider to delete or deidentify CDR data subject to a [CDR Outsourcing Arrangement], where the other party's accreditation has been suspended or revoked"* (Office of Victorian Information Commissioner).

SUSPENSION, REVOCATION OR SURRENDER OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
24.	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient's accreditation being suspended, revoked, or surrendered (see ***Step 10 in the Original CDR PIA report***), which will also apply to situations where a Provider surrenders their accreditation, or their accreditation is suspended or revoked.	*See Original CDR PIA report.*	*See Original CDR PIA report.*

Additional changes to the CDR Rules, and other identified risks

ADDITIONAL CHANGES TO THE CDR RULES, AND OTHER IDENTIFIED RISKS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
25.	**Confusion over 'collection' of CDR Data from Data Holder** There may be confusion as to when a Principal will be considered to have 'collected' CDR Data. That is, does the Principal 'collect' the CDR Data when it is received by the Provider (given the Provider is collecting 'on behalf of the Principal') or when the Provider provides the CDR Data to the Principal.	It appears that if a Provider collects CDR Data on behalf of a Principal from a Data Holder, this will be considered to be a collection by the Provider, and then when the Provider discloses that CDR Data to the Principal, this is the stage at which the Principal will collect that CDR Data. We have deduced this based on the proposed amendment to Rule 7.5, which states a permitted use or disclosure includes when a Provider in a CDR Outsourcing Arrangement discloses CDR Data to the Principal under the CDR Outsourcing Arrangement (meaning that the Provider must disclose CDR Data to the Principal, and that Principal must accordingly have collected that CDR Data)[13].	We consider that the CDR Rules, especially given the language 'on behalf of', do not make it clear when the Principal collects CDR Data (if the Provider collects the CDR Data on its behalf from the Data Holder). Accordingly, we **recommend** that the ACCC consider explicitly clarifying that, if the Principal uses a Provider to collect CDR Data from a Data Holder on its behalf, the Principal only 'collects' the CDR Data when the Provider discloses that CDR Data to the Principal (rather than when the Provider collects that CDR Data from the Data Holder) (**Recommendation 10**).

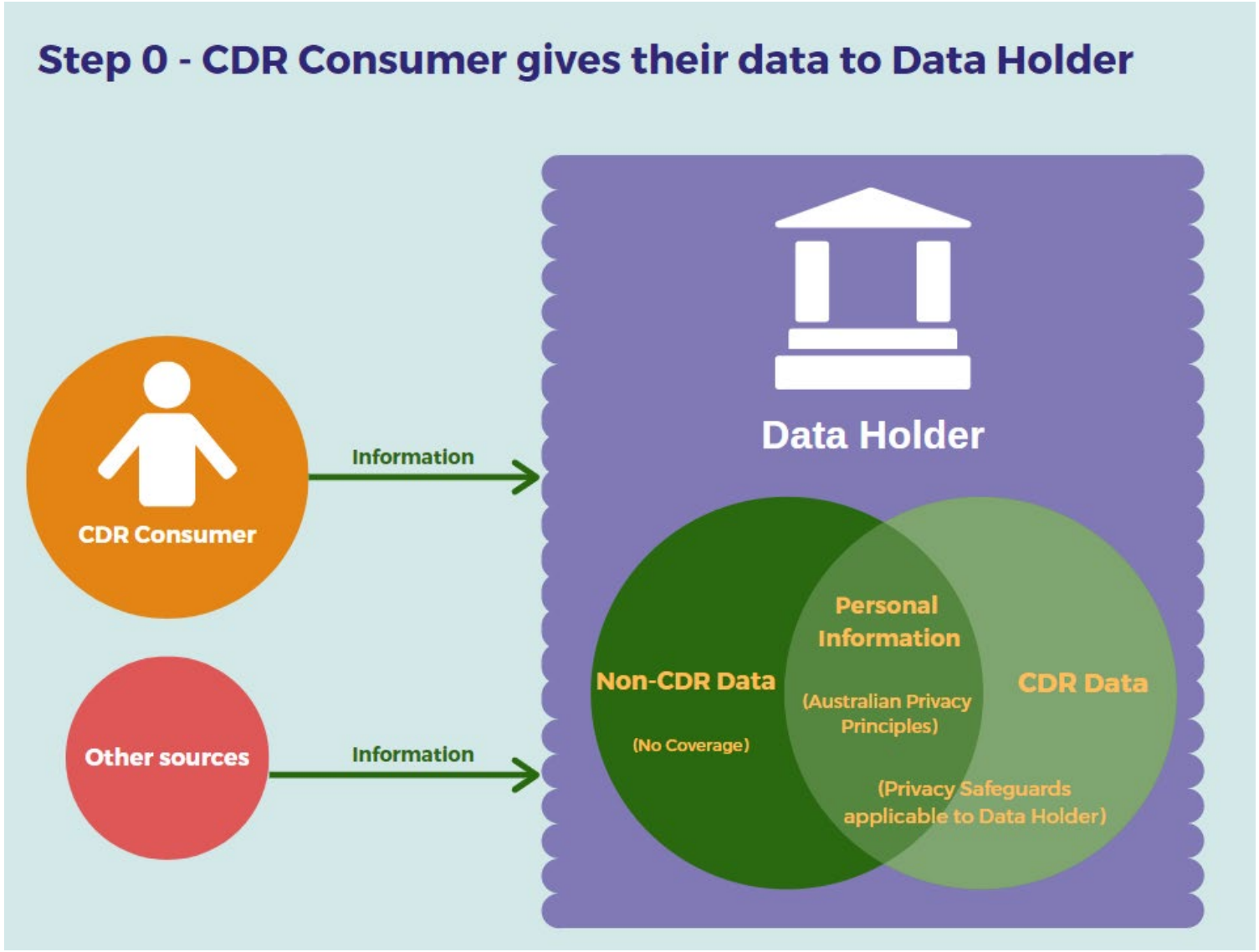
[13] We understand that this may have been clarified/changed in further amendments to the CDR Rules after our analysis was conducted.

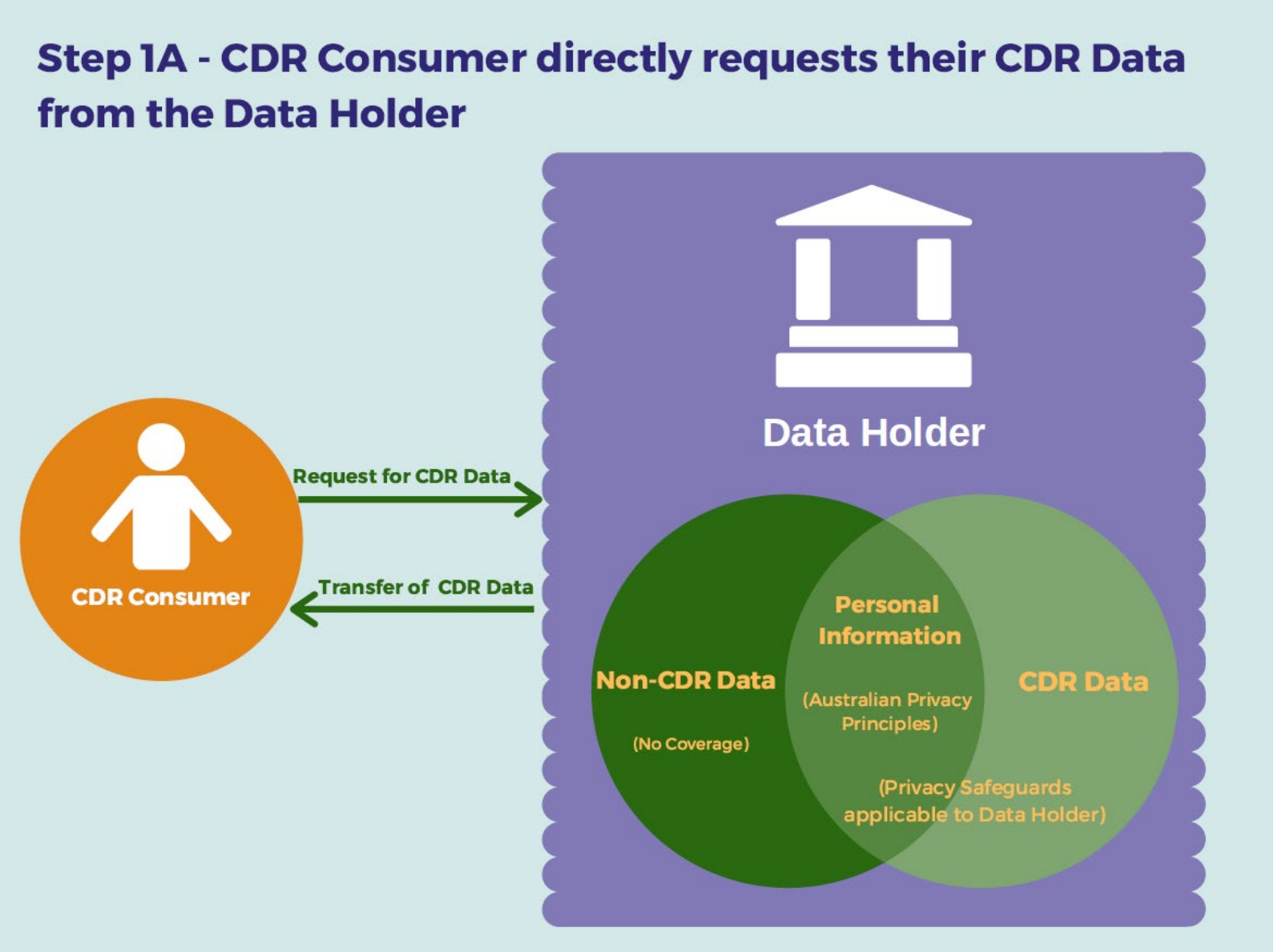
ADDITIONAL CHANGES TO THE CDR RULES, AND OTHER IDENTIFIED RISKS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
26.	**Confusion between 'CDR Data' vs. 'service data'** Given the already complex nature of the legislative framework, the proposed introduction of a new concept of 'service data' may be confusing for Accredited Data Recipients and Data Holders, and what the difference is between this new concept, and CDR Data.	We understand that service data is a subset of CDR Data (Rule 1.10(4)).	We **recommend** that the ACCC consider: • providing additional guidance for CDR participants about the distinction between CDR Data and service data, and how the CDR Rules apply to each category; and • ensuring there are no overlaps or gaps that occur in the application of the CDR Rules to CDR Data and service data. (**Recommendation 10**)

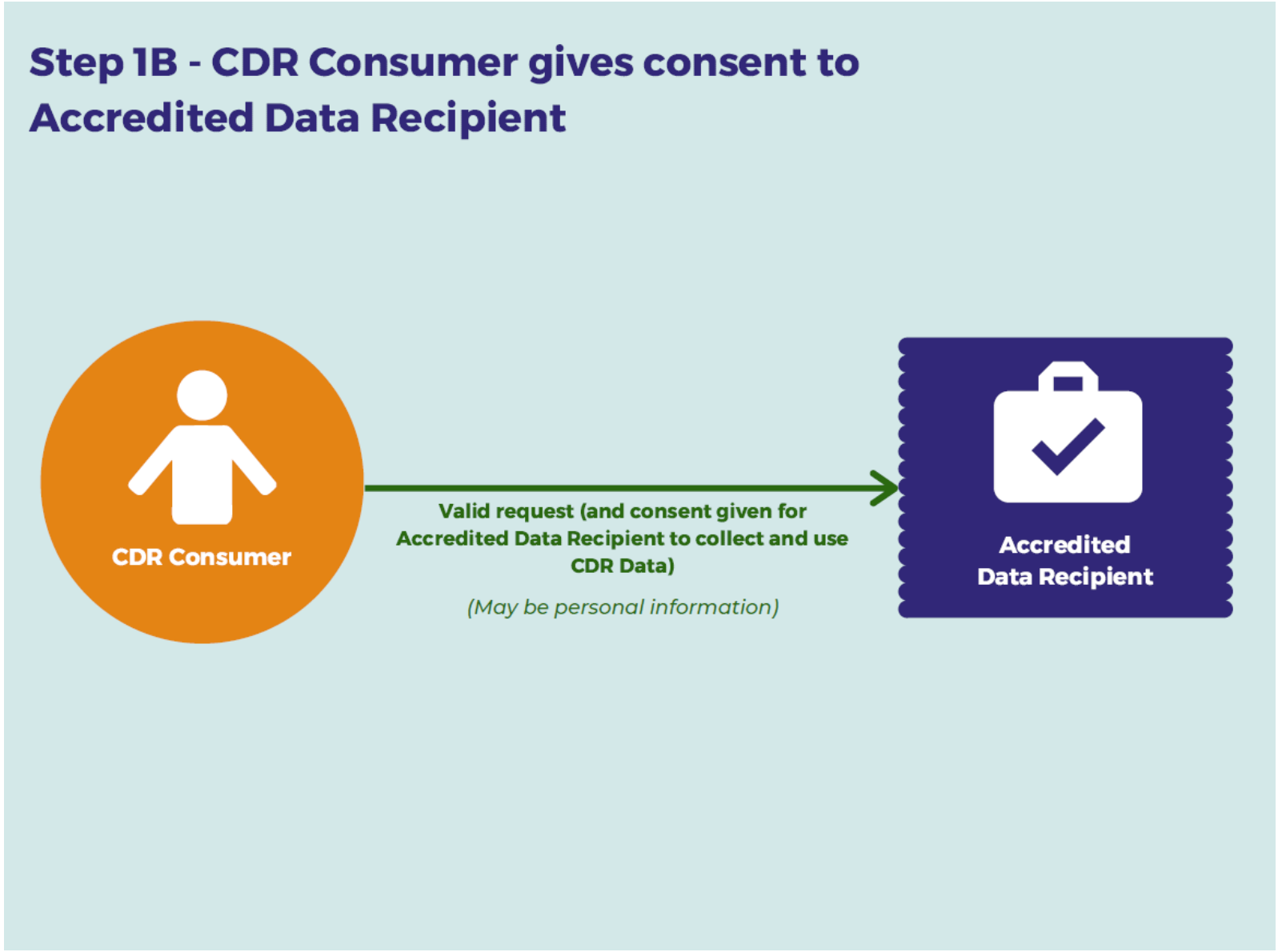
Attachment 1 Glossary

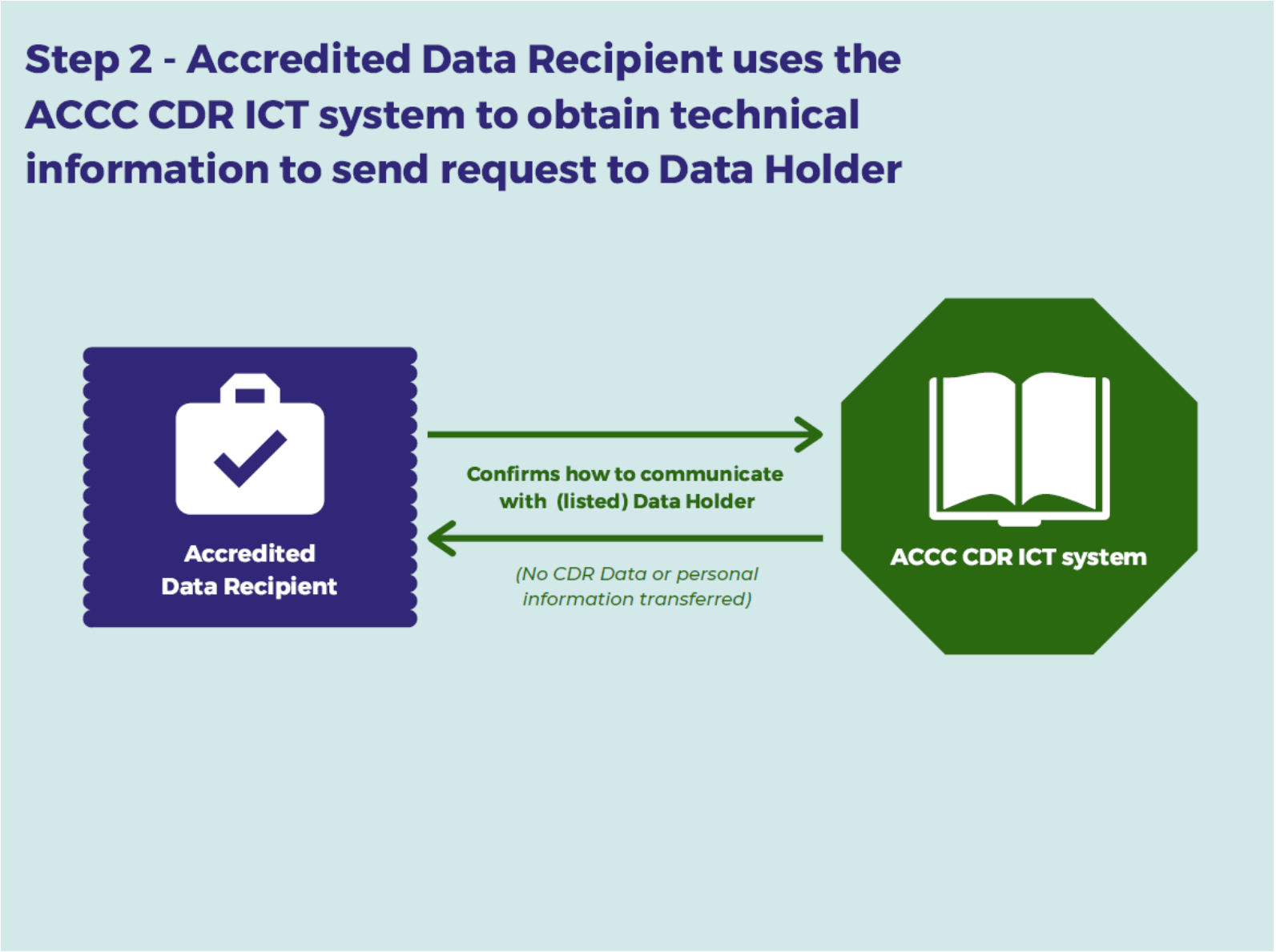
Term	Meaning
ACCC	means the Australian Competition and Consumer Commission.
Accreditation Register	means the register established in accordance with subsection 56CE(1) of the CC Act.
Accredited Data Recipient (ADR)	has the meaning given by section 56AK of the CC Act.
Australian Privacy Principles (APPs)	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 CDR Rules. (b) in relation to a Data Holder, has the meaning given by Rule 1.14 of the CDR Rules.
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	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.
Sector(s)	means a sector of the Australian economy.

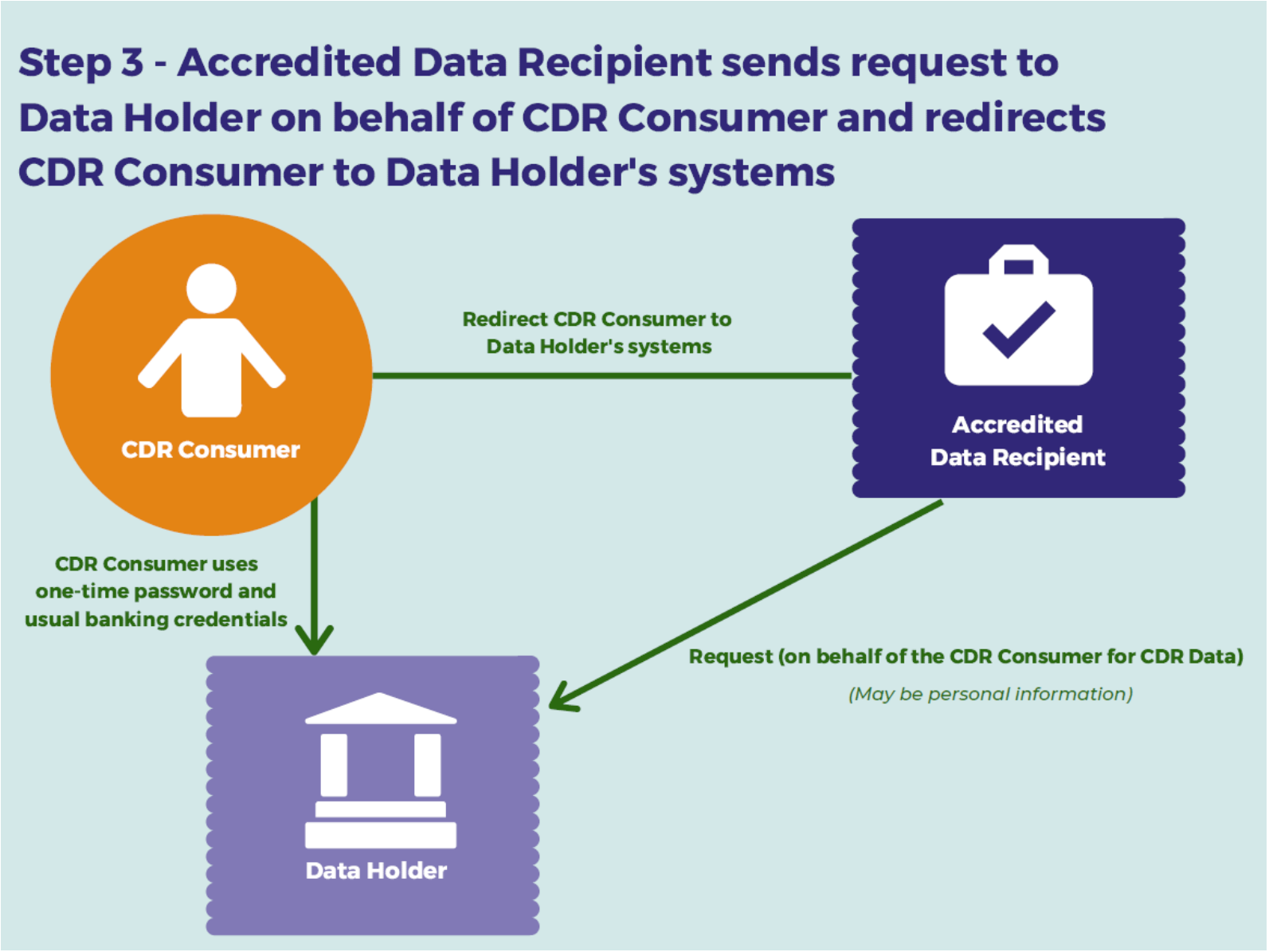
Attachment 2 Steps in the Original CDR PIA report (Diagram of Information Flows)

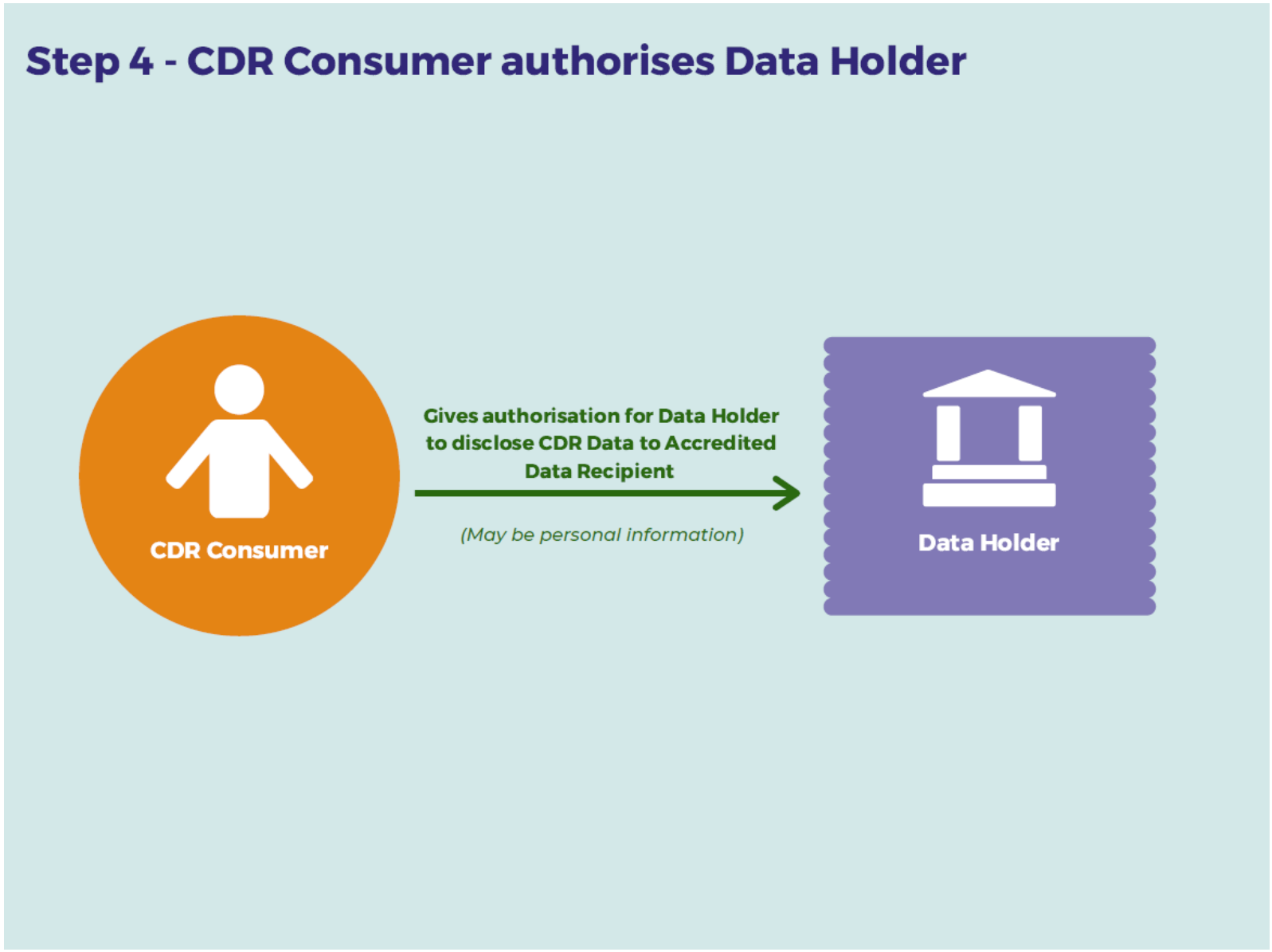





Step 1B - CDR Consumer gives consent to Accredited Data Recipient
CDR Consumer
Valid request (and consent given for Accredited Data Recipient to collect and use CDR Data)
(May be personal information)
Accredited Data Recipient


Step 2 - Accredited Data Recipient uses the ACCC CDR ICT system to obtain technical information to send request to Data Holder
Accredited Data Recipient
Confirms how to communicate with (listed) Data Holder
(No CDR Data or personal information transferred)
ACCC CDR ICT system

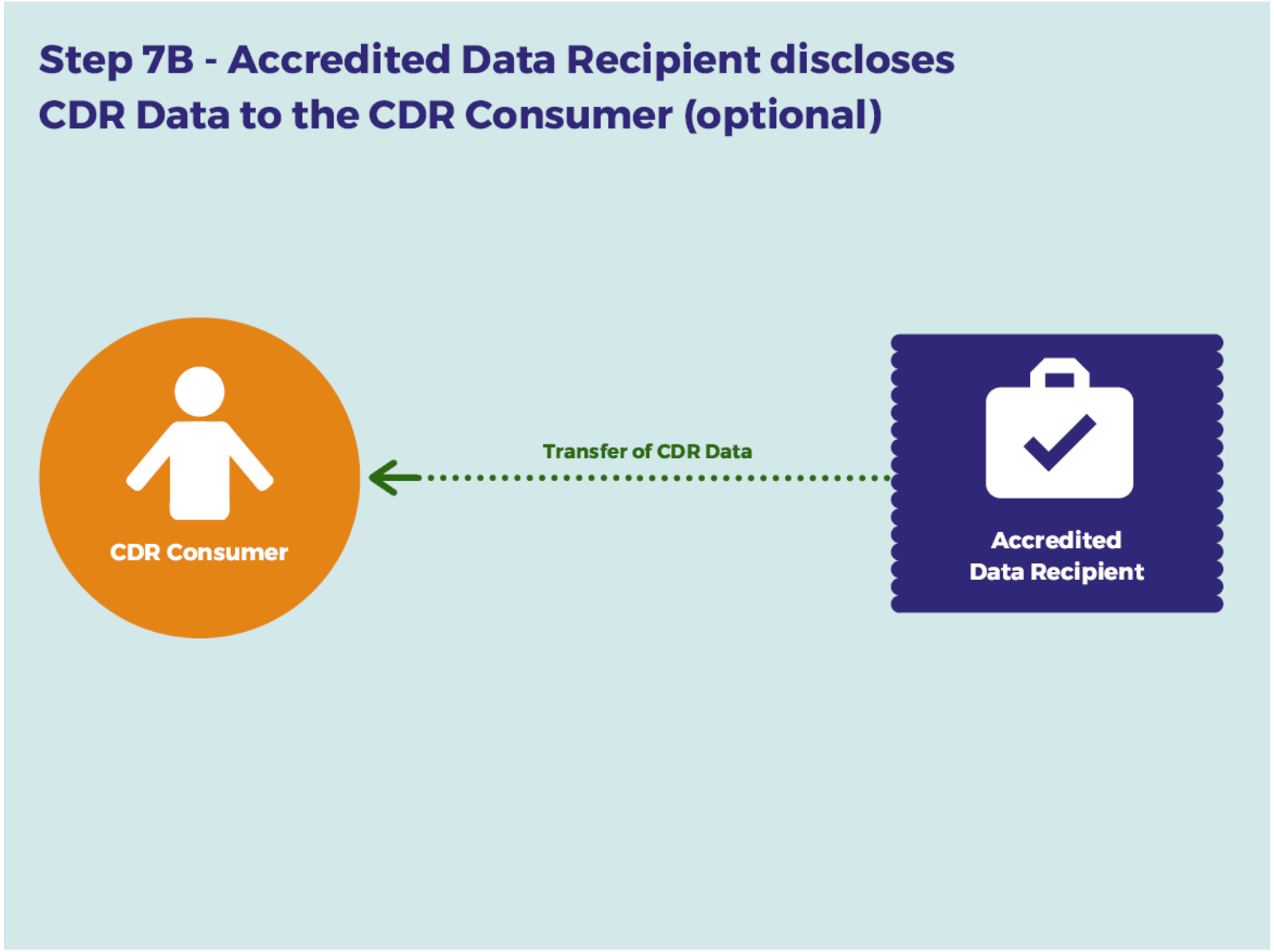

Step 3 - Accredited Data Recipient sends request to Data Holder on behalf of CDR Consumer and redirects CDR Consumer to Data Holder's systems
CDR Consumer
Redirect CDR Consumer to Data Holder's systems
Accredited Data Recipient
CDR Consumer uses one-time password and usual banking credentials
Request (on behalf of the CDR Consumer for CDR Data)
(May be personal information)
Data Holder

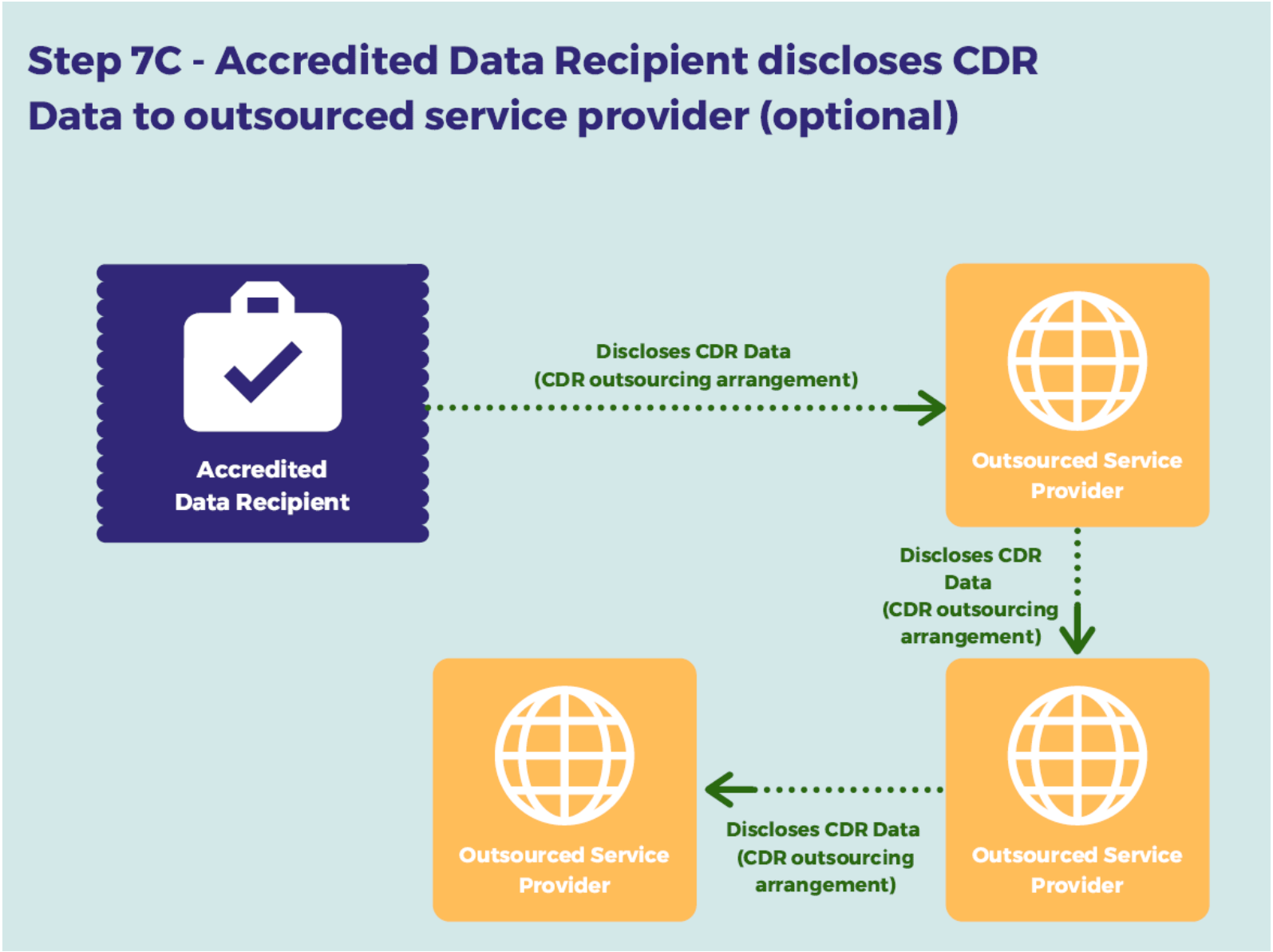

Step 4 - CDR Consumer authorises Data Holder
CDR Consumer
Gives authorisation for Data Holder to disclose CDR Data to Accredited Data Recipient
(May be personal information)
Data Holder

Step 5 - Data Holder checks credentials of Accredited Data Recipient using ACCC CDR ICT system (and Accreditation Register)

Step 6 - Data Holder sends CDR Data to the Accredited Data Recipient and Accredited Data Recipient collects the CDR Data

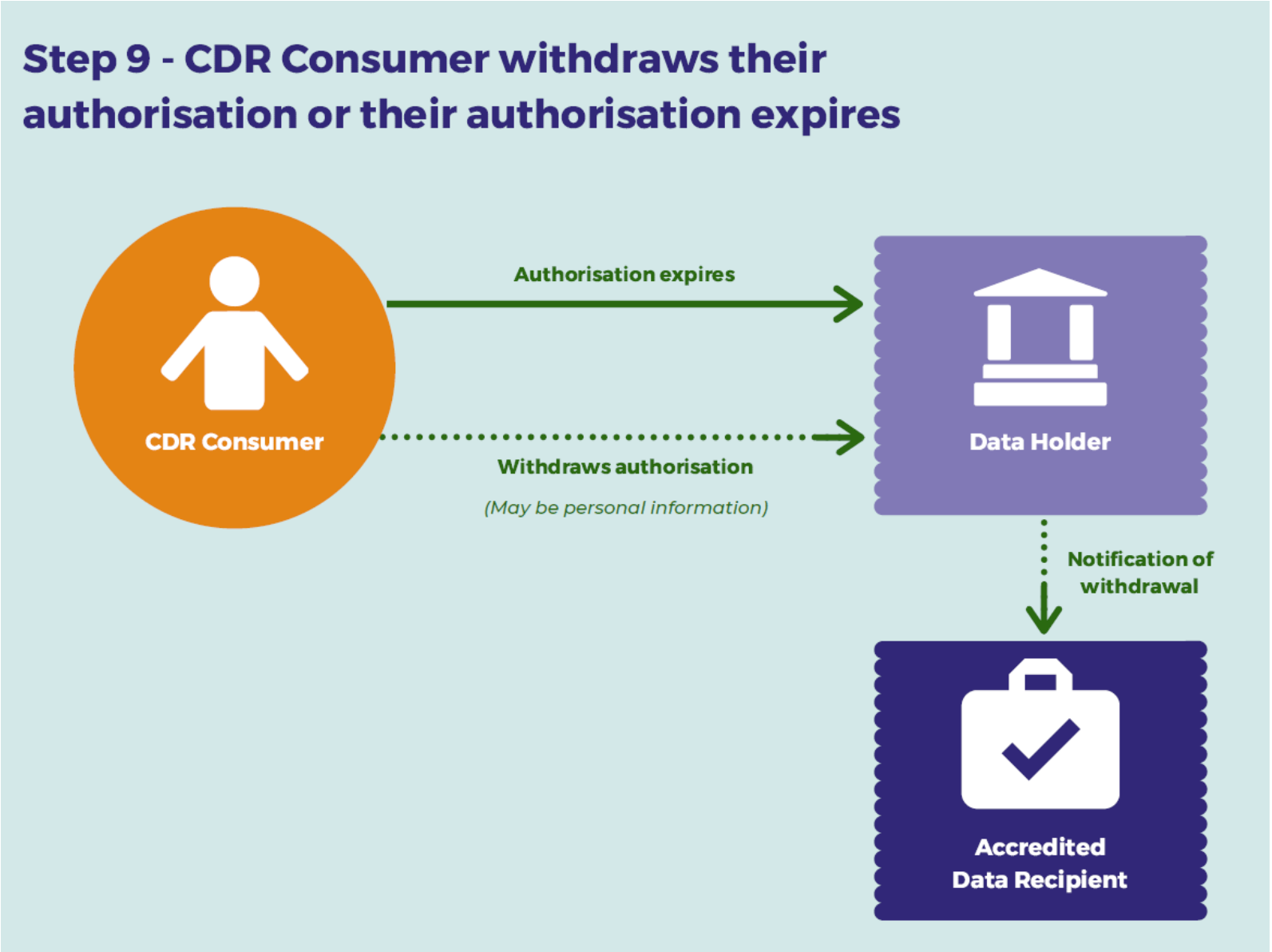
Step 7A - Accredited Data Recipient uses CDR Data to provide goods or services requested by the CDR Consumer

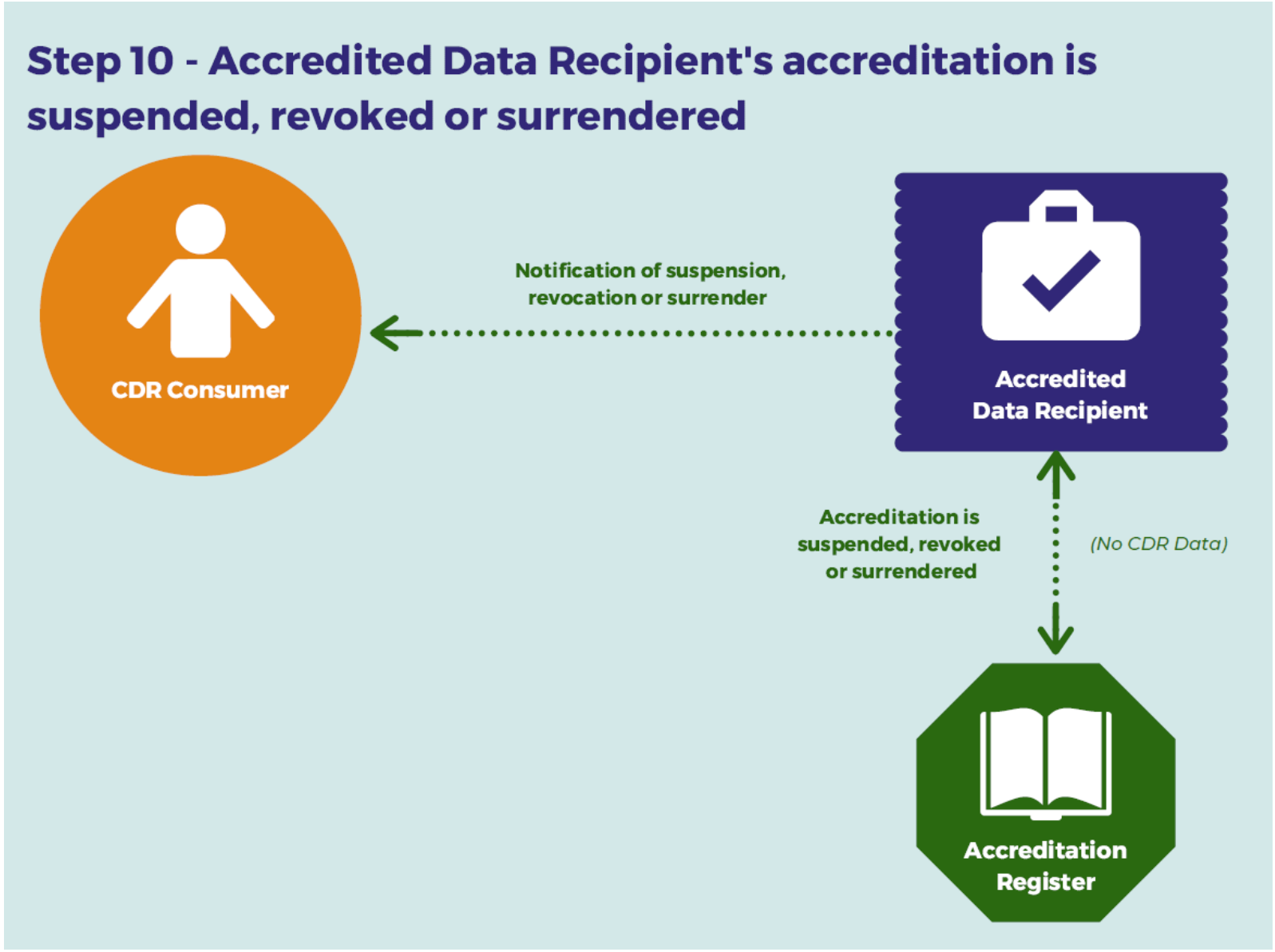

Step 7B - Accredited Data Recipient discloses CDR Data to the CDR Consumer (optional)
CDR Consumer
Transfer of CDR Data
Accredited Data Recipient


Step 7C - Accredited Data Recipient discloses CDR Data to outsourced service provider (optional)
Accredited Data Recipient
Discloses CDR Data (CDR outsourcing arrangement)
Outsourced Service Provider
Discloses CDR Data (CDR outsourcing arrangement)
Outsourced Service Provider
Discloses CDR Data (CDR outsourcing arrangement)
Outsourced Service Provider

Step 7D - Accredited Data Recipient discloses de-identified data (optional)


Step 8 - CDR Consumer withdraws their consent or their consent expires
CDR Consumer
Consent expires
Withdraws consent
(May be personal information)
Accredited Data Recipient


Step 9 - CDR Consumer withdraws their authorisation or their authorisation expires
CDR Consumer
Authorisation expires
Withdraws authorisation
(May be personal information)
Data Holder
Notification of withdrawal
Accredited Data Recipient


Step 10 - Accredited Data Recipient's accreditation is suspended, revoked or surrendered
CDR Consumer
Notification of suspension, revocation or surrender
Accredited Data Recipient
Accreditation is suspended, revoked or surrendered
(No CDR Data)
Accreditation Register