Maddocks

Australian Competition and Consumer Commission

CONSUMER DATA RIGHT REGIME

Update 1 to Privacy Impact Assessment

CONSULTATION DOCUMENT ONLY

[Draft as at 19 June 2020]

Contents

Part A Introduction 3

1. Overview 3
2. Structure of the document 4

Part B Methodology 5

3. Our methodology 5
4. Scope of this document 6

Part C Project Description 7

5. Background to the development of the changes to the CDR regime 7
6. Overview of CAP Arrangements 7
7. Collection of CDR Consumer's consent 8
8. Obtaining of Data Holder's information from ACCC CDR ICT system, sending of request to Data Holder, and redirection of CDR Consumer 9
9. Data Holder uses the ACCC CDR ICT system to check credentials of, the Principal ADR or Provider ADR (as relevant) 9
10. Data Holder discloses CDR Data 10
11. Withdrawal or expiry of CDR Consumer's consent 11
12. Withdrawal or expiry of CDR Consumer's authorisation 11
13. Suspension, revocation or surrender of accreditation 11
14. Additional changes to the CDR Rules 11

Part D Analysis of Risks 13

15. Introduction 13

CAP Arrangements 14

Collection of CDR Consumer's consent 17

Obtaining of Data Holder's information from ACCC CDR ICT system, sending of request to Data Holder, and redirection of CDR Consumer 20

Data Holder uses the ACCC CDR ICT system to check credentials of, the Principal ADR, Provider ADR, or both (as relevant) 22

Data Holder discloses CDR Data to Provider ADR, and Provider ADR collects that CDR Data 25

Data Holder discloses CDR Data to Principal ADR, and Principal ADR collects that CDR Data 27

Provider ADR discloses CDR Data to Principal ADR 28

Withdrawal or expiry of CDR Consumer's consent 30

Withdrawal or expiry of CDR Consumer's authorisation 32

Attachment 1 Glossary 37

Attachment 2 Steps in the Original CDR PIA report (Diagram of Information Flows) 40

Part A Introduction

1. Overview

1.1 Maddocks has been engaged to undertake an 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 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 Original CDR PIA report was undertaken as a "point in time" analysis of the development of the legislative framework (that is, the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth) (**CDR Act**), Competition and Consumer (Consumer Data Right) Rules 2020 (Cth) (**Draft Rules**), Draft 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 The ACCC is responsible for making the *Competition and Consumer (Consumer Data Right) Rules 2020* (Cth) (**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. These proposed amendments relate to the ability for Accredited Data Recipients to enter into arrangements between themselves in relation to the collection, use and disclosure of CDR Data.

1.6 The PIA Update report is intended to complement the Original CDR PIA report. It will not seek to repeat existing privacy risks or mitigation strategies that were discussed in the Original CDR PIA report. Rather, it will focus 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.

Note to Stakeholders: *Maddocks is keen to consult with interested and affected stakeholders, to ensure that the PIA Update 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 in relation to the proposed changes to the CDR Rules discussed in this document. This draft document should therefore only be considered as a very preliminary analysis of the privacy risks, current or proposed mitigation strategies in relation to those risks, and our identified gaps and 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 D*** *and any additional mitigation strategies that are already in place or which are proposed in the amendments to the CDR*

[1] Recommendation 1 in the CDR PIA report.

Rules, or further strategies that should be considered in relation to the proposed CDR Rule changes (as discussed in Part C of this document).

2. Structure of the document

2.1 This document is comprised of the following sections which will, when finalised, form part of the PIA Update report:

2.1.1 **Part B - Methodology:** This section details how we are undertaking the PIA Update report, and includes information about the scope of the PIA Update report.

2.1.2 **Part C - 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.

Note to Stakeholders: *The Original CDR PIA report set out the steps involved in the CDR process, and included diagrams which illustrated those steps (these original diagrams are set out in* ***Attachment 2*** *for ease of reference).*

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

Note to Stakeholders: *Our work has been undertaken on an urgent basis, in parallel with the drafting for the proposed amendments to the CDR Rules. We have had only very limited time to consider the proposed amendments. In addition, the version of the proposed amendments to the CDR Rules published by the ACCC may be different from the version we reviewed, and may include further changes which we have not yet had the opportunity to consider. We will, however, further refine our analysis in this document during the period that it is also being considered by stakeholders, to reflect the wording proposed for the amendments.*

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

2.1.5 **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 Methodology

3. Our methodology

3.1 We are conducting our PIA Update broadly in accordance with the Office of the Australian Information Commissioner's *Guide to undertaking privacy impact assessments* (**PIA Guide**). This involves 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. ***Note to Stakeholders:*** *As discussed above, our work has occurred in parallel with the drafting of the proposed amendments to the CDR Rules. The version of the proposed amendments to the CDR Rules published by the ACCC at the same time as this document, may include further changes which we have not yet had the opportunity to consider. We will, however, further refine our analysis in this document during the period that it is also being considered by stakeholders, to reflect the wording proposed for the amendments.* We also agreed on the scope of the PIA Update report (discussed further in this **Part B** below), the approach to undertaking a broader stakeholder consultation process, and the timeframes for the necessary activities involved in conducting the 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.	*[In progress]* **Privacy impact analysis and compliance check:** In this stage, we are working 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 will take the same approach to risk assessment which was adopted in the original CDR regime analysis, and not endeavour to quantify or label the level of risk associated with each of the identified privacy risks.
4.	*[In progress]* **Privacy management and addressing risks:** We are working to consider potential mitigation strategies which could further address any additional negative privacy impacts identified during the privacy impact analysis stage.

Stage	Description of steps
5.	*[In progress]* **Stakeholder consultation**: A draft of this document has been 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 will provide us with those submissions, from which we will identify and consider further valuable insights. ***Note to Stakeholders:*** *We will gratefully receive all written submissions in relation to privacy issues which are submitted to the ACCC in accordance with their published submission process. Stakeholders do **not** need to provide a separate submission in relation to this document – if privacy issues are raised in a submission which is submitted to the ACCC in relation to the proposed amendments to the CDR Rules, we will also take these into account.* *We will use all submissions to assist us in identifying the privacy risks, undertake our PIA analysis, and formulate our final recommendations. We may disclose submissions in order for us to finalise the PIA Update report, including by quoting relevant sections of a submission in our PIA Update report if this assists us to explain stakeholder views.* *If we do include a quote from a submission, we will reference the organisation as the author of that quote, but we do not intend to include copies of any submissions in the PIA Update report. While we will fully consider each submission we receive, we may not adopt or accept the views or ideas in submissions, or discuss them in detail in our PIA Update report. We will assume that stakeholders who provide a submission have agreed to these conditions.* *After we receive submissions, we plan to contact some stakeholders if we believe this would assist us to ensure that we have fully understood their submissions.*
6.	*[Not yet completed]* **Privacy management and addressing risks:** We will further refine the potential mitigation strategies which could further address any additional negative privacy impacts identified during the privacy impact analysis stage.
7.	*[Not yet completed]* **Recommendations:** From the stages referred to above, we will prepare recommendations to remove or reduce identified avoidable privacy risks.
8.	*[Not yet completed]* **Report:** We will finalise the PIA Update report.
9.	*[Not yet completed]* **Respond and review:** We understand that the ACCC will review the PIA Update report, in consultation with other stakeholders as required, to include responses to our recommendations.

4. Scope of this document

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

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

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

4.2 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 CDR Act, CDR Rules, Data Standards and the Open Banking Designation.

Part C Project Description

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

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

5.1 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).

5.2 As discussed in the Original CDR PIA report[2], the ACCC is responsible for developing and administering the CDR Rules made under the CDR Act.

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

5.3.1 the CDR Rules on 6 February 2020; and

5.3.2 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.[3]

5.4 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 Accredited Data Recipients, in order to permit two Accredited Data Recipients to make arrangements between themselves (known as "CAP arrangements"), as discussed further below in paragraph 6 of this **Part C [Project Description]**.

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

6. Overview of CAP Arrangements

6.1 The proposed amendments to the CDR Rules introduce a concept of combined accredited person arrangements (**CAP Arrangements**). One Accredited Data Recipient (the **Principal ADR**) is permitted to enter into a CAP Arrangement with another Accredited Data Recipient (the **Provider ADR**). Under a CAP Arrangement:

6.1.1 the Provider ADR may be permitted to collect CDR Data from a Data Holder on behalf of the Principal ADR. This may include obtaining consent from the CDR Consumer, and making consumer data requests to the Data Holder; and/or

[2] Paragraphs 9.4 and 12 of Part D [Project Description] of the Original CDR PIA report.
[3] The *Competition and Consumer (Consumer Data Right) Amendment Rules (No.1) 2020* are available at https://www.legislation.gov.au/Details/F2020L00757.

6.1.2 the Principal ADR may be permitted to disclose CDR Data to the Provider ADR in order for the Provider ADR to provide goods or services to the Principal ADR in relation to that CDR Data.

6.2 Importantly, a Provider ADR may only do a thing in relation to CDR Data that is subject to a CAP Arrangement, if the Principal ADR is authorised to do that thing in relation to CDR Data.

6.3 Unlike the CDR Rules applying to CDR outsourcing arrangements, the proposed changes to the CDR Rules will not result in any requirements for the content or form of a CAP Arrangement being specified in the CDR Rules.[4]

6.4 However, the changes will effectively mean that (unless the CDR Rules specify otherwise), where there is a CAP Arrangement in place in relation to CDR Data:

6.4.1 either the Principal ADR or the Provider ADR may do any act that is permitted by the CDR Rules;

6.4.2 the obligations in the CDR Rules in relation to CDR Data are imposed on both the Principal ADR and the Provider ADR (but if one party has discharged the obligation, the other party does not need to also discharge that obligation); and

6.4.3 a breach of an obligation in the CDR Rules by the Provider ADR is taken to also be a breach of that obligation by the Principal ADR.

6.5 In addition, the CDR Rules will expressly provide that, if CDR Data is collected by, or disclosed to, a Provider ADR in accordance with a CAP Arrangement, any use or disclosure of that CDR Data by the Provider ADR (whether or not in accordance with the CAP Arrangement) is taken to have also been a use or disclosure by the Principal ADR.

6.6 It is possible that under a CAP Arrangement, the Provider ADR and the Principal ADR will make agreements about the provision and maintenance of the Accredited Data Recipient's Consumer Dashboard. A Consumer Dashboard must contain, if the CDR Data may be collected by, or disclosed to, a Provider ADR under a CAP Arrangement:

6.6.1 the Provider ADR's name; and

6.6.2 the Provider ADR's accreditation number.

6.7 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.

7. Collection of CDR Consumer's consent

7.1 Depending on the agreements contained in the CAP Arrangement, either the Principal ADR or the Provider ADR (on behalf of the Principal ADR) will collect a CDR Consumer's consent in relation to their CDR Data. If the Principal ADR collects the CDR Consumer's consent, it will have to, at some stage, communicate the consent obtained, and the relevant information about the CDR Consumer, to the Provider ADR. If the Provider ADR is to collect the CDR Consumer's consent, the Principal ADR will still need to communicate relevant contact information about the CDR Consumer to the Provider ADR, in order to facilitate that collection. The amendments to the CDR Rules do not specify a communication method, so

[4] For clarity, we note that the proposed amendments to the CDR Rules do not preclude a Principal ADR from having both a CAP Arrangement and a CDR outsourcing arrangement with a Provider ADR (noting that there could be overlap between requirements in the CDR Rules the Provider ADR, as an Accredited Data Recipient, is obliged to comply with, and the obligations imposed on outsourced service providers in the CDR Rules).

we presume that this may be done in accordance with arrangements specified in the CAP Arrangement.

7.2 Irrespective of whether the Principal ADR or the Provider ADR collects the CDR Consumer's consent, when the CDR Consumer's consent is sought, the CDR Consumer must be provided with the following information:

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

7.2.2 the Provider ADR's name;

7.2.3 the Provider ADR's accreditation number;

7.2.4 a link to the Provider ADR's CDR policy; and

7.2.5 a statement that the CDR Consumer can obtain further information about such collections or disclosures from the Provider ADR's CDR policy.

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

8.1 Depending on the CAP Arrangement in place, and which party is to make a request to the Data Holder, the Principal ADR or the Provider ADR 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.

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

8.3 The Principal ADR, or the Provider ADR (using the information provided to it by the Principal ADR), 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.

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

9.1 If the Data Holder is disclosing the CDR Data to the Principal ADR, it will check the credentials of, and obtain the technical information required to communicate with, the Principal ADR using the ACCC CDR ICT system (and Accreditation Register).

9.2 It is not yet clear to us whether, if the Data Holder is disclosing the CDR Data to the Provider ADR (as specified in the CAP Arrangement), the Data Holder will check the credentials of the Principal ADR, the Provider ADR, or both (including which entities the Data Holder will check to ensure that their accreditation has not expired or been suspended or revoked).

9.3 However, in all cases, the Data Holder will obtain the technical information required to communicate with the Provider ADR using the ACCC CDR ICT system (and Accreditation Register).

10. Data Holder discloses CDR Data

10.1 The Data Holder will then disclose the CDR Data to:

10.1.1 the Principal ADR; or

10.1.2 the Provider ADR,

and the relevant Accredited Data Recipient will collect that CDR Data.

Provider ADR collects CDR Data from the Data Holder

10.2 If the Provider ADR collects the CDR Data from the Data Holder, then, before the Provider ADR discloses the CDR Data to the Principal ADR (and the Principal ADR collects that CDR Data), the Provider ADR may:

10.2.1 use the CDR Data to provide the goods or services requested by the CDR Consumer;

10.2.2 disclose the CDR Data to its outsourced service providers; and

10.2.3 disclose de-identified data to third parties,

in accordance with:

10.2.4 the consent provided by the CDR Consumer; and

10.2.5 its CAP Arrangement with the Principal ADR.

Principal ADR collects CDR Data from the Data Holder

10.3 If the Principal ADR collects the CDR Data from the Data Holder, then the information flows described in the Original CDR PIA report apply.

10.4 This means that the Principal ADR may:

10.4.1 use the CDR Data to provide the goods or services requested by the CDR Consumer;

10.4.2 disclose the CDR Data to the CDR Consumer;

10.4.3 disclose the CDR Data to its outsourced service providers; and

10.4.4 disclose de-identified data to third parties.

10.5 In addition, the Principal ADR may, under a CAP Arrangement, disclose the CDR Consumer's CDR Data to a Provider ADR. If this occurs, and the Provider ADR correspondingly collects that CDR Data, then the Provider ADR may use and disclose the CDR Data as specified in paragraph 10.2 of this **Part C [Project Description]**, before it then discloses the CDR Data back to the Principal ADR.

Provider ADR discloses CDR Data to the Principal ADR

10.6 In accordance with the CAP Arrangement, the Provider ADR will disclose the CDR Data to the Principal ADR:

10.6.1 if the Provider ADR has collected the CDR Data from the Data Holder, after that collection (and any of the uses or disclosures listed in paragraph 10.2 of this **Part C [Project Description]** in accordance with the CAP Arrangement); and

10.6.2 if the Principal ADR has collected the CDR Data from the Data Holder and disclosed that CDR Data to the Provider ADR, after any of the uses or disclosures by the Provider ADR listed in paragraph 10.2 of this **Part C [Project Description]** in accordance with the CAP Arrangement.

10.7 We understand that the proposed amendments to the CDR Rules will also require transfer of CDR Data between the Provider ADR and Principal ADR to be encrypted in accordance with Schedule 2 to the CDR Rules.

11. Withdrawal or expiry of CDR Consumer's consent

11.1 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 Accredited Data Recipient or by using the Accredited Data Recipient's Consumer Dashboard.

11.2 The intention is that a CAP Arrangement should specify the mechanisms by which each party will be made aware of any withdrawal or expiry of a CDR Consumer's consent.

12. Withdrawal or expiry of CDR Consumer's authorisation

12.1 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.

13. Suspension, revocation or surrender of accreditation

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

14. Additional changes to the CDR Rules

14.1 The CDR Rules will also be changed to include some additional protections in the Privacy Safeguards:

14.1.1 **Privacy Safeguard 1** will be changed to require that an Accredited Data Recipient's CDR Policy must also include:

(a) a list of the Accredited Data Recipients with whom they have a CAP Arrangement; and

(b) for each such CAP Arrangement, if applicable:

(i) information about the nature of the services one party provides to the other party; and

(ii) information about the CDR Data or classes of CDR Data that may be disclosed by one party to the other; and

(iii) a link to the CDR policy of the other party,

14.1.2 **Privacy Safeguard 5** will be changed so that a Principal ADR who has collected CDR Data must update the Accredited Data Recipient's Consumer Dashboard to also include the fact that the CDR Data was collected by a Provider ADR.

14.1.3 **Privacy Safeguard 10** will be changed so that a Data Holder must, as soon as practicable after disclosing CDR Data to a Provider ADR, update the Data Holder's Consumer Dashboard to also include the fact that the CDR Data was provided to a Provider ADR.

14.1.4 **Privacy Safeguard 12** will be changed so that only a Principal ADR can decide that it is appropriate in the circumstances to de-identify rather than delete the redundant data (in which case the steps in Privacy Safeguard 12 will apply).

Part D Analysis of Risks

15. Introduction

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

15.2 For convenience, we have grouped the following information flows and concepts[5], which may involve new or changed privacy considerations in addition to those identified in the Original CDR PIA report:

15.2.1 CAP Arrangements;

15.2.2 collection of CDR Consumer's consent;

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

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

15.2.5 Data Holder discloses CDR Data to Provider ADR, and Provider ADR collects that CDR Data;

15.2.6 Data Holder discloses CDR Data to Principal ADR, and Principal ADR collects that CDR Data;

15.2.7 Provider ADR discloses CDR Data to Principal ADR;

15.2.8 withdrawal or expiry of CDR Consumer's consent;

15.2.9 withdrawal or expiry of CDR Consumer's authorisation;

15.2.10 suspension, revocation or surrender of accreditation; and

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

15.3 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.

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

CAP Arrangements

CAP ARRANGEMENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**Content of CAP Arrangements unclear** The proposed amendments to the CDR Rules do not specify any mandatory provisions that must be included in CAP Arrangements.	Both parties to CAP Arrangements are already Accredited Data Recipients in their own right and are therefore subject to a range of obligations under the CDR regime.	As discussed in relation to a number of the risks below, the inclusion of mandatory provisions in the CAP Arrangements may be a key mitigation strategy. For example, it may be beneficial for CAP Arrangements to be required to contain a mutual obligation upon the parties to notify each other if a CDR Consumer withdraws their consent or authorisation, so that the other party does not inadvertently continue to use or disclose CDR Data without an appropriate consent and authorisation. Additionally, it may be beneficial to include an express requirement that a CAP Arrangement be in writing, so that it can be reviewed or considered by the appropriate regulatory bodies if necessary to manage or respond to privacy concerns raised by a CDR Consumer (noting the proposed amendments to the CDR Rules will require Accredited Data Recipients to keep copies of the relevant CAP Arrangement, which suggests that CAP Arrangements should be in writing).

CAP ARRANGEMENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
2.	**Confusion over liability regime in CDR Rules, and which obligations apply to either the Principal ADR, the Provider ADR, or both** There is a risk that the parties to a CAP Arrangement will not understand which obligations in the CDR regime "in relation to CDR Data" are able to be discharged by either of the parties, and which obligations must be discharged by both parties. This may cause obligations imposed on Accredited Data Recipients in the CDR Rules to not be discharged by either party, as they think the other party is responsible for doing so. It may also cause confusion as some Provider ADRs may think that an obligation in the CDR Rules is being performed by the Principal ADR (e.g. in relation to security), so they do not also need to comply.		The proposed changes to the CDR Rules do not specify how liability is to be apportioned contractually between the Principal ADR and the Provider ADR (i.e. this is left to the CAP Arrangement). There may be confusion about which party to a CAP Arrangement is responsible for discharging a particular obligation in respect of CDR Data, noting that if an obligation is not discharged it will necessarily impact upon the privacy protections afforded to CDR Consumers. To ensure that there is clarity about which obligations are to be discharged by the Principal ADR, and which obligations are to be discharged by the Provider ADR, the ACCC should consider specifying in the CDR Rules that CAP Arrangements must accurately and completely describe the parties' obligations and those obligations that are separate from the CAP Arrangement (i.e. those obligations that all Accredited Data Recipients must meet, regardless of being a party to a CAP Arrangement).

CAP ARRANGEMENTS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
3.	**Information in Accredited Data Recipient Consumer Dashboard may not provide sufficient clarity to CDR Consumers** There is a risk that CDR Consumers will not know which Accredited Data Recipient is handling their information.	The proposed changes to the CDR Rules will require an Accredited Data Recipient's Consumer Dashboard, and the CDR policy of the Principal ADR, to list all Provider ADRs with which the Principal ADR has a CAP Arrangement.	This information in isolation will not ensure that a CDR Consumer knows which of the listed Provider ADRs will be handling their CDR Data. The ACCC may wish to consider whether CDR Consumers should be provided with more granular information (e.g. Provider ADR "X" will be used to collect CDR Data from Data Holder "X").

Collection of CDR Consumer's consent

COLLECTION OF CDR CONSUMER'S CONSENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
4.	**Security of the communication pathway between the Principal ADR and the Provider ADR for non-CDR Data about the CDR Consumer** There is a risk that the communication pathway between the Principal ADR and Provider ADR 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 Accredited Data Recipients 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 CDR 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 Accredited Data Recipients must comply with.	It is not entirely clear whether the parties to a CAP Arrangement are required to ensure that proposed amendments in Schedule 2 will be used by the parties to transfer non-CDR Data. The ACCC may wish to consider whether the legislative framework should contain specific technical requirements for any communications that occur between the Principal ADR and the Provider ADR for information that is not CDR Data (such as information about a CDR Consumer's consent, or their contact information). This would further assist to ensure that the information is appropriately protected.
5.	**Details of CDR Consumer's consent and contact information not accurately transferred from Principal ADR to Provider ADR** If the Principal ADR collects the CDR Consumer's consent,	See ***Item 4*** above.	See ***Item 4*** above.

COLLECTION OF CDR CONSUMER'S CONSENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	or requires the Provider ADR to collect the consent on its behalf, it will need to transfer to the Provider ADR 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 ADR (about the consent or their contact information) to the Provider ADR is not accurate (so that the Provider ADR seeks information about the 'wrong' Data Holder from the ACCC CDR ICT system, or contacts the 'wrong' CDR Consumer to seek their consent).		
6.	**CDR Consumer unaware of to whom they are providing their consent** It is unclear to us how CDR Consumers will know whether they are providing their consent to the Principal ADR, the Provider ADR, or both.	If a Principal ADR will be using a Provider ADR under a CAP Arrangement, the proposed amendments to CDR Rules 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), the Provider ADR; • the Provider ADR's name;	In our view, the proposed amendments to the CDR Rules will not necessarily provide this clarity to CDR Consumers.

COLLECTION OF CDR CONSUMER'S CONSENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		• the Provider ADR's accreditation number; • a link to the Provider ADR's CDR policy; and • a statement that the CDR Consumer can obtain further information about such collections or disclosures from the Provider ADR's CDR policy.	
7.	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 ADR or the Provider ADR (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**
8.	**Technical information does not match the CDR Consumer's consent** If, as discussed in ***Item 5*** above, the information about the CDR Consumer and their consent is not correctly transferred from the Principal ADR to the Provider ADR, there is a risk that the technical information obtained by the Provider ADR does not match the requirements of the consent provided by the CDR Consumer to the Principal ADR (so that the request received by the Data Holder does not match the consent provided by the CDR Consumer).	See ***Item 5***.	See ***Item 5***.
9.	The Original CDR PIA report discusses the risks associated with the Accredited Data	*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			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	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 ADR or the Provider ADR (as relevant) uses the ACCC CDR ICT system.		
10.	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 ADR or the Provider ADR (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 ADR, Provider ADR, or both (as relevant)

DATA HOLDER USES THE ACCC CDR ICT SYSTEM TO CHECK CREDENTIALS OF, THE PRINCIPAL ADR OR PROVIDER ADR (AS RELEVANT)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
11.	**Data Holder sends CDR Data to an Accredited Data Recipient that is no longer accredited** If a Provider ADR is to collect the CDR Consumer's CDR Data from a Data Holder, and the Provider ADR is to then disclose that CDR Data to a Principal ADR, it is not clear if the Data Holder will check both the Provider ADR and Principal ADR'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 ADR 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 ADR to check the status of the Principal ADR'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, the ACCC may wish to consider whether Data Holders should know whether the Accredited Data Recipient is acting in the role of a Provider ADR or a Principal ADR. The Data Holder could then be required to check the credentials for both the Provider ADR and the Principal ADR, including whether each accreditation has expired or been suspended or revoked.

DATA HOLDER USES THE ACCC CDR ICT SYSTEM TO CHECK CREDENTIALS OF, THE PRINCIPAL ADR OR PROVIDER ADR (AS RELEVANT)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
12.	**Misuse of Principal ADR's credentials by Provider ADR** It is unclear whether there may be situations in which a Provider ADR could use the credentials of a Principal ADR (i.e. the "PKI certificate" for the ACCC CDR ICT system) for purposes outside of those in the CAP Arrangement.	If a Principal ADR is to engage a Provider ADR, there must be a CAP 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 ADR's credentials by a Provider ADR. If such a use of the Principal ADR's credentials is to be permitted, the ACCC may wish to consider amending the CDR Rules to require CAP Arrangements to contain strict obligations in relation to the use of the Principal ADR's credentials by the Provider ADR.
13.	The Original CDR PIA report discusses the risks associated with the CDR Consumer providing their authorisation to the Data Holder (see ***Step 4 in the Original CDR PIA report***), which will also apply to situations where the CDR Consumer has provided their consent to the Principal ADR or the Provider ADR (as relevant).	*See Original CDR PIA report.*	*See Original CDR PIA report.*
14.	The Original CDR PIA report discusses the risks associated with the Data Holder checking	*See Original CDR PIA report.*	*See Original CDR PIA report.*

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

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

DATA HOLDER DISCLOSES CDR DATA TO PROVIDER ADR, AND PROVIDER ADR 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 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 ADR.	*See Original CDR PIA report.*	*See Original CDR PIA report.*
16.	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 ADR uses the CDR Consumer's CDR Data after receiving it from the Data Holder or from the Principal ADR (as relevant).	*See Original CDR PIA report.* In addition, the Provider ADR must only use the CDR Data in accordance with its CAP Arrangement with the Principal ADR. The proposed amendments to the CDR Rules mean that any breach of an obligation in the CDR Rules by, and any use or disclosure of CDR Data collected by, or disclosed to, the Provider ADR is also attributed to the Principal ADR, such that the parties to a CAP Arrangement will be jointly liable.	*See Original CDR PIA report.*
17.	The Original CDR PIA report discusses the risks associated with the Accredited Data Recipient disclosing CDR Data	*See Original CDR PIA report.*	*See Original CDR PIA report.*

DATA HOLDER DISCLOSES CDR DATA TO PROVIDER ADR, AND PROVIDER ADR COLLECTS THAT CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	to its outsourced service providers (see ***Step 7C in the Original CDR PIA report***), which will also apply to situations where the Provider ADR discloses CDR Data to its outsourced service providers.	In addition, the Provider ADR must only use the CDR Data in accordance with its CAP Arrangement with the Principal ADR. The proposed amendments to the CDR Rules mean that any breach of an obligation in the CDR Rules by, and any use or disclosure of CDR Data collected by, or disclosed to, the Provider ADR is attributed to the Principal ADR, such that the parties to a CAP Arrangement will be jointly liable.	
18.	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 ADR discloses de-identified data to third parties.	*See Original CDR PIA report.* In addition, the Provider ADR must only use the CDR Data in accordance with its CAP Arrangement with the Principal ADR. The proposed amendments to the CDR Rules mean that any breach of an obligation in the CDR Rules by, and any use or disclosure of CDR Data collected by, or disclosed to, the Provider ADR is attributed to the Principal ADR, such that the parties to a CAP Arrangement will be jointly liable.	*See Original CDR PIA report.*

Data Holder discloses CDR Data to Principal ADR, and Principal ADR collects that CDR Data

DATA HOLDER DISCLOSES CDR DATA TO PRINCIPAL ADR, AND PRINCIPAL ADR COLLECTS THAT CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
19.	The Original CDR PIA report discusses the risks associated with the Data Holder disclosing CDR Data to the 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 Principal ADR.	*See Original CDR PIA report.*	*See Original CDR PIA report.*

Provider ADR discloses CDR Data to Principal ADR

PROVIDER ADR DISCLOSES CDR DATA TO PRINCIPAL ADR			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
20.	**Pathway security between the Provider ADR and the Principal ADR is compromised** There is a risk that the pathways used by the Provider ADR to communicate with, and send CDR Data to, the Principal ADR could be compromised.	Both the Provider ADR and the Principal ADR will be required to comply with the protections for CDR Data set out in Schedule 2.	
21.	**Incorrect recipient of CDR Data** There is a risk that CDR Data is sent to the incorrect Accredited Data Recipient, particularly if the Provider ADR is the Provider ADR for several Principal ADRs (and therefore has multiple CAP 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 ADR provides the CDR Data to the 'wrong' Accredited Data Recipient).	As discussed in relation to accurate transmission of consent in ***Item 5***, the ACCC may wish to consider whether the legislative framework should contain specific technical requirements which will reduce the risks of CDR Data being sent to the incorrect Accredited Data Recipient. We consider it may be appropriate for the CDR Rules to contain requirements for the Provider ADR, 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 ADR on whose behalf it collected the

PROVIDER ADR DISCLOSES CDR DATA TO PRINCIPAL ADR			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			CDR Data from the Data Holder, or the Principal ADR who disclosed the CDR Data to it.

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**
22.	**Withdrawal or expiry of CDR Consumer's consent not communicated** There is a risk that the CDR Consumer only notifies one party to a CAP Arrangement that they have withdrawn their consent (or it has expired), and this party does not notify the other party 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 used or disclosed after the CDR Consumer has withdrawn their consent, or it has expired.		There is an assumption that the CAP Arrangements will specify a requirement that each party must notify the other party if the CDR Consumer withdraws their consent, or their consent otherwise expires. There is no such requirement in the proposed amendments to the CDR Rules. Accordingly, as specified in ***Item 1***, the ACCC may wish to consider specifying in the proposed amendments to the CDR Rules certain mandatory matters that CAP Arrangements need to include (such as a mechanism or process to ensure one party notifies the other of the withdrawal or expiry of a CDR Consumer's consent). The CDR Rules could also be amended to include an express obligation on a party to the CAP Arrangement to notify the other 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.
23.	The Original CDR PIA report discusses the risks associated with the withdrawal or expiry of	*See Original CDR PIA report.*	*See Original CDR PIA report.*

WITHDRAWAL OR EXPIRY OF CDR CONSUMER'S CONSENT			
a	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	the CDR Consumer's consent (see ***Step 8 in the Original CDR PIA report***), which will also apply to situations where a Principal ADR engages a Provider ADR under a CAP Arrangement.		

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**
24.	**Withdrawal or expiry of CDR Consumer's authorisation not communicated** There is a risk that one party to a CAP 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 22.***	See ***Item 22.*** 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 ADR who is collecting CDR Data for a Principal ADR under a CAP Arrangement, or whether it will know which Accredited Data Recipient is the Principal ADR. If the Data Holder does not know that it is providing CDR Data to a Provider ADR (and therefore does not know it is informing a Provider ADR of the withdrawal or expiry of the CDR Consumer's authorisation), or know which Accredited Data Recipient is the Principal ADR, there is a risk of disconnect, as the Provider ADR may not notify the Principal ADR of the authorisation ending, and the Data Holder has no ability to also notify the Principal ADR of this fact.
25.	The Original CDR PIA report discusses the risks associated with the withdrawal or expiry of the CDR Consumer's authorisation (see ***Step 9 in***	*See Original CDR PIA report.*	*See Original CDR PIA report.*

WITHDRAWAL OR EXPIRY OF CDR CONSUMER'S AUTHORISATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	the Original CDR PIA report), which will also apply to situations where a Principal ADR engages a Provider ADR under a CAP Arrangement.		

Suspension, revocation or surrender of accreditation

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

26.	**Continued use of CDR Data by, or disclosure to, previously-accredited data recipient (either Principal ADR or Provider ADR), after accreditation ends**
	
	There is a risk that a previously-accredited data recipient (either the Provider ADR or the Principal ADR) 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 CAP Arrangement (either the Principal ADR or the Provider ADR, as relevant).
			Noting the seriousness of this risk, we consider that it would be appropriate for the CDR Rules to clearly provide further protections for CDR Consumers, which could include:
			
			• requiring, if either the Principal ADR's, or the Provider ADR'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 ADR or the Provider ADR, 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 CAP Arrangement;
			• implementing systems (e.g. through the ACCC CDR ICT system) which will ensure anyone using the Principal ADR's credentials (including a Provider ADR) is notified of a suspension, revocation or surrender of the Principal ADR's accreditation; and

SUSPENSION, REVOCATION OR SURRENDER OF ACCREDITATION			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			• broadening the obligations in the CDR Rules so that, if a party to a CAP Arrangement is notified regarding the other party (i.e. the previously-accredited ADR 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 (noting there is no clear ability in the CDR Rules as currently drafted for the Principal ADR to direct the Provider ADR to delete or de-identify the redundant data, as necessary).
27.	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 Principal ADR or Provider ADR (as relevant) 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**
28.	It is not entirely clear from the proposed amendments to the CDR Rules when a Principal ADR will be considered to have 'collected' CDR Data. That is, does the Principal ADR 'collect' the CDR Data when it is received by the Provider ADR or only when the Provider ADR provides the CDR Data to the Principal ADR.		The ACCC may wish to consider whether this needs to be clarified.

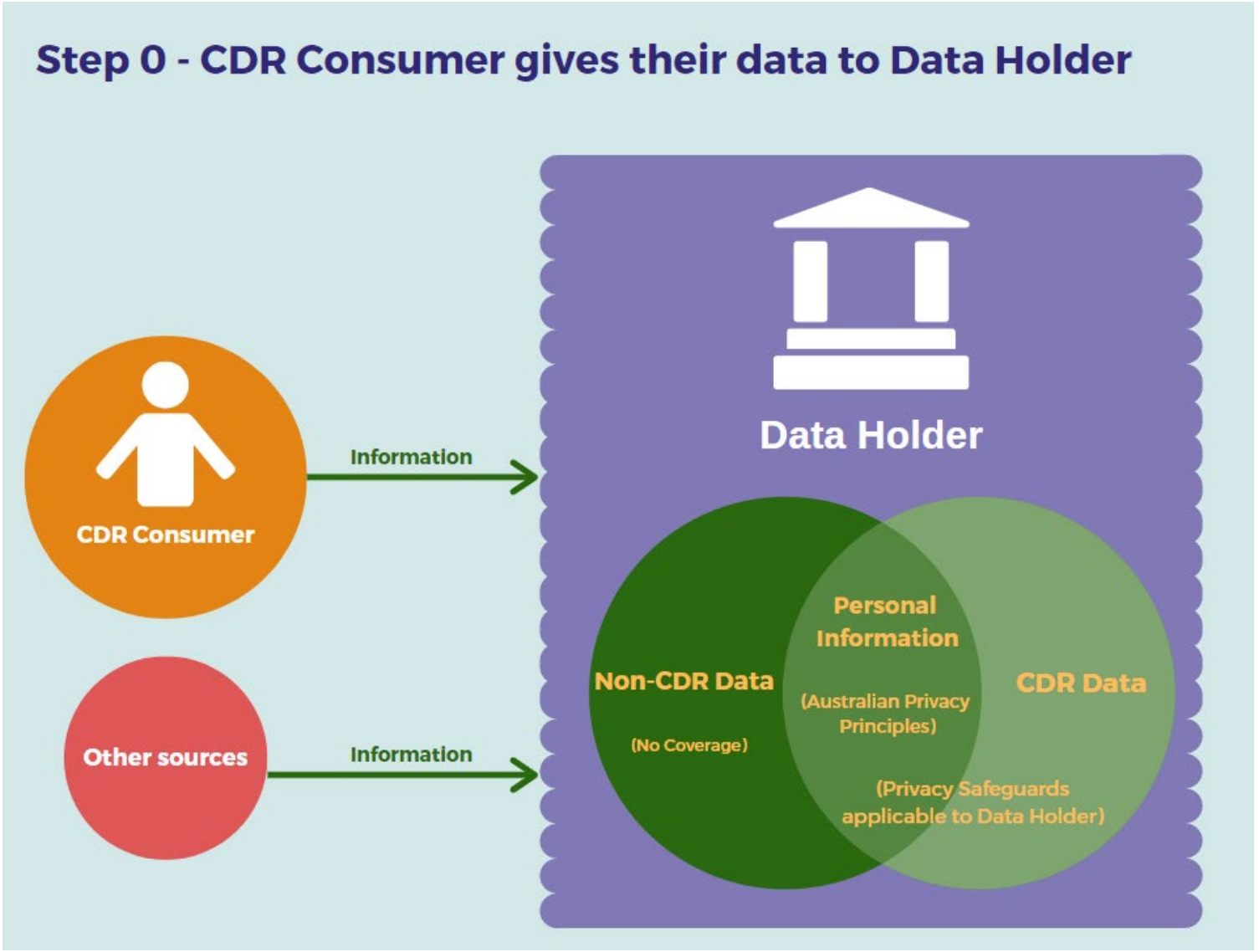
Attachment 1 Glossary

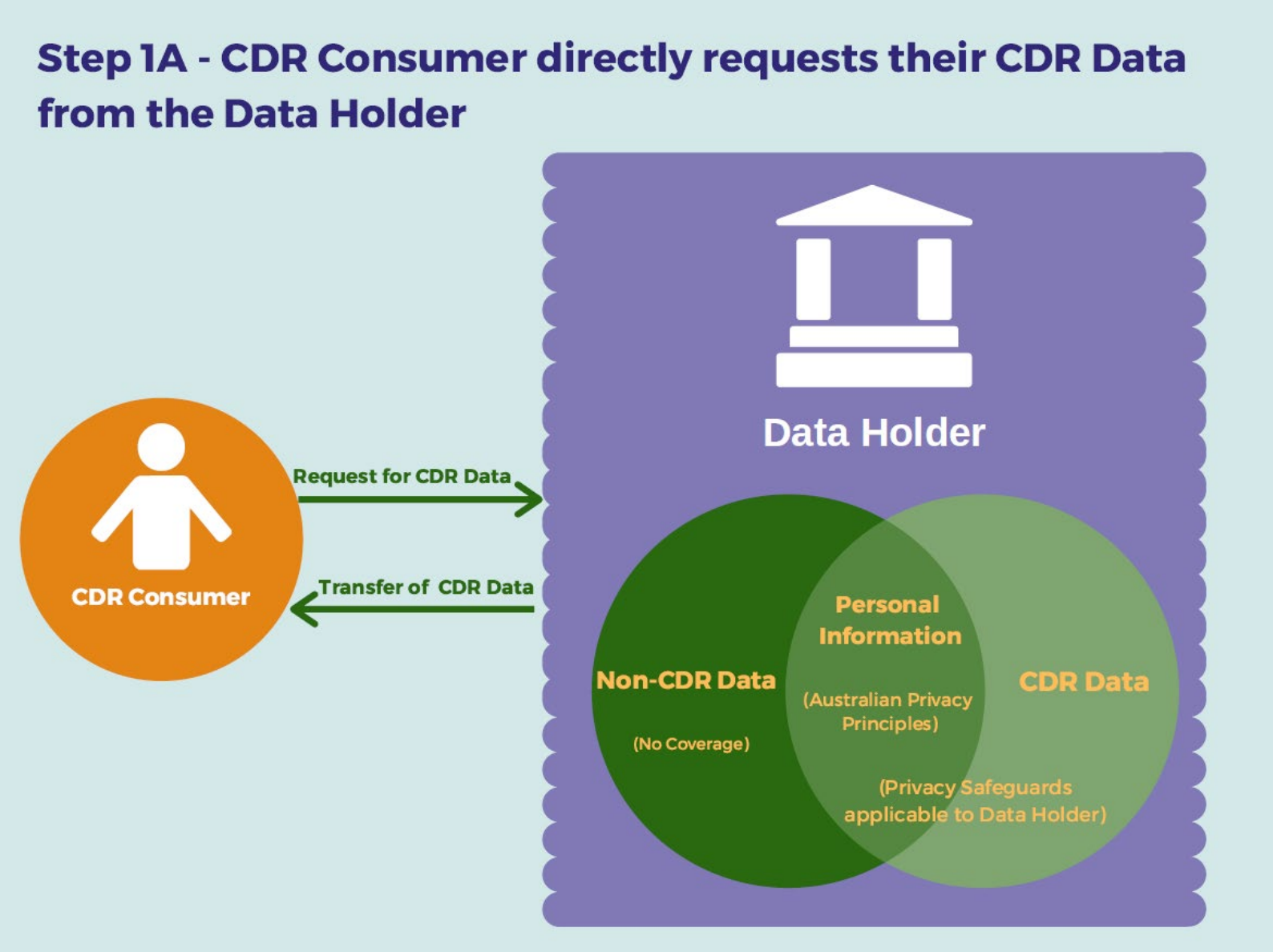
Term	Meaning
ACCC	means the Australian Competition and Consumer Commission.
Accreditation Register	means the register to be established in accordance with subsection 56CE(1) in the CDR Act.
Accredited Data Recipient (ADR)	has the meaning given by section 56AK in the CDR Act.
AFCA	means the Australian Financial Complaints Authority.
APP Privacy Policy	means a policy that is made available in accordance with APP 1.
APRA	means the Australian Prudential Regulation Authority.
ASIC	means the Australian Securities and Investment Commission.
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 Act	means the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth).
CDR Bill	means the *Treasury Laws Amendment (Consumer Data Right) Bill 2019* (Cth).
CDR Consumer(s)	has the meaning given by subsection 56AI(3) in the CDR Act.
CDR Data	has the meaning given by subsection 56AI(1) in the CDR Act.
CDR Participant	has the meaning given by subsection 56AL(1) in the CDR Act.
CDR Policy	means a policy that a CDR entity must have and maintain in compliance with subsection 56ED(3) in the CDR Act.
Chair of the Data Standards Body	means the person holding an appointment under section 56FG in the CDR 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 Data Right	means the consumer data right established by the CDR Act.
Consumer Experience	means the guidelines of that name, as published by Data61.

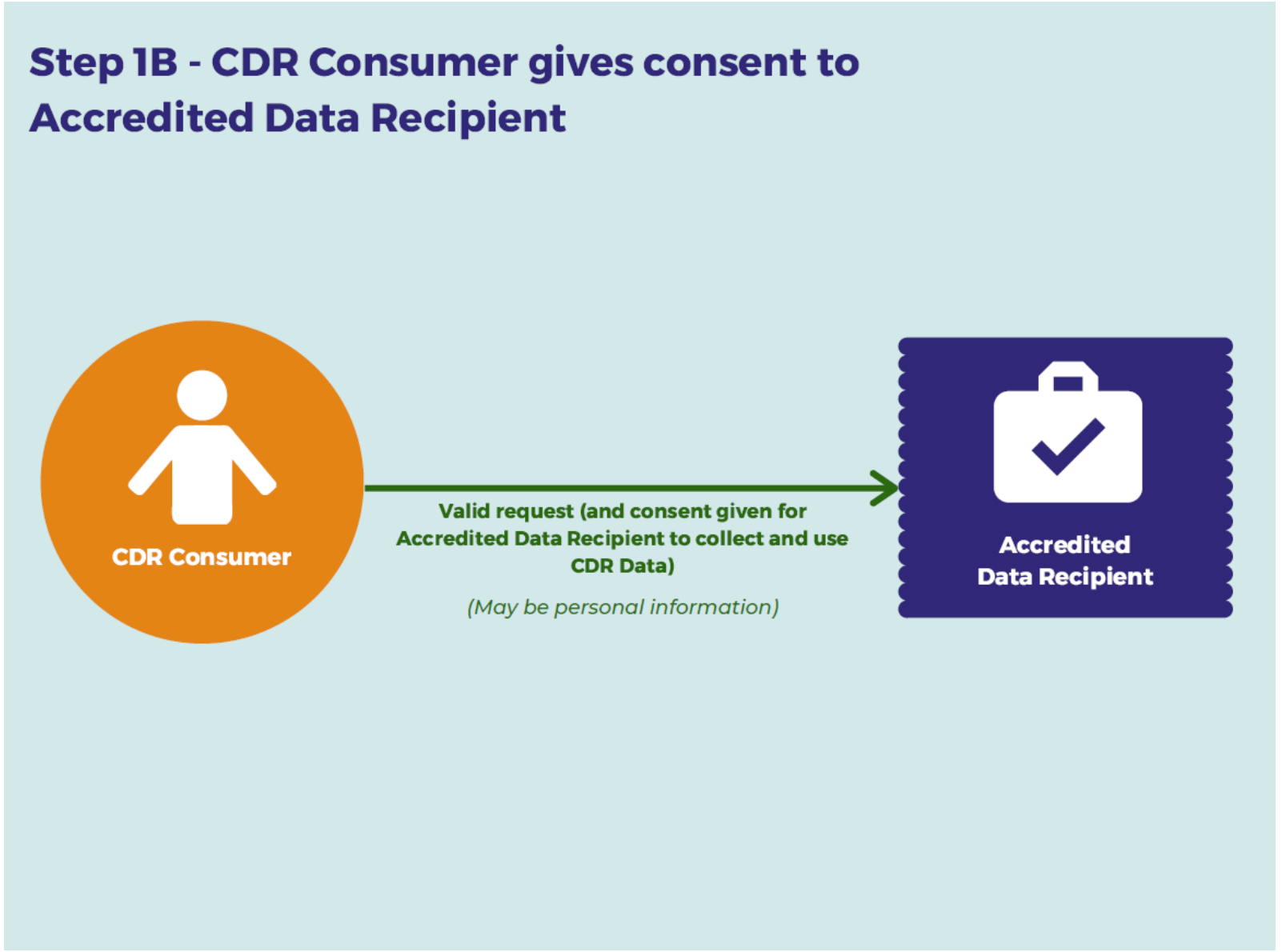
Guidelines (CX Guidelines)	
Data Holder	has the meaning given by subsection 56AJ in the CDR Act.
Data Recipient Accreditor	means the person appointed to the role of Data Recipient Accreditor in accordance with subsection 56CG in the CDR Act.
Data Standards Body	means the body holding an appointment under subsection 56FJ(1) in the CDR Act.
De-identification Decision-Making Framework	means the framework of that name, as published by the OAIC and Data61.
Department	means the Department of the Treasury.
Draft API Standards	means the standards created in response to the CDR Act, which will be binding once finalised.
Data Standards	means the data standards made under subsection 56FA in the CDR Act.
CDR Rules	means the *Competition and Consumer (Consumer Data Right) Rules 2020*.
Eligible Data Breach	has the meaning given to that term in the *Privacy Amendment (Notifiable Data Breaches) Act 2017* (Cth).
Final Report	means the Final Report of the Open Banking Review.
General Data Protection Regulation (GDPR)	means the *General Data Protection Regulation 2016/679.*
Information Commissioner Act	means the *Australian Information Commissioner Act 2010* (Cth).
Key Principles	means the key principles underpinning the implementation of the CDR regime.
OAIC	means the Office of the Australian Information Commissioner.
Open Banking Designation	means the *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (Cth).
Open Banking Review	means the review of that name, commissioned by the Australian Government on 20 July 2017.
PIA Guide	means the *Guide to undertaking privacy impact assessments,* published by the OAIC.
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 in the CDR Act.
Product Data	means CDR Data for which there are no CDR Consumers.
Product(s)	means a product offered by a Data Holder.

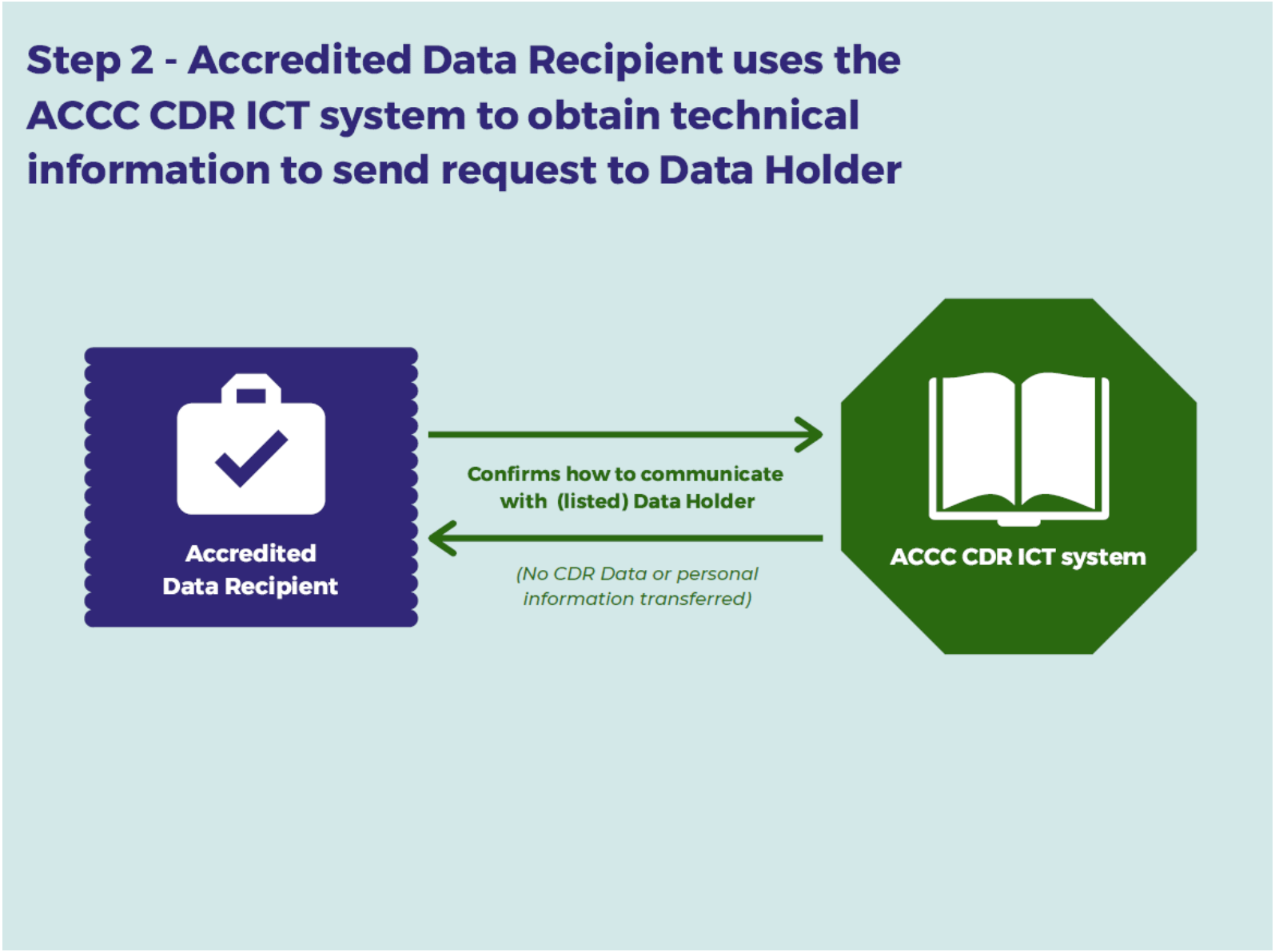
Project Description	means the project description at Part D of this PIA Update report.
Sector(s)	means a sector of the Australian economy.
Senate Committee	means the Senate's Economics Legislation Committee.
Senate Report	means the final report of the Senate's Economics Legislation Committee.

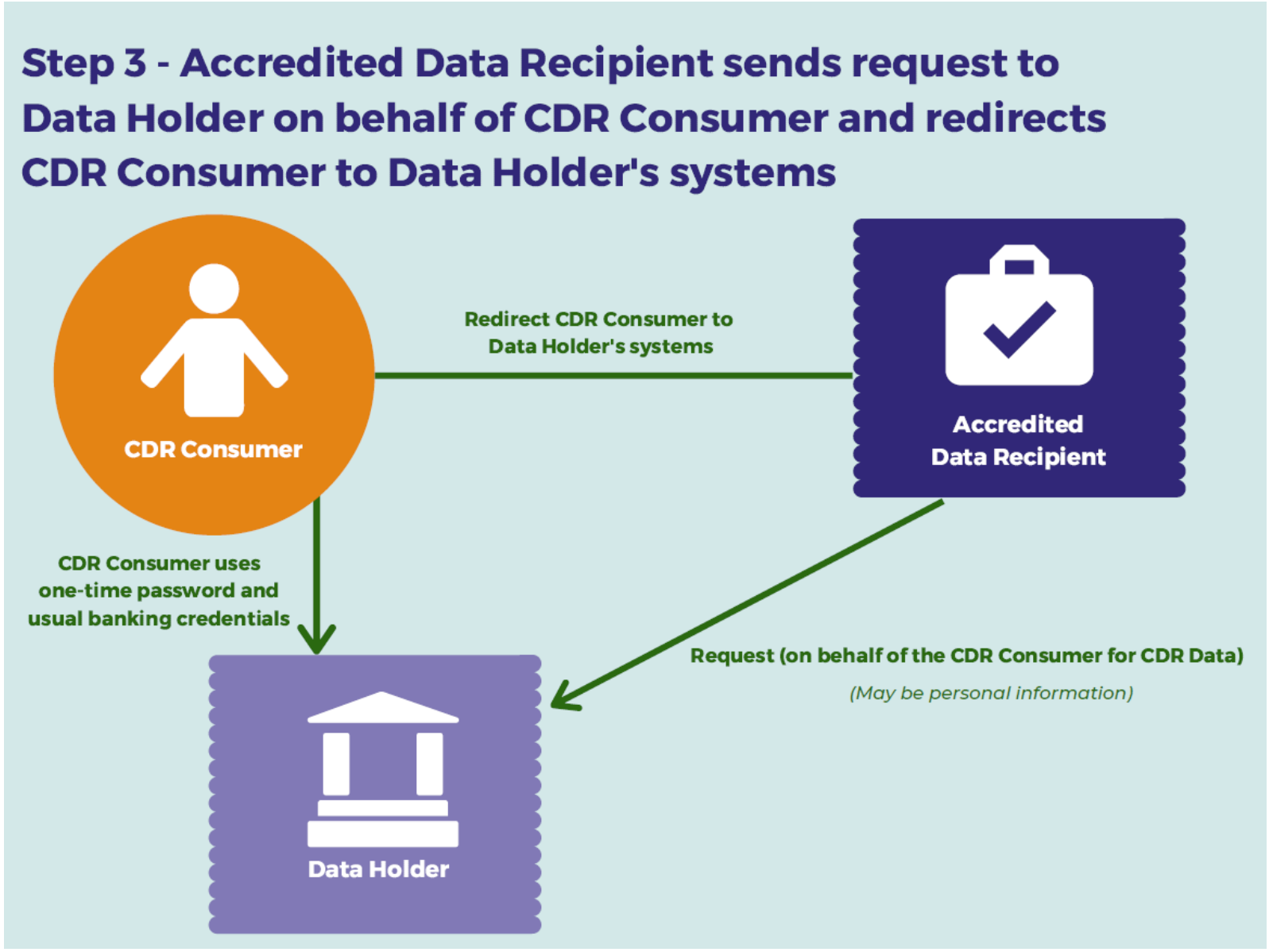
Attachment 2 Steps in the Original CDR PIA report (Diagram of Information Flows)

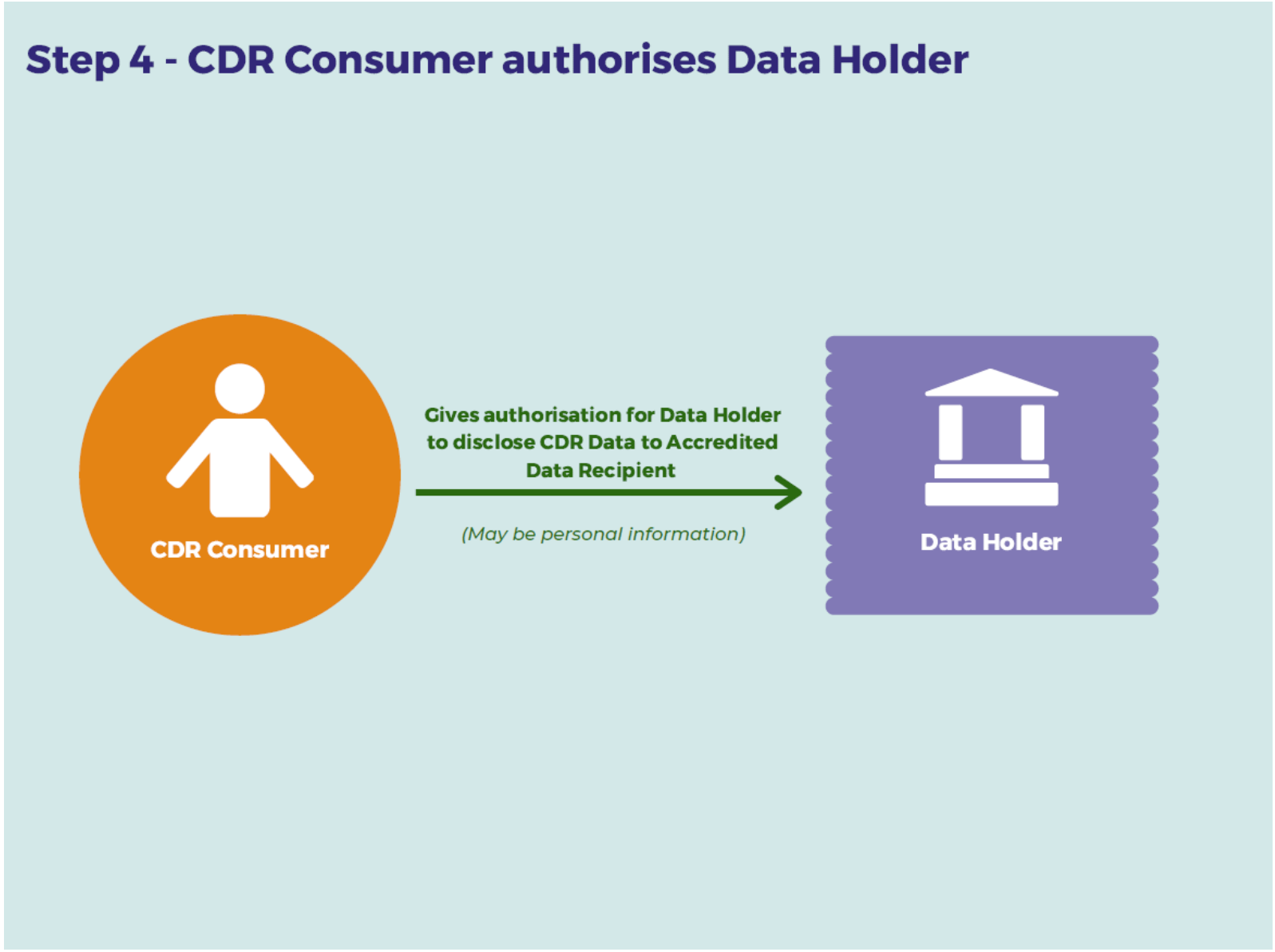


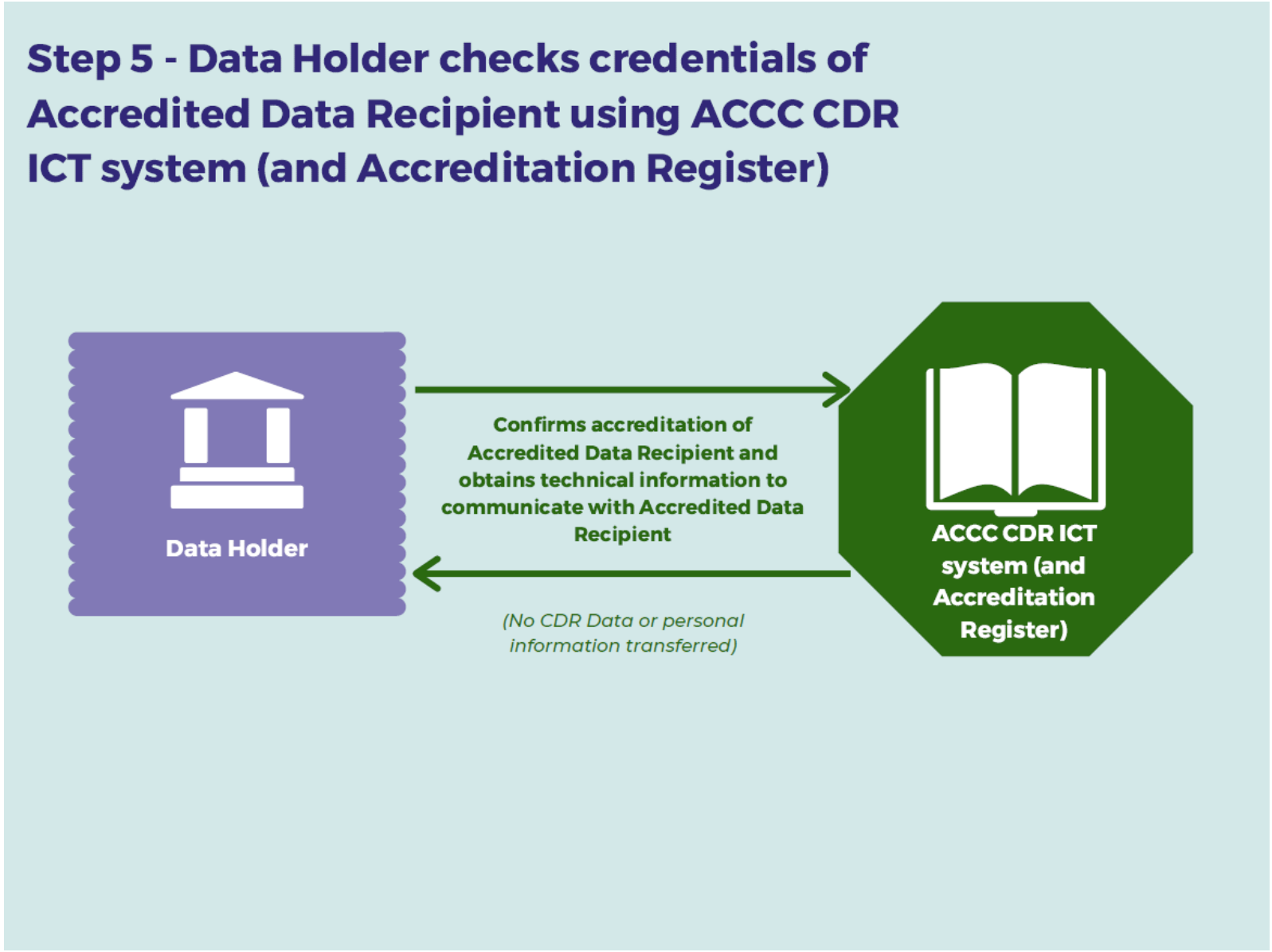

Step 1A - CDR Consumer directly requests their CDR Data from the Data Holder
Data Holder
Request for CDR Data
Transfer of CDR Data
CDR Consumer
Non-CDR Data
(No Coverage)
Personal Information
(Australian Privacy Principles)
CDR Data
(Privacy Safeguards applicable to Data Holder)


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

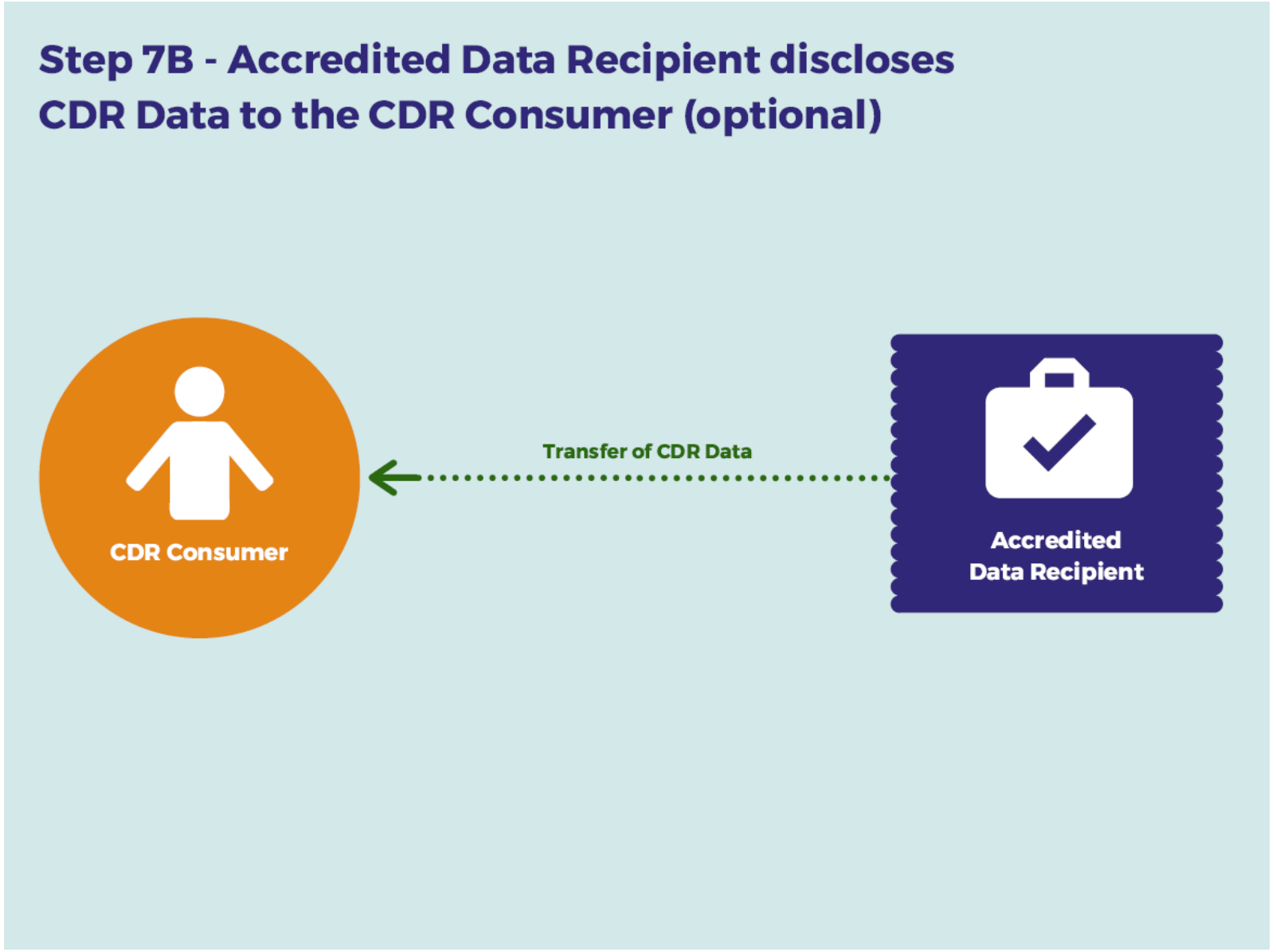

Step 3 - Accredited Data Recipient sends request to Data Holder on behalf of CDR Consumer and redirects CDR Consumer to Data Holder's systems
CDR Consumer
Redirect CDR Consumer to Data Holder's systems
Accredited Data Recipient
CDR Consumer uses one-time password and usual banking credentials
Request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

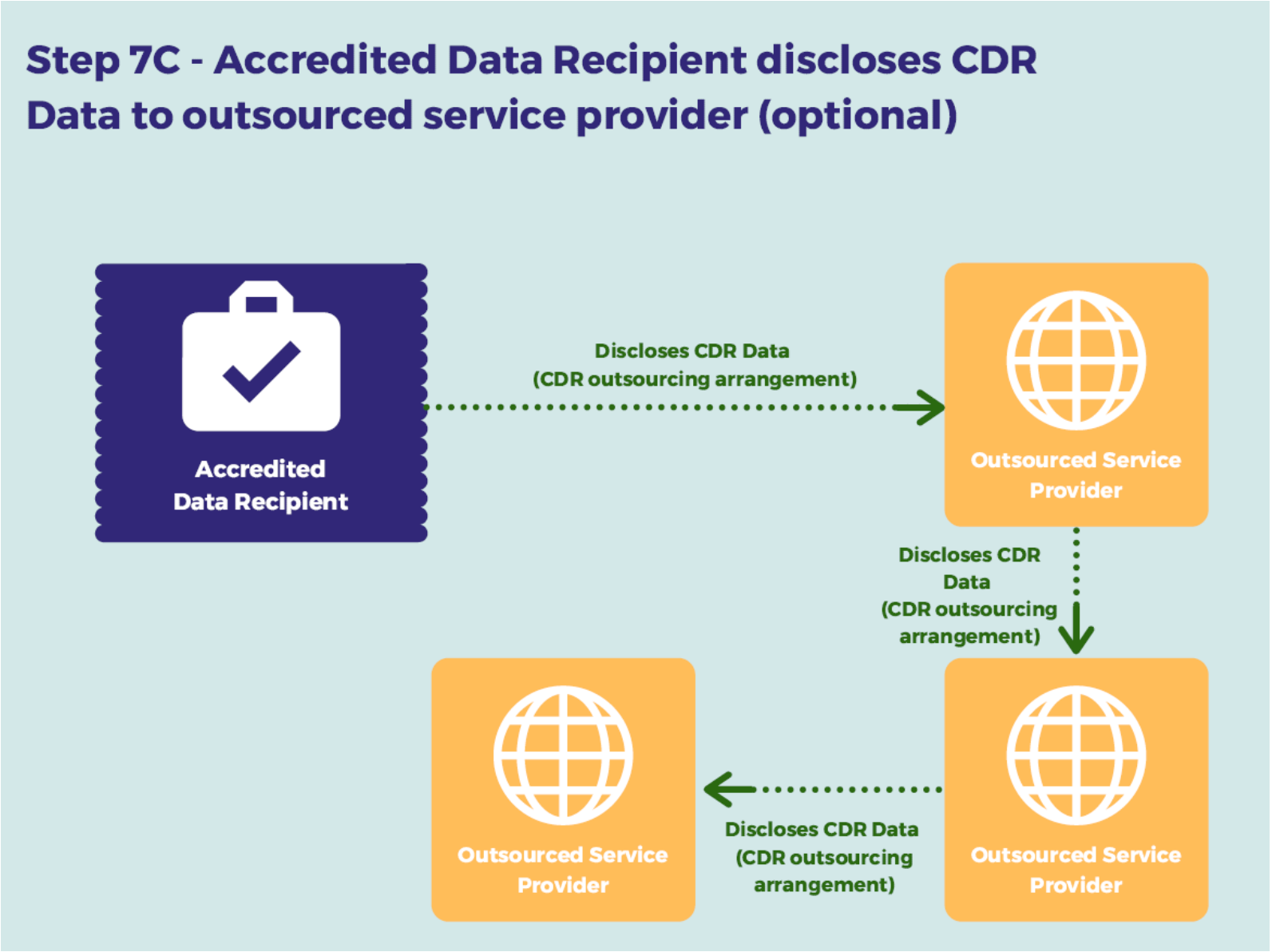

Step 4 - CDR Consumer authorises Data Holder
CDR Consumer
Gives authorisation for Data Holder to disclose CDR Data to Accredited Data Recipient
(May be personal information)
Data Holder


Step 5 - Data Holder checks credentials of Accredited Data Recipient using ACCC CDR ICT system (and Accreditation Register)
Data Holder
Confirms accreditation of Accredited Data Recipient and obtains technical information to communicate with Accredited Data Recipient
(No CDR Data or personal information transferred)
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

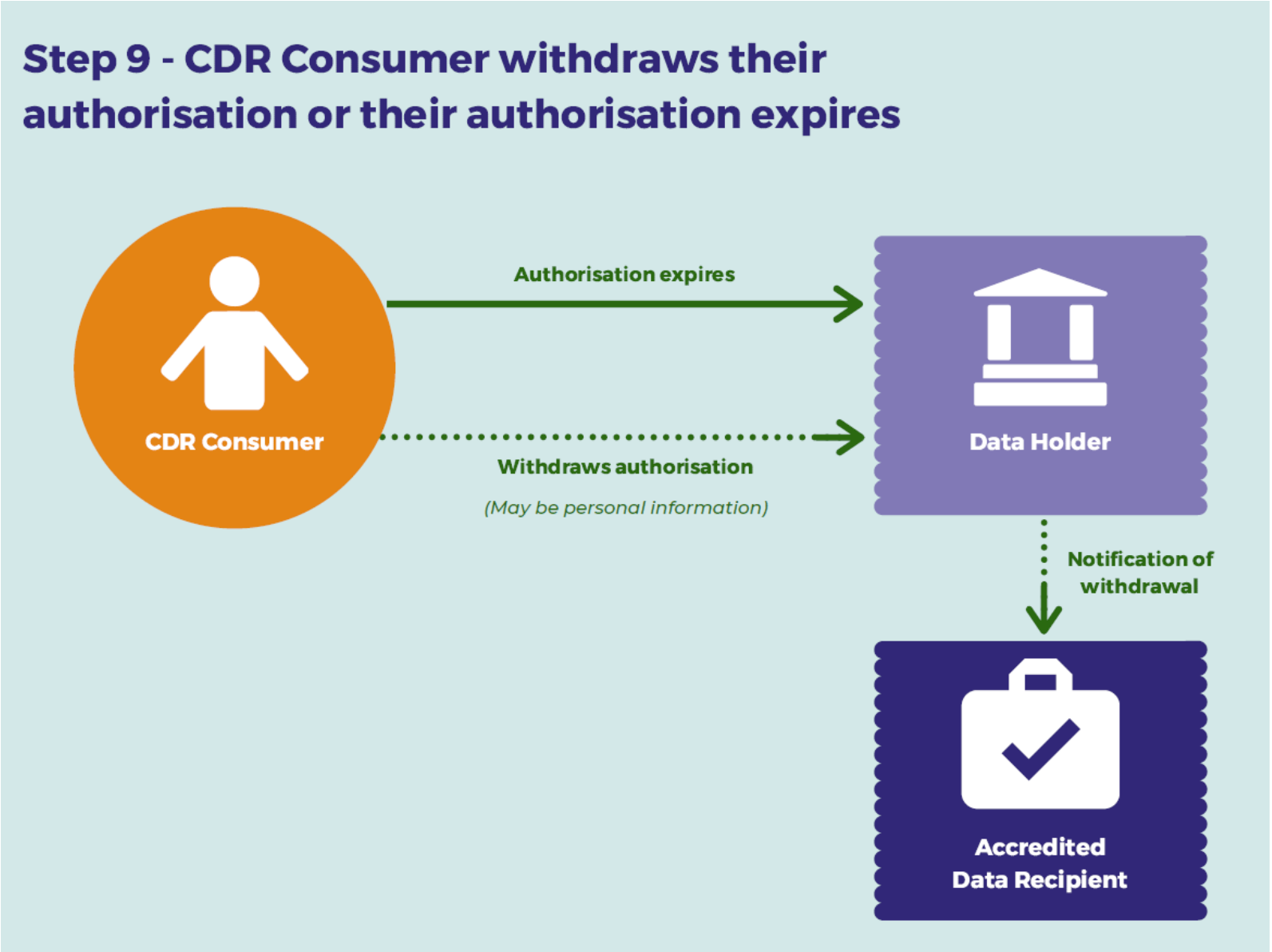
Step 7A - Accredited Data Recipient uses CDR Data to provide goods or services requested by the CDR Consumer

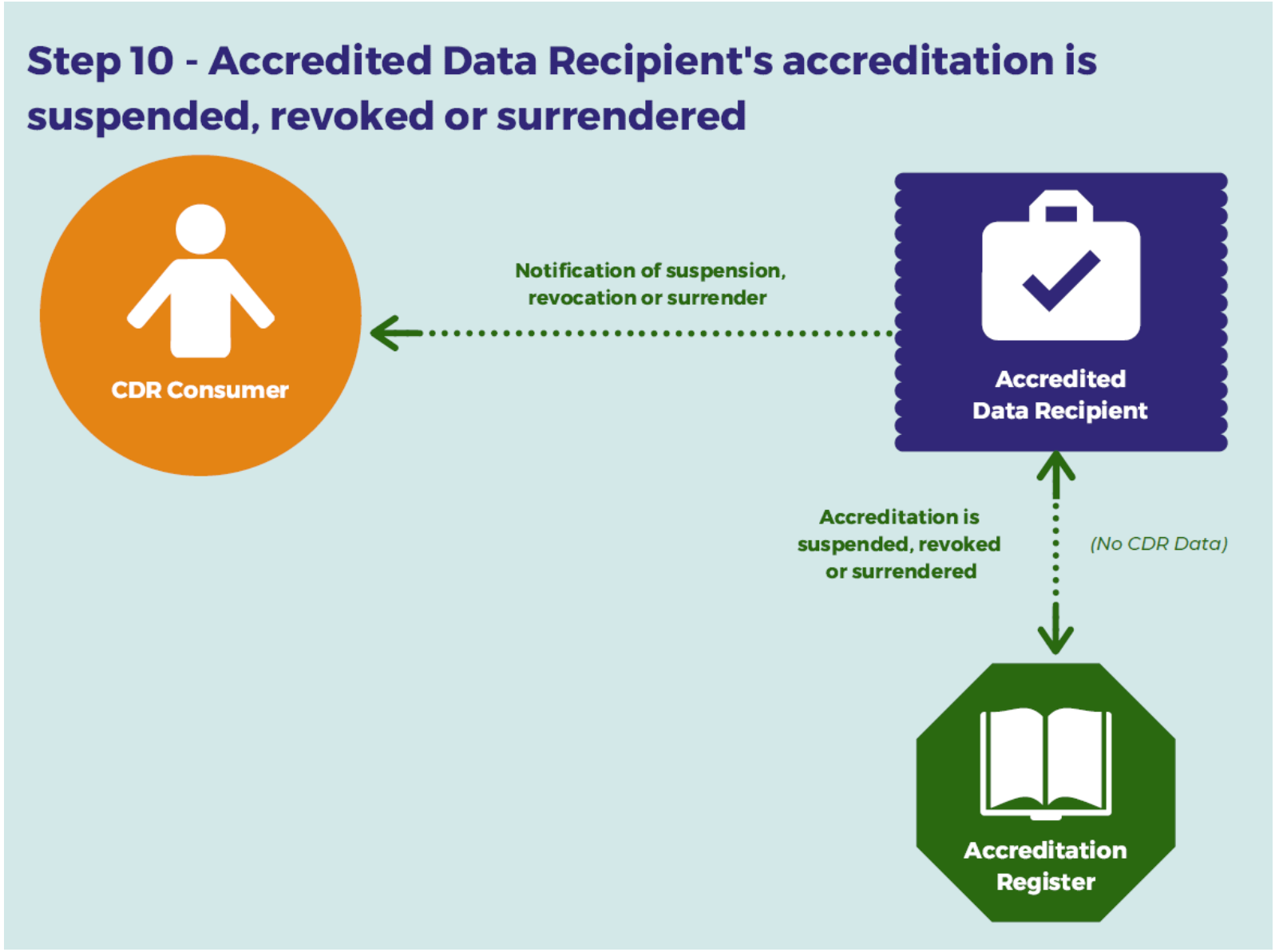

Step 7B - Accredited Data Recipient discloses CDR Data to the CDR Consumer (optional)
Transfer of CDR Data
CDR Consumer
Accredited Data Recipient


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