Maddocks

Department of the Treasury

CONSUMER DATA RIGHT REGIME

[Analysis as at 23 September 2019]

PIA report finalised on 29 November 2019

Contents

Part A – Introduction

1. Overview

1.1 Maddocks is very pleased to provide this **[draft]** privacy impact assessment report (**PIA report**) to the Department of the Treasury (**Department**).

1.2 In undertaking an independent privacy impact assessment (**PIA**) in relation to the initial implementation of the CDR regime, we have been conscious of the importance of the introduction of the CDR regime and the fundamental need to ensure its framework contains appropriate privacy safeguards so that individuals are not unnecessarily exposed to risks of harm. We have approached the PIA with genuine enthusiasm about the opportunity to help shape the future of privacy in Australia.

1.3 We would like to acknowledge the support we have received from stakeholders during our undertaking of this PIA. Many stakeholders have been very generous in providing their time and resources to help us to better understand the various privacy risks, the operation of the technological infrastructure that will be used, and the interactions between the various legislative components of the CDR regime. We are grateful for their cooperative attitude towards the undertaking of this PIA.

1.4 As explained in **Part C** of this PIA report, we have undertaken this PIA as a "point in time" analysis of the proposed initial implementation of the CDR regime. During the conduct of our PIA, the legislative framework which will implement the CDR regime has continued to evolve.

1.5 However, we have been pleased to see that further iterations of the CDR Bill which eventually became the CDR Act, and new versions of the Draft Rules and Draft Data Standards which were published during our analysis, often addressed privacy risks that we had identified, by introducing further mitigation strategies to reduce the likelihood or impact of those privacy risks. In addition, after completion of our analysis, further draft guidance about the CDR regime was released by the OAIC, which we trust will provide further clarity for CDR Participants and consumers as recommended in this PIA report.

1.6 We hope that the analysis contained in this report, and our recommendations if implemented, will continue this process of improvement, in order to ensure that the CDR regime is, and can be demonstrated to be, a privacy-enhancing component of Australia's privacy regime.

2. Structure of this PIA report

2.1 This PIA report is structured into the following sections:

2.1.1 **Part B - Executive Summary**: This 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 details how we have undertaken the PIA, and some information about its scope.

2.1.3 **Part D - Project Description:** This contains a summary of the initial implementation of the CDR regime, describes the applicable legislative framework,

and discusses the various relationships and information flows involved in the CDR regime.

2.1.4 **Part E - Fundamental Concepts:** Because the legislative framework is complex, in this section we discuss some key concepts in order to provide further background to our analysis.

2.1.5 **Part F - Analysis of APP Application and Compliance:** In this section, we have analysed the application of the Australian Privacy Principles (**APPs**) under the Privacy Act and the Privacy Safeguards (**PSs**) in the CDR Act, and key differences between them.

2.1.6 **Part G - Analysis of Risks Associated with Information Flows in the CDR regime:** In this section, we have analysed the risks that we have identified as being associated with particular information flows in the CDR regime. We have identified the current mitigation strategies, and conducted a gap analysis to identify any areas of concern. To assist we have created information flow diagrams for each step that we have identified (these are set out in **Attachment 2** to this PIA report).

2.1.7 **Part H - Other Privacy Risks:** This section sets out further privacy risks that have not been discussed in detail in other parts of this PIA report.

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

2.1.9 **Attachment 2 - Information Flow Diagrams:** This contains larger versions of the diagrams that are referenced in **Part G** of this PIA report.

2.1.10 **Attachment 3 - List of Material Reviewed:** This will contain a list of relevant material we have reviewed as part of undertaking our analysis.

2.1.11 **Attachment 4 - List of Stakeholders Consulted:** This contains a list of stakeholders that we have consulted, including stakeholders who provided us with a submission in relation to a draft version of this 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 CDR regime, as well as a consolidated list of all of the recommendations we have made as a result of our analysis of the CDR regime and the associated privacy risks we have identified during that analysis.

3.2 This **Part B [Executive Summary]** will also contain consolidated responses from the Department, in consultation with other Commonwealth agency stakeholders as required.

4. Summary of findings

4.1 We have identified several privacy risks related to the initial implementation of the CDR regime. These include privacy risks associated with:

4.1.1 changes being made to the CDR regime after the "point in time" analysis that we have completed (such as the CDR regime being applied to another Sector) without any additional privacy risks associated with the change not being identified, and appropriately mitigated;

4.1.2 the complexity of the CDR legislative framework, meaning that CDR Participants may not understand their rights and obligations under the CDR regime, including:

(a) when CDR Data is governed by the APPs and/or the Privacy Safeguards;

(b) their obligations as a particular type of CDR Participant; and

(c) how the APPs and the Privacy Safeguards apply to them and the data that they hold, including interactions between the APPs and the Privacy Safeguards;

4.1.3 CDR Consumers, particularly vulnerable consumers, not understanding how their CDR Data will be managed under the CDR regime, or the implications of providing consent, authorisation or other agreement;

4.1.4 some areas that could be further expanded in scope or clarified in the Draft Rules (as specified in further detail throughout this PIA report);

4.1.5 the complexity of the Draft Data Standards (including because of the use of language which does not make it easy to determine which parts of the Draft Data Standards are binding legal requirements);

4.1.6 the sensitivity of dealing with joint account holders in the banking Sector, and in balancing interests between the protection of privacy of joint account holders against the need to facilitate access to information;

4.1.7 third party information included in CDR Data being disclosed by Data Holders to Accredited Data Recipients;

4.1.8 Accredited Data Recipients of CDR Data subsequently becoming Data Holders for that CDR Data, without CDR Consumers understanding the implications of this;

4.1.9 lack of clarity around the legal obligations of Data Holders about their required interactions with the Accreditation Registrar, including testing to ensure compliance with the Draft Data Standards;

4.1.10 resourcing for OAIC and ACCC, as the relevant regulators, to ensure that the risks identified in this PIA report (including the above risks) are appropriately addressed; and

4.1.11 the framework for ongoing monitoring and enforcement of CDR regime, and the need for a clear, effective and consistent process for resolution of complaints by CDR Consumers.

4.2 Each of these risks is discussed further in the subsequent Parts of this PIA report, and many of them already have some privacy protections built into the legislative framework in order mitigate against the likelihood or severity of that risk.

4.3 However, we have made the recommendations in paragraph 5 of this **Part B [Executive Summary]** to further mitigate against these risks where we consider existing strategies may not be desirable. We believe that implementation of these recommendations will further enhance privacy protections for individuals in connection with the CDR regime.

4.4 We do acknowledge that (as discussed in more detail in **Part C [Methodology]**) our analysis has been conducted from a privacy perspective, and our recommendations have arisen from that analysis. We recognise that, although the protection of privacy is of the utmost importance, implementation of our recommendations will need to be considered and balanced against other competing priorities and policy requirements. Factors such as the time for implementation, the costs of implementation, technical capabilities and limitations of the CDR Participants in the CDR regime, and the need to achieve the objectives of the CDR Act as passed by the Australian Parliament, will also factor into whether, and if so how, each recommendation is adopted. Nevertheless, we trust that our recommendations will raise awareness of the different privacy risks associated with the CDR regime, and assist in ensuring that their importance is considered during implementation of the CDR regime.

5. List of Recommendations

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 report.

Recommendation 1: Further updates to this PIA

Our analysis in this PIA report has been undertaken on the basis of the "point in time" development of the CDR Act, Draft Rules, Draft Data Standards and the Open Banking Designation (i.e. the legislative framework).

We **recommend** that this PIA report be treated as a "living document", which is further updated and/or supplemented as the various components of the legislative framework are revised and/or extended.

We also **recommend** that the criteria for triggering a further PIA should be clearly identified, and either included in the Draft Rules, or be otherwise publicly committed. For example, such criteria could include reconsideration of this PIA being triggered by any of the following being proposed:

- a change which would apply the CDR regime to another Sector;
- a change to the scope of the data for which the CDR regime will apply in a particular Sector;
- a change to the scope of Data Holders for which the CDR regime will apply in a particular Sector;
- the introduction of designated gateways or other intermediaries in a particular Sector, where this was not part of the initial implementation of the CDR regime for that Sector;
- changes to other legislation that affects, or intersects with, the privacy obligations under the CDR regime (such as future changes to the Privacy Act);
- changes that would alter the information flows identified in this PIA report, or would remove or reduce any privacy mitigation strategies identified in this PIA report;
- changes to the legislative framework (including the Draft Rules or Draft Data Standards) that would impact on the application of the Privacy Safeguards and/or APPs, or remove or reduce any privacy mitigation strategies in the legislative framework identified in this PIA report, or which would introduce new privacy risks; or
- a 'significant' Eligible Data Breach occurs (where 'significant' is defined as affecting a certain number of CDR Consumers, or having a defined likelihood or impact of harm).

In addition to the above, the Department could consider adopting regular reviews to assess whether any criteria have been triggered requiring this PIA report to be updated, and such reviews should be scheduled into the Department's work schedule.

This PIA report could also be updated or supplemented once further information about the Accreditation Register (e.g. information about its design and operation), and how it will operate within the ACCC's broader ICT system for the CDR regime, is available. For example, a future post implementation review could be conducted once all elements of the CDR regime are settled and finalised, including the Accreditation Register and the ACCC's broader ICT system for the CDR regime.

Recommendation 2: Further guidance on operation of the CDR regime

The CDR legislative framework, operating across different documents, is very complex. We suggest that guidelines which may be issued, and other activities which may be undertaken, by the Information Commissioner under section 56EQ in the CDR Act will be critical to ensuring that Data Holders, Accredited Data Recipients, outsourced service providers and CDR Consumers are able to understand their rights and obligations under the CDR regime.

We **recommend** that the Information Commissioner be asked to particularly focus on providing guidance about:

2.1 when the protections in the CDR legislative framework will apply to particular data (including explaining if data may be subject to both the APPs and Privacy Safeguards, and at what point the information is captured by the CDR regime and no longer falls within the protections of the APPs);

2.2 when entities will be a Data Holder under the CDR regime (and particularly when an Accredited Data Recipient may become a Data Holder in respect of CDR Data it has collected in accordance with the Draft Rules); and

2.3 when data will be defined as CDR Data (including explaining the complexities around "materially enhanced data" and data which is "wholly or partly" derived from other data).

Further guidance could also be provided:

2.4 about measures that Data Holders and Accredited Data Recipients can take to ensure that their APP Privacy Policy and CDR Policy can be easily accessed and compared by CDR Consumers;

2.5 to assist CDR Consumers to understand the implications if they agree to an Accredited Data Recipient de-identifying their CDR Data for the purposes of further disclosure;

2.6 to assist CDR Consumers, who wish to complain about privacy issues in connection with the CDR regime, to understand how their complaint will be managed, and by which regulator;

2.7. about the required treatment of redundant data, including the technical requirements for de-identification in accordance with the Draft Rules and Draft Data Standards; and

2.8. to assist Accredited Data Recipients and Data Holders in understanding the potential impact of any disclosure to a CDR Consumer of actual or suspected family violence as the reason for a refusal to provide CDR Data.

We note that since completion of the analysis in this PIA report, the OAIC has released further draft guidance about the CDR regime,[1] and the OAIC may wish to consider whether that draft guidance appropriately covers the above issues.

We have noted the clear view expressed by some stakeholders that consumer education is not, by itself, likely to be sufficient to mitigate against identified privacy risks, and that this is particularly so for vulnerable CDR Consumers (where vulnerability is likely to be broader than just that related to lack of education or disability, but may include vulnerability related to financial or other stress). Accordingly, we do not consider that **Recommendation 2** in isolation is likely to be sufficient protection for these individuals or businesses.

Recommendation 3: Further consideration of the Draft Rules

The Draft Rules have not yet been finalised. We **recommend** that the ACCC should be asked to consider whether the Draft Rules should be further amended before finalisation to:

3.1 include a process for testing a Data Holder's compliance with the Draft Data Standards (including when, how, and how often, testing will occur), possibly also including assessment of a Data Holder's security in relation to the transmission of CDR Data;

[1] We understand that this guidance is primarily designed to assist Data Holders and Accredited Data Recipients, but that further guidance designed to assist CDR Consumers is being developed.

3.2	include an obligation on Data Holders to "warn" CDR Consumers when providing them with their CDR Data pursuant to their request (for example to state that the protections of the CDR regime (and possibly the APPs) will not apply if they provide that data to a third party). Similarly, if an Accredited Data Recipient discloses CDR Data to the CDR Consumer (which is a 'permitted use' of that CDR Data), indicate whether a similar protection is required in these circumstances;
3.3	require CDR receipts to be given in respect of both consents and authorisations, and also provide advice about what the CDR Consumer should do if the consent(s) and authorisation(s) recorded do not match their understanding of the consent(s) and authorisation(s) that have been given. The Draft Rules could also be clarified to determine the consequences if the CDR Consumer acts on this advice (e.g. whether the consent(s) and/or authorisation(s) are rendered void and need to be re-obtained); or
3.4	expressly ensure that contractual arrangements between an Accredited Data Recipient and a CDR Consumer cannot override rights and protections provided to CDR Consumers by the legislative framework (e.g. by providing that any such clause will have no effect). If it is decided that it is not legally and/or technically necessary to implement this recommendation, we consider that the ACCC should take steps to ensure that Accredited Data Recipients have clear guidance in relation to the effect of attempting to override the rights and protections for CDR Consumers in the CDR regime.

Recommendation 4: CDR Consumer right to access CDR Data held by the Accredited Data Recipient

We **recommend** that the Department consider whether a right for CDR Consumers to access their CDR Data whilst it is held by the Accredited Data Recipient (similar to the rights afforded under APP 12) should be included in the CDR regime.

Recommendation 5: Draft Data Standards

We **recommend** that the Draft Data Standards should be recast into language that will allow CDR Participants to easily distinguish which parts of Draft Data Standards are binding legal requirements. Further, we **recommend** that as the Draft Data Standards change and are updated, there needs to be adequately detailed version control to allow for easy identification of any changes to the Draft Data Standards (to ensure the consistent implementation of the Draft Data Standards by all CDR Participants).

Recommendation 6: Joint account holders in the banking Sector

We **recommend** that the Department consider whether the CDR legislative framework implements an appropriate policy balance between the protection of the privacy of joint account holders, against the need to facilitate access to information by victims of family violence. The Department may wish

to issue a public statement in this regard, explaining how the competing privacy and policy issues were considered.

Further guidance should also be provided about the operation of the CDR regime to joint accounts, including the level of evidence that a Data Holder requires in order to come to a view about whether it should refuse to update a joint account holder's Consumer Dashboard in order to prevent physical or financial harm or abuse.

Recommendation 7: CDR Data which includes personal information about third parties

We understand that, for the initial implementation, CDR Data which is disclosed by a Data Holder may include information about third party individuals (for example, transaction data about payment made to the CDR Consumer's account).

The third party individual will not have provided any consents (and is unlikely to be aware) that their information has been disclosed by the Data Holder to the Accredited Data Recipient, and will be used by the Accredited Data Recipient.

We understand that this issue has been carefully considered by the ACCC and the Department, including how this issue is treated in other jurisdictions (e.g. under the GDPR). We understand that the position that has been reached represents a balancing of interests, between the privacy rights of the third party individual against the utility for CDR Consumers to access and use their information, and the benefits of encouraging competition and innovation.

Although this disclosure will be permitted by law, we expect that the Australian community may have privacy concerns about this aspect of the CDR regime. We therefore **recommend** that the Department consider publishing information to support this aspect, including a clear description of the benefits for CDR Consumers, how privacy concerns have been balanced against the potential concerns third party individuals may have (including the reasons why personal information in relation to third party individuals is not required to be redacted by the Data Holder before release).

Recommendation 8: Seeking CDR Consumer agreement for an Accredited Data Recipient to become a Data Holder of CDR Data

We **recommend** that the ACCC considers whether the Draft Rules should incorporate additional protections about *how* the Accredited Data Recipients may seek agreement from the CDR Consumer for an Accredited Data Recipient of CDR Data to become a Data Holder, similar to the protections currently afforded for how consent may be sought.

Recommendation 9: Adequate ACCC and OAIC resourcing

The OAIC and ACCC, as the relevant regulators, will have critical roles to play in ensuring that risks identified in this PIA report are appropriately addressed, through the provision of suitable guidance material and the implementation of effective monitoring and enforcement regimes.

We have not investigated, or been provided with, any information about current or future funding levels for these agencies, but we **recommend** that the Department consider whether the OAIC and ACCC will have the necessary funding and resources to provide appropriate guidance material and undertake other educational activities, and to implement effective monitoring and enforcement regimes.

Recommendation 10: Consistent and effective complaints and compliance processes

We **recommend** that the ACCC and the OAIC have consistent processes so that complaints by CDR Consumers about their privacy under the CDR regime are handled by the appropriate regulator. This could include, for example, similar or identical processes and information on their websites .

We **recommend** that external dispute resolution schemes for each Sector be carefully considered, with additional guidance and resources provided as appropriate, to ensure effective resolution of any issues experienced by CDR Consumers.

We also **recommend** that the OAIC and the ACCC consider the strategies that should be included in a compliance framework for the CDR regime, and whether these should be made publicly available.

Part C Methodology

6. Our general approach to this PIA

6.1 Following an approach to market process, the Department engaged Maddocks to undertake an independent PIA in relation to the CDR regime.

6.2 A privacy impact assessment is a systematic assessment of a project that identifies the impact that the project might have on the privacy of individuals, and sets out recommendations for managing, minimising or eliminating that impact.[2]

6.3 In conducting this PIA, we have sought to:

6.3.1 inform stakeholders about the CDR regime, and illustrate the focus and value being given to privacy risks and risk mitigation;

6.3.2 assess the risks to individual privacy presented by the CDR regime, with reference to the initial implementation of the legislative framework;

6.3.3 consider compliance with the Privacy Act, including the APPs;

6.3.4 consider the Privacy Safeguards and other mitigation strategies currently proposed for the CDR regime, including to secure personal information and CDR Data from misuse, interference or loss, or from unauthorised access, modification or disclosure;

6.3.5 set out the various steps involved in the PIA and the associated information flows, in order to assist in highlighting privacy risks and treatments, and areas for potential improvement through risk mitigation; and

6.3.6 provide practical recommendation to mitigate identified privacy risks and further enhance privacy protections in the CDR regime.

7. Our methodology

7.1 We have conducted our PIA broadly in accordance with the *Guide to undertaking privacy impact assessments* (the **PIA Guide**).[3] This has involved the following steps:

[2] *Guide to undertaking privacy impact assessments (May 2014),* published by the Office of the Australian Information Commissioner (**OAIC**) (https://www.oaic.gov.au/privacy/guidance-and-advice/guide-to-undertaking-privacy-impact-assessments/).
[3] Ibid.

Stage	Description of steps
1.	**Plan for the PIA:** We reviewed publicly available background material, together with other relevant material provided by the Department (see **Attachment 3** to this PIA report). We then conducted an initial workshop with the Department, and representatives from the ACCC, the Data Standards Body, and the OAIC, to facilitate our understanding of the proposed operation of the CDR regime. We also agreed on the scope of the PIA (discussed further in this **Part C** below), the approach to a broader stakeholder consultation process, and the timeframes for the necessary activities involved in conducting the PIA.
2.	**Project description and information flows:** We prepared an initial draft Project Description, which described the CDR regime, including aims and the various relationship and information flows. The initial draft was refined following feedback from the initial workshop participants.
3.	**Initial stakeholder consultation:** In addition to ongoing consultation with the initial workshop participants, a series of targeted initial workshops were conducted with key stakeholders (the Australian Privacy Foundation, the Australian Banking Association, the Financial Rights Legal Centre, Fintech Australia, and the Consumer Policy Research Centre). These workshops were designed to allow us to confirm our understanding of the operation, implementation and privacy risks of the CDR regime from several different perspectives, with a view to ensuring the initial drafts of the documents that we produced for the PIA report properly identified and considered key potential privacy risks (with the aim of reducing time and resources needed by the broader stakeholder community).
4.	**Privacy impact analysis and compliance check:** In this stage, we identified and critically analysed how the initial implementation of the CDR regime will impact upon privacy, both positively and negatively. We noted stakeholder feedback from the previous PIA (conducted internally by the Department with assistance from an external privacy expert) about the difficulty of quantifying and then labelling the level of risk associated with privacy risks. We considered that there is merit in the submission that it is almost impossible to do this in a sufficiently robust manner. This is because the likelihood and impact if a particular privacy risk eventuates will vary (from insignificant to extreme; from very unlikely to almost certain) for each individual, depending on the particular circumstances of that individual and the situation in which the risk occurs. This means that if we were to attribute an average or median risk rating for each identified risk, it would not accurately reflect the level of risk specific for any individual. For this reason, we did not attempt to provide a 'risk level' or 'risk rating' for the identified risks. Most stakeholders agreed with this approach, however we note the view of one stakeholder that including risk taxonomy would have allowed for more fulsome consideration of the impact of the risk. From the stages referred to above, we developed our recommendations to remove or reduce identified avoidable privacy risks.
5.	**Further revision in light of the revised Draft Rules**: Following the introduction of the proposed rules in August 2019, we reconsidered our analysis and recommendations to reflect any changes in the Draft Rules, including its additional mitigation strategies.
6.	**Privacy management and addressing risks:** We considered potential mitigation strategies which could further address any additional negative privacy impacts identified during the privacy impact analysis stage.

Stage	Description of steps
7.	**Recommendations:** From the stages referred to above, we prepared draft recommendations to remove or reduce identified avoidable privacy risks.
8.	**Further stakeholder consultation:** To ensure consultation with a broad range of stakeholders, Maddocks developed a publicly available PIA-specific portal, through which any person or entity who works or has an interest in the area of privacy, including in relation to the CDR regime, and who has a genuine interest in being part of the CDR PIA process, was able to register as a stakeholder. We understand that information about the portal was distributed by the Department to various contact lists of persons who had previously indicated their interest in the CDR regime. We received 57 expressions of interest in being a stakeholder through the portal. Draft documents containing aspects of this PIA report were distributed to all initial stakeholders and to this broader stakeholder list as they were developed, with an invitation to provide any feedback and other input in relation to those documents.
9.	**Stakeholder submissions and further stakeholder engagement**: We received 13 written submissions from stakeholders, and we carefully considered the feedback in each of these submissions. Where we considered that further engagement with a particular stakeholder was required in order for us to fully understand and appreciate the matters raised by the stakeholder in their submission, we undertook further discussions with that stakeholder as required.
10.	**Privacy management and addressing risks:** We further refined the potential mitigation strategies which could further address any additional negative privacy impacts identified during the privacy impact analysis stage.
11.	**Recommendations:** From the stages referred to above, we refined our recommendations to remove or reduce identified avoidable privacy risks.
12.	**Report:** We finalised this PIA report.
13.	**Respond and review:** We understand that the Department will review this PIA report, in consultation with other stakeholders as required, to include responses to our recommendations.

8. Scope of this PIA

"Point in time" analysis of the initial implementation of the CDR regime

8.1 As discussed in more detail in **Part D [Project Description]** of this PIA report, the CDR Act has been specifically designed to allow further expansion of the CDR regime after the initial implementation (i.e. to an expanded range of Data Holders, and covering an expanded range of CDR Data, in the banking Sector; and then further expansion to Sectors other than the banking Sector).

8.2 During the process of conducting this PIA, the CDR Bill received royal assent, thus becoming the CDR Act, but the Open Banking Designation, Draft Rules, and the Draft Data Standards, were still subject to further examination, consultation and development.

8.3 It was determined that, despite the likelihood that the Open Banking Designation, Draft Rules and the Draft Data Standards would change before being finalised, the most useful approach was for us to undertake a "point in time" analysis and consider only the initial implementation of the CDR regime, if it was to be implemented by the versions of the CDR Act, and the Open Banking Designation, Draft Rules, and Draft Data Standards, as at 23 September 2019. Following the publication of the revised Draft Rules in August 2019, we noted that

many of the risks we had previously identified had been further mitigated and accordingly we revised our draft analysis and draft recommendations.

8.4 We note that a few stakeholders submitted that ideally our PIA process would have been conducted during the initial planning for the CDR regime, to provide enhanced confidence that privacy issues were embedded into the legislative framework as part of a genuine 'privacy by design' process.[4] Despite this, we note that our examination of the privacy impacts associated with the introduction of the CDR Act, the Open Banking Designation, the Draft Rules and the Draft Data Standards as at 23 September 2019 will allow current privacy impacts identified in this PIA report to be considered and addressed before all aspects of the legislative framework are finalised.

8.5 Accordingly, the scope of this PIA does not include consideration of:

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

8.5.2 any possible future versions of the Open Banking Designation, the Draft Rules and the Draft Data Standards.[5]

8.6 Our analysis in this PIA report has been undertaken on the basis of the "point in time" development of the CDR Act, Draft Rules, Draft Data Standards and the Open Banking Designation.

8.7 We recommend that this PIA report be treated as a "living document", which is further updated and/or supplemented as the various components of the legislative framework are revised and/or extended (see **Recommendation 1**).

8.8 We also recommend that the criteria for triggering a further PIA should be clearly identified, and either included in the Draft Rules, or be otherwise publicly committed. For example, criteria for reconsideration of this PIA could include where any of the following are proposed:

8.8.1 a change which would apply the CDR regime to another Sector;

8.8.2 a change to the scope of the data for which the CDR regime will apply in a particular Sector;

8.8.3 a change to the scope of Data Holders for which the CDR regime will apply in a particular Sector;

8.8.4 the introduction of designated gateways or other intermediaries in a particular Sector, where this was not part of the initial implementation of the CDR regime for that Sector;

8.8.5 changes to other legislation that affects, and intersects with, the privacy obligations under the CDR regime (such as future changes to the Privacy Act)[6];

8.8.6 changes that would alter the information flows identified in this PIA report, or would remove or reduce any privacy mitigation strategies identified in this PIA report;

[4] We do note that that the Department undertook an initial privacy impact assessment process (with assistance from an external privacy expert), with the final report published in March 2019. This privacy impact assessment was undertaken before substantial development of the Draft Rules or Draft Data Standards.
[5] A new version of the Draft Data Standards (version 1.0.0) has been published, but as this occurred after the "point in time" analysis conducted for this PIA, this PIA does not consider version 1.0.0 of the Draft Data Standards.
[6] For example, relevant changes to the Privacy Act could potentially arise out of the recommendations of the ACCC's 'Digital platforms inquiry' Report (https://www.accc.gov.au/publications/digital-platforms-inquiry-final-report).

8.8.7 any other change to the legislative framework (including the Draft Rules and Draft Data Standards) that would impact on the application of the Privacy Safeguards and/or APPs; and

8.8.8 a 'significant' Eligible Data Breach occurs (where 'significant' is defined as affecting a certain number of CDR Consumers, or having a defined likelihood or impact of harm)

(see **Recommendation 1**).

8.9 This PIA report could also be updated or supplemented once further information about the Accreditation Register (e.g. information about its design and operation), and how it will operate within the ACCC's broader ICT system for the CDR regime, is available. For example, a future post implementation review could be conducted once all elements of the CDR regime are settled and finalised, including the Accreditation Register and the ACCC's broader ICT system for the CDR regime (see **Recommendation 1**).

8.10 In addition to the above, the Department could consider adopting regular reviews to assess whether any criteria have been triggered requiring this PIA report to be updated, and such reviews should be scheduled into the Department's work schedule. We suggest that any such updates to the PIA occur with appropriate stakeholder consultation, to ensure that a broad range of views are obtained in relation to any such update.

8.11 We note that stakeholders who provided submissions broadly agreed with this **Recommendation 1**. As one stakeholder put it "*any changes to the CDR regime"* that are *"likely to have a significant impact on the privacy of individuals"* warrant the *"reconsideration of the risks and recommendations made by the PIA. This review process is crucial to ensuring that the CDR regime will meet its stated goal of being 'consumer focussed' "* (Submission by the Australian Banking Association).

The effectiveness of the current Privacy Act provisions

8.12 We note that there has been some criticism of the proposed CDR regime on the basis that it cannot achieve appropriate protections for individuals because the protections in Australia's other privacy laws, including the Privacy Act, are not adequate (for example, because Australians should have rights equivalent to those in the GDPR, or the protection of an Australian bill of rights).

8.13 The scope of this PIA does not extend to an examination of the appropriateness or otherwise of Australia's existing privacy laws – rather it aims to analyse the impact of the CDR regime given the application of the existing laws.

8.14 However, in general we would support the undertaking of such an examination of Australia's privacy laws, particularly given the reliance on current privacy laws to protect CDR Data when it is not covered by the additional protections of the CDR regime's legislative framework in certain circumstances (see **Part F [Analysis of APP Application Compliance]** of this PIA report for further analysis of this). We note that the recommendations arising out of the ACCC's 'Digital platforms inquiry'[7] may strengthen privacy laws in Australia to provide additional privacy protections under the CDR regime.

[7] See footnote 6 above.

The use of designated gateways or other intermediaries

8.15 Although the CDR regime has been designed so that a Sector may have one or more gateways (to which CDR Data is to be disclosed under the CDR regime), the initial implementation of the CDR regime in the banking Sector will not include such gateways.

8.16 Accordingly, this PIA report does not reference the legislative provisions dealing with designated gateways, or consider any additional or differing privacy risks associated with their potential use.

8.17 Similarly, the legislative framework may permit further disclosures of CDR Data to intermediaries acting for CDR Consumers in certain circumstances. Again, this is not contemplated for the initial implementation of the CDR regime, and so is not within the scope of this PIA.

The internal design or operation of the Accreditation Register and the ACCC's broader ICT system for the CDR regime.

8.18 The Accreditation Register will be part of a broader ICT system to be implemented by the ACCC for the CDR regime. The Accreditation Register and the broader CDR ICT system, will not collect, use, disclose, or store, any CDR Data, although it may handle other personal information including in connection with the application processes to become an Accredited Data Recipient or registered Data Holder. We also understand that although members of the public may search the Accreditation Register for information about Data Holders and Accredited Data Recipients, the Accreditation Register will not record personal information about individual members of the public accessing the Accreditation Register.

8.19 Although this PIA does consider relevant information flows to and from the Accreditation Register and the broader CDR ICT system, this PIA is not a privacy impact assessment of:

8.19.1 the Data Recipient Accreditor's handling of any personal information (for example, in or in relation to applications by persons who wish to become "accredited persons");

8.19.2 the internal design or operation of the Accreditation Register or the ACCC's broader ICT system for the CDR regime; or

8.19.3 any other handling of personal information by the Data Recipient Accreditor, or the ACCC, in connection with the Accreditation Register or the ACCC's broader ICT system for the CDR regime.

8.20 Accordingly, such matters are not within the scope of this PIA.

8.21 Some stakeholders indicated that this was unfortunate, with one stakeholder emphasising the importance of considering the internal design and operation of the Accreditation Register and its impacts on privacy risks (e.g. issues of unavailability of the Accreditation Register, and whether this would result in the Data Holder disclosing CDR Data to a person whose accreditation had been revoked or suspended).

8.22 We do appreciate that there are likely to be privacy risks associated with the Accreditation Register (including its design) and the ACCC's broader ICT system for the CDR regime, especially as technology evolves, and recognise the importance of ensuring the design of the system evolves with the latest technical standards and requirements. However, as at our "point in time" analysis, the necessary information was not available to allow this consideration in this PIA. This is why, in **Recommendation 1**, we have suggested that this PIA could also be updated once further information about the Accreditation Register and how it operates within the broader ecosystem is available.

Requests in relation to Product Data

8.23 A PIA is concerned with the impact upon the privacy of individuals. Product Data is CDR Data that relates to Products offered by a Data Holder, but which does not identify any individual CDR Consumer. Accordingly, we have not in this PIA considered issues associated with requests for Product Data, or the provision of that Product Data, under the CDR regime.

Non-privacy issues

8.24 This PIA focusses on issues that are related to personal information or privacy generally. It does not examine other related issues that, although important, are out of scope for this PIA. For example, although we understand that some concerns have previously been raised in relation to potential charges for access to CDR Data and the potential for price discrimination and/or exclusive access to products and services for some groups of individuals,[8] these matters have not been considered as part of this PIA. We note the views of some stakeholders that charging for information and access are important issues which may present a barrier for consumers in using the data portability rights afforded by the CDR regime. We have considered this aspect in relation to identified risks for a CDR Consumer's access to their CDR Data held by an Accredited Data Recipient, but remain of the view that more general consideration of this issue is not within the scope of this PIA.

Other assumptions

8.25 We have assumed that:

8.25.1 the Draft Rules may properly be made under the CDR Act (we have not, for example, examined whether they are within the permitted scope of Rules that may be validly made under the CDR Act); and

8.25.2 the Draft Data Standards may properly be made under the Draft Rules (again, we have not examined whether they are within the scope of Data Standards that may be validly made under the CDR Act and Draft Rules).

[8] This comment relates to concerns generally expressed before release of the Draft Rules. Note that, for the initial implementation of CDR regime, no charges may be payable for provision of 'required consumer data' to an Accredited Data Recipient, only for 'voluntary consumer data'.

Part D Project Description

9. Overview of the Consumer Data Right

9.1 A Consumer Data Right (**CDR**) regime is being introduced in Australia. The CDR regime aims to:

9.1.1 give CDR Consumers greater control over their data, by ensuring that they can:

(a) access their own data in a usable form; and

(b) direct the secure transfer of data to trusted third parties; and

9.1.2 give CDR Consumers greater access to data about key goods and services on offer to them.

9.2 The Australian Government wishes to implement the CDR regime according to four key principles (**Key Principles**), as follows:[9]

9.2.1 The CDR regime should be **consumer focussed**. It should be for the CDR Consumer, be about the CDR Consumer, and be seen from the CDR Consumer's perspective.

9.2.2 The CDR regime should **encourage competition**. It should seek to increase competition for products and services available to CDR Consumers so that CDR Consumers can make better choices.

9.2.3 The CDR regime should **create opportunities**. It should provide a framework from which new ideas and business can emerge and grow, establishing a vibrant and creative data sector that supports better services enhanced by personalised data.

9.2.4 The CDR regime should be **efficient and fair**. It should be implemented with security and privacy in mind, so that it is sustainable and fair, without being more complex or costly than needed.

9.3 These Key Principles are reflected in the objectives in the CDR Act,[10] which are described as:

9.3.1 enabling CDR Consumers in certain Sectors of the Australian economy to require information relating to themselves in those Sectors to be disclosed safely, efficiently and conveniently:

(a) to themselves for use as they see fit; or

(b) to Accredited Data Recipients for use subject to the Privacy Safeguards; and

[9] As noted in the Consumer Data Right booklet, published by the Department on 9 May 2018.
[10] These objectives are included in the CDR Act by an amendment to section 56AA of the CC Act. In this PIA report (unless otherwise specified), we have referenced the relevant sections of the CC Act contained in Schedule 1 of the CDR Act as being "section X in the CDR Act".

9.3.2 enabling any person to efficiently and conveniently access information in those Sectors that:

(a) are about goods (such as products) or services; and

(b) do not relate to any identifiable, or reasonably identifiable, CDR Consumers; and

9.3.3 creating more choice and competition, or otherwise promoting the public interest, as a result of paragraphs 9.3.1 and 9.3.2 above.

9.4 The CDR regime will be implemented via a framework that consists of:

9.4.1 legislation (the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (**CDR Act**)), which makes amendments to the *Competition and Consumer Act 2010* (Cth) (**CC Act**), the *Privacy Act 1988* (Cth) (**Privacy Act**) and the *Australian Information Commissioner Act 2010* (Cth) (**Information Commissioner Act**);

9.4.2 Rules made under the CDR Act, which will be developed and administered by the Australian Competition and Consumer Commission (**ACCC**);

9.4.3 Data Standards to be made under the Rules, pursuant to section 56FA in the CDR Act, which will be drafted and administered by the Chair of a new Data Standards Body;

9.4.4 a "register of accredited persons" (in this PIA report, called the Accreditation Register), with an associated accreditation regime, established in accordance with the CDR Act and the Draft Rules; and

9.4.5 legislative instruments to be made under section 56AC(2) in the CDR Act, which will designate the Sectors of the Australian economy to which the CDR regime will apply.

9.5 Initially, the implementation of the CDR regime will commence in the banking Sector, pursuant to the *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (**Open Banking Designation**). In the initial implementation, information that is designated, and therefore subject to the CDR regime, is limited to the classes or categories of information described in the Open Banking Designation as including:

9.5.1 information about a CDR Consumer to whom a Product is being or has been supplied, that was provided in connection with that person's acquisition or use of the Product, or is otherwise obtained by the Data Holder;

9.5.2 information about the use of the Product by the CDR Consumer; and

9.5.3 information about Products.[11]

9.6 CDR Data includes raw data that falls within the above specified categories and classes of information, and information that is "wholly or partially derived" from that raw data. However, the Open Banking Designation expressly excludes any "materially enhanced information" from information which is about the use of the Product. This is defined as information which was wholly or partly derived through the application of insight or analysis of information about the use of the Product, which renders the information significantly more valuable than the source material. The Open Banking Designation specifies that certain publicly available information (or which is otherwise required to be provided) and other specific information is not "materially enhanced information".[12]

[11] This is a high level summary only – for a more detailed analysis please see **Part E [Fundamental Concepts]**.
[12] Again, for a more detailed analysis, please see **Part E [Fundamental Concepts].**

9.7 The Open Banking Designation does not currently specify any categories or classes of information for which mandatory access is subject to a fee (in accordance with section 56AM in the CDR Act).

9.8 It is also proposed that the initial Data Holders for the CDR regime will be limited to the Westpac Banking Corporation, the National Australia Bank Limited, the Commonwealth Bank of Australia and the Australia and New Zealand Banking Group Limited, but it is intended that certain other entities may choose to participate in the CDR regime as a "voluntarily participating ADI".

9.9 Following the initial implementation of the CDR regime in the banking Sector, the CDR regime will be implemented in a staged manner (as described in Schedule 3 to the Draft Rules) in relation to an expanded range of information and entities in the banking Sector, and then to other specific Sectors, such as the energy and telecommunications Sectors. It is envisaged that the CDR regime will eventually be rolled-out on an economy-wide, Sector by Sector, basis.[13]

10. Background to the development of the CDR regime

10.1 On 20 July 2017, the Australian Government commissioned the Open Banking Review, which sought to recommend the most appropriate model for "open banking" in Australia. It was envisaged that open banking would give CDR Consumers greater access to, and control of, their banking data and, as such, would benefit CDR Consumers in their interactions with their banks.

10.2 On 26 November 2017, the Australian Government (in response to the recommendations of the Productivity Commission's Data Availability and Use inquiry) announced that a CDR regime would be implemented in Australia. It was announced that the Treasurer would be responsible for the development of the CDR regime, with the design of the regime to be informed by the recommendations stemming from the Open Banking Review.

10.3 The Australian Government received the Final Report of the Open Banking Review in December 2017 and released it for comment in February 2018. The Australian Government announced that it was adopting the recommendations in the Final Report (except for some minor aspects regarding the timing for implementation) as part of the 2018-19 Budget.

10.4 The Final Report from the Open Banking Review made 50 recommendations in relation to open banking, including in relation to:

10.4.1 the proposed regulatory framework;

10.4.2 the type of banking data which should be in scope for open banking;

10.4.3 appropriate privacy and security safeguards for CDR Consumers;

10.4.4 appropriate mechanisms for the transfer of CDR Consumer data; and

10.4.5 implementation issues that could arise.

[13] Consumer Data Right booklet, published by the Department on 9 May 2018.

10.5 On 13 February 2019, the *Treasury Laws Amendment (Consumer Data Right) Bill 2019* (**CDR Bill**) was introduced into the House of Representatives. Additionally, the CDR Bill was referred to the Senate's Economics Legislation Committee (**Senate Committee**) for inquiry and report. On 21 March 2019, the Senate Committee published its final report (**Senate Report**). In undertaking its enquiry into the CDR Bill, the Senate Committee:

10.5.1 advertised the inquiry on its website;

10.5.2 invited submissions (noting that it received 31 submissions); and

10.5.3 held public hearings in Melbourne and Sydney.

10.6 Also in March 2019, the Department published an internally drafted privacy impact assessment (which was produced with assistance from an external privacy expert). However, this privacy impact assessment was undertaken before substantial development of the Draft Rules or Draft Data Standards.

10.7 The CDR Bill lapsed on the dissolution of Parliament on 11 April 2019, however it was re-introduced by the Australian Government on 26 July 2019.

10.8 On 30 July 2019, the CDR Bill was passed by the House of Representatives, and on 1 August 2019, it was passed by the Senate. The CDR Bill received royal assent on 12 August 2019, thus becoming the CDR Act.

10.9 On 18 September 2019, the *Treasury Laws Amendment (2019 Measures No. 2) Bill 2019* was introduced into the House of Representatives, requiring the ACCC to make rules in relation to the deletion of CDR Data.[14]

11. The CDR Act

11.1 The CDR Act makes amendments to the CC Act, the Privacy Act and the Information Commissioner Act. These amendments:

11.1.1 set out the roles, functions and powers of the regulatory bodies (being the ACCC, the Office of the Australian Information Commissioner (**OAIC**) and the Data Standards Body);

11.1.2 outline, at a high level, the overarching objectives and principles for the CDR regime;

11.1.3 create a legislative power for the Treasurer to apply the CDR regime to new Sectors; and

11.1.4 enshrine a guaranteed minimum set of privacy protections (as further described in the Draft Rules).

11.2 Importantly, there are also a number of Privacy Safeguards which are established by the CDR Act. These are:

11.2.1 Privacy Safeguard 1 – Open and transparent management of CDR Data;

11.2.2 Privacy Safeguard 2 – Anonymity and pseudonymity;

[14] We note that the *Treasury Laws Amendment (2019 Measures No. 2) Bill 2019* has been, after the "point in time" completion of our PIA, passed by the House of Representatives and the Senate, and on 28 October 2019, it received royal assent, thus becoming the *Treasury Laws Amendment (2019 Measures No. 2) Act 2019*.

11.2.3 Privacy Safeguard 3 – Collecting solicited CDR Data;

11.2.4 Privacy Safeguard 4 – Dealing with unsolicited CDR Data;

11.2.5 Privacy Safeguard 5 – Notifying the collection of CDR Data;

11.2.6 Privacy Safeguard 6 – Use or disclosure of CDR Data;

11.2.7 Privacy Safeguard 7 – Use or disclosure of CDR Data for direct marketing by Accredited Data Recipients;

11.2.8 Privacy Safeguard 8 – Cross-border disclosure of CDR Data by Accredited Data Recipients;

11.2.9 Privacy Safeguard 9 – Adoption or disclosure of government related identifiers;

11.2.10 Privacy Safeguard 10 – Notifying of the disclosure of CDR Data;

11.2.11 Privacy Safeguard 11 – Quality of CDR Data;

11.2.12 Privacy Safeguard 12 – Security of CDR Data; and

11.2.13 Privacy Safeguard 13 – Correction of CDR Data.

11.3 Further detail about these Privacy Safeguards, and their interaction with the APPs in the Privacy Act, is included in **Part F [Analysis of APP Application and Compliance]** of this PIA report.

12. Draft Rules (proposed rules – August 2019)

12.1 The ACCC will be responsible for the development and administration of Rules made in accordance with the CDR Act, that will further set out the rights and obligations of Participants under the CDR regime in any given Sector (e.g. the banking Sector).

12.2 The Draft Rules are designed so that they will apply generally to all Sectors, but with provisions in the Schedules that will apply only in relation to certain classes of Product Data and CDR Data for the different designated Sectors. Schedule 3 to the Draft Rules applies specifically to the banking Sector. Initially, the Draft Rules will apply only in relation to certain Products that are offered by certain Data Holders within the banking Sector. The Draft Rules will then apply to a progressively broader range of Data Holders and Products.

12.3 The Draft Rules must be read in conjunction with:

12.3.1 the CDR Act and in particular, Part IVD in the CDR Act, which sets out the general framework for the CDR regime;

12.3.2 the relevant designation instrument made under section 56AC in the CDR Act (currently the Open Banking Designation);

12.3.3 any guidelines made by the Information Commissioner under section 56EQ in the CDR Act (noting that none have been published as at 23 September 2019);

12.3.4 Data Standards made in accordance with section 56FA in the CDR Act (currently the Draft Data Standards); and

12.3.5 the *Competition and Consumer Regulations 2010* (Cth) (noting that none relating to the CDR regime have been published as at 23 September 2019).

13. Draft Data Standards (July 2019 working draft) [15]

13.1 The Data Standards will be developed and administered by the Chair of the Data Standards Body, in accordance with the CDR Act and the Draft Rules.

13.2 The Data Standards will set out how Data Holders and Accredited Data Recipients within a given Sector must comply with the Draft Rules, and will be Sector-specific. We understand that the intention is that the Data Standards will contain technical standards about:

13.2.1 processes in relation to:

(a) requests for CDR Data; and

(b) authorisations and consents;

13.2.2 the format of CDR Data;

13.2.3 the types (and descriptions of those types) of CDR Data;

13.2.4 the disclosure and security of CDR Data;

13.2.5 the collection, use, accuracy, storage, security and deletion of CDR Data;

13.2.6 requirements for Data Holders and Accredited Data Recipients;

13.2.7 de-identifying CDR Data, including so that it no longer relates to:

(a) an identifiable person; or

(b) a person who is reasonably identifiable;

13.2.8 ancillary or administrative services that need to be provided by CDR Participants to facilitate communications between them; and

13.2.9 any other matters prescribed by the regulations (noting that no regulations have been proposed as at 23 September 2019).

13.3 The Data Standards Body has released various documents, including:

13.3.1 a document described as "the Draft API Standards (July 2019 version)", which is headed "Data Standards" – we understand that, when finalised, this is intended to be the form for the Data Standards made in accordance with the Rules and the CDR Act (so we refer to this document in this PIA as the 'Draft Data Standards');

13.3.2 the Draft Information Security Profile (which is the key technical artefact that defines the security requirements for the CDR regime); and

13.3.3 a draft of the Consumer Experience Guidelines (**CX Guidelines**) (we understand that these are currently not themselves intended to be legally binding except to the extent that the relevant requirements are incorporated into the Data Standards and Draft Rules – we understand that the process of determining whether any items within this document should be included within the Draft Rules, or be elevated to become Data Standards rather than guidance material, will continue).

[15] As described in footnote 5 above, we are aware that a new version of the Draft Data Standards has subsequently been published (version 1.0.0), but this was published after the "point in time" established for the conduct of this PIA. Accordingly, this PIA does not consider version 1.0.0 of the Draft Data Standards.

13.4 The latest drafts of these documents reflect recent policy decisions that have been taken about the initial implementation of the CDR regime, including that:

13.4.1 a single consistent flow for the authorisation process will be adopted, so that CDR Consumers will be provided with a single one time password in order to be redirected from the Accredited Data Recipient's CDR service to the relevant Data Holder in order to provide their authorisation;

13.4.2 if a CDR Consumer wishes to extend the period of their consent to collect and use their CDR Data, a full re-authorisation process will be required; and

13.4.3 the initial implementation of the CDR regime involves a consent process that will allow the CDR Consumer to select, with only some degree of granularity, the categories of CDR Data that will be disclosed to the Accredited Data Recipient (the Draft Data Standards require pre-defined categories which have greater specificity than the categories of information in the Open Banking Designation). Accordingly, a mandatory consent API to achieve greater granularity and other objectives will not be included in the initial Draft Data Standards.

14. Relationships between the participants in the CDR regime

14.1 We have also found it useful to consider the various relationships between the various participants in the CDR regime. We have considered relationships between:

14.1.1 the CDR Consumer and an Accredited Data Recipient (see paragraph 15 of this **Part D**);

14.1.2 the CDR Consumer and a Data Holder (see paragraph 16 of this **Part D**);

14.1.3 the Accredited Data Recipient, the Data Holder, the Accreditation Register, and the ACCC's broader ICT system for the CDR regime (see paragraph 17 of this **Part D**);

14.1.4 the Data Holder and the Accredited Data Recipient (see paragraph 18 of this **Part D**); and

14.1.5 an Accredited Data Recipient and their outsourced service provider (if applicable) (see paragraph 19 of this **Part D**).

14.2 Please note that the above list does not reflect a sequential description of the information flow steps involved – see **Part G [Analysis of Risks Associated with Information Flows in the CDR Regime]** of this PIA report.

14.3 We have discussed each of these relationships, and associated information flow categories, in further detail in the paragraphs below.

15. Information flows between the CDR Consumer and an Accredited Data Recipient

Summary

15.1 Once the CDR regime is implemented, eligible CDR Consumers will be able to request Accredited Data Recipients to make consumer data requests to a Data Holder, to disclose the CDR Consumer's CDR Data to the Accredited Data Recipient. This is so that the Accredited Data Recipient can provide goods and services to the CDR Consumer (where the Accredited Data Recipient needs to access that CDR Data in order to provide those goods and services).[16] The consumer data request may be for "required consumer data" or "voluntary consumer data", or both.

15.2 For the banking Sector, a CDR Consumer is "eligible" if:

15.2.1 the CDR Consumer is 18 years of age or older (if the CDR Consumer is an individual); and

15.2.2 the CDR Consumer has an account with the Data Holder that is open and can be accessed online (such as by using an internet browser or a mobile phone application).

15.3 The CDR Consumer must provide the Accredited Data Recipient with their consent to:

15.3.1 collect their CDR Data from the Data Holder; and

15.3.2 use their CDR Data for specific purposes once it is received.[17]

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

15.5 The CDR Consumer must be provided with certain information under the CDR Act and the Draft Rules, including certain information if the Accredited Data Recipient will disclose the CDR Consumer's CDR Data to an outsourced service provider (for the provision of goods or services to the Accredited Data Recipient by that outsourced service provider).

15.6 Accredited Data Recipients must provide the CDR Consumer with an online service (i.e. the Consumer Dashboard) in order to manage their requests to collect CDR Data from Data Holders and the associated consents to collect and use their CDR Data. It is not intended that the Consumer Dashboard will be used for the CDR Consumer to request the Accredited Data Recipient to provide goods or services, or to provide required consents, it is rather a mechanism which allows the CDR Consumer to see and manage the consumer data requests which have been made and the consents which they have given. The Accredited Data Recipient will verify the identity of the CDR Consumer when the CDR Consumer accesses the Consumer Dashboard.

[16] We note that general references to 'CDR Consumers' in this PIA report are intended to refer to "eligible CDR Consumers" unless specified otherwise.
[17] As further explained in the CX Guidelines, consents to both collect, and to use, CDR Data will be obtained at the same time.

When can an Accredited Data Recipient make a request to a Data Holder?

15.7 A request may only be made to the Data Holder if the CDR Consumer has given the Accredited Data Recipient a valid request.

15.8 In giving their consents, the CDR Consumer gives the Accredited Data Recipient a valid request to collect that CDR Data from the Data Holder. Upon receipt of a valid request, so long as the request has not ceased to be valid (i.e. it has not expired or been withdrawn) and the consents provided by the CDR Consumer are current,[18] the Accredited Data Recipient may request the Data Holder to disclose some or all of the CDR Data to the Accredited Data Recipient, noting that:

15.8.1 the CDR Data disclosed must be the subject of the relevant consent to collect CDR Data; and

15.8.2 the Accredited Data Recipient must be able to collect this CDR Data in accordance with the data minimisation principle.

Is there a limit on what CDR Data can be collected?

15.9 An Accredited Data Recipient is only able to collect and use CDR Data in accordance with the "data minimisation principle". An Accredited Data Recipient will comply with the data minimisation principle if:

15.9.1 when making requests to a Data Holder on behalf of a CDR Consumer, the Accredited Data Recipient does not collect more CDR Data than is reasonably needed, or CDR Data that relates to a longer time period than is reasonably required, in order to provide goods or services requested by the CDR Consumer; and

15.9.2 when using CDR Data that is collected under such requests, the Accredited Data Recipient does not use the CDR Data beyond what is reasonably needed in order to provide the requested goods or services.[19]

How is consent obtained and recorded?

15.10 As discussed above, the consent will be provided using the Accredited Data Recipient's systems, and will be recorded on the Consumer Dashboard provided by the Accredited Data Recipient for the relevant CDR Consumer.

15.11 In the initial implementation of the CDR regime, the CDR regime will contain restrictions on what an Accredited Data Recipient can ask a CDR Consumer to consent to in relation to the use or disclosure of their CDR Data. These restrictions include:

15.11.1 the Accredited Data Recipient selling the CDR Data it receives under the CDR regime (unless de-identified in accordance with the CDR Data de-identification process[20]); and

15.11.2 the Accredited Data Recipient aggregating CDR Data for the purposes of identifying, compiling insights in relation to, or building a profile in relation to, any person who is not the CDR Consumer who made the consumer data request.

[18] In the Draft Rules, "current" means that the consent or authorisation has not expired.
[19] See Rule 1.8 (for the definition), Rule 4.4, Rule 4.12 and Rule 7.5.
[20] The CDR Data de-identification process can be found in Rule 1.17.

15.12 We note that the restriction provided for in paragraph 15.11.2 above does not apply in relation to a person whose identity is readily apparent from the CDR Data, if the Accredited Data Recipient is seeking consent to:

15.12.1 derive, from that CDR Data, CDR Data about that person's interactions with the CDR Consumer; and

15.12.2 use that derived CDR Data in order to provide the requested goods or services.

15.13 We understand that consumer research and other work has been undertaken to further develop guidance. The Draft Rules require an Accredited Data Recipient to have regard to any "consumer experience guidelines", which include that an Accredited Data Recipient's processes for asking a CDR Consumer to give consent must be as easy to understand as practicable, including by use of concise language and, where appropriate, visual aids.

15.14 Importantly, there is no mechanism in the CDR regime for the CDR Consumer's consent to be implied (i.e. express consent is required). Further, the CDR regime means that consent cannot be obtained from any CDR Consumer on an "opt-out" basis, nor by the use of "pre-selected options".

15.15 Further, an Accredited Data Recipient must give the CDR Consumer a CDR receipt after the CDR Consumer consents to the Accredited Data Recipient collecting and using CDR Data, or the CDR Consumer withdraws their consent. A CDR receipt must include:

15.15.1 the details that relate to the consent;

15.15.2 the name of each Data Holder the CDR Consumer has consented to the collection of CDR Data from; and

15.15.3 any other information the Accredited Data Recipient provided to the CDR Consumer when obtaining the consent.

15.16 If the CDR receipt relates to the withdrawal of a CDR Consumer's consent, the CDR receipt must state when the consent expired. Further, a CDR receipt must be given in writing and in a form other than through the CDR Consumer's Consumer Dashboard (we note however, that a copy of the CDR receipt may also be included in the CDR Consumer's Consumer Dashboard).

Are there requirements for Consumer Dashboards?

15.17 The Draft Rules contain certain minimum requirements for Consumer Dashboards (provided by either Accredited Data Recipients or Data Holders). The Accredited Data Recipient's Consumer Dashboard must have a functionality that:

15.17.1 allows a CDR Consumer, at any time, to withdraw their consent to collect and use CDR Data and elect that redundant data be deleted in accordance with the Draft Rules (with an ability to withdraw such an election);

15.17.2 is simple and straightforward to use; and

15.17.3 is prominently displayed.

15.18 The Consumer Dashboard must also contain the following details in relation to each consent to collect and use CDR Data given by the CDR Consumer:

15.18.1 the CDR Data to which the consent relates;

15.18.2 details of the specific use or uses for which the CDR Consumer has given their consent;

15.18.3 when the consent was given, noting that this can be given for:

(a) a single instance; or

(b) a period of time (which cannot exceed 12 months);

15.18.4 if the consent was given for a period of time:

(a) what that period of time is; and

(b) how often CDR Data has been, and is expected to be, collected over that period; and

15.18.5 the date of expiry of the consent.

15.19 Additionally, if an Accredited Data Recipient receives a consent to collect or use CDR Data, or if the consent expires, the Accredited Data Recipient must update the Consumer Dashboard as soon as practicable.

15.20 Further, the Accredited Data Recipient must notify the CDR Consumer that their consent to collect and use particular CDR Data is current, if 90 days have elapsed since:

15.20.1 the CDR Consumer consented to the collection and use of the CDR Data;

15.20.2 the CDR Consumer last used their Consumer Dashboard; or

15.20.3 the Accredited Data Recipient last sent the CDR Consumer a notification in accordance with this paragraph 15.20.

15.21 This notification must be given in writing and in a form other than through the CDR Consumer's Consumer Dashboard (we note however, that a copy of the notification may also be included in the CDR Consumer's Consumer Dashboard).

Are there particular requirements for consents?

15.22 An express object of the Draft Rules is to ensure that consents given by CDR Consumers for Accredited Data Recipients to collect and use their CDR Data are:

15.22.1 voluntary;

15.22.2 express;

15.22.3 informed;

15.22.4 specific as to purpose;

15.22.5 time limited; and

15.22.6 easily withdrawn.

15.23 The Draft Rules provide that when an Accredited Data Recipient seeks consent from a CDR Consumer, the Accredited Data Recipient must:

15.23.1 seek consent in accordance with the Draft Data Standards;

15.23.2 having regard to any consumer experience guidelines, be as easy to understand as practicable, including by use of concise language and, where appropriate, visual aids;

15.23.3 not include or refer to other documents so as to reduce comprehensibility; and

15.23.4 not bundle consents with other directions, permissions, consents or agreements.

15.24 Further, the Accredited Data Recipient must:

15.24.1 allow the CDR Consumer to choose the types of CDR Data to be collected and used by enabling the CDR Consumer to actively select which particular types of CDR Data the CDR Consumer is consenting to the Accredited Data Recipient collecting, and the specific uses of that CDR Data;

15.24.2 allow the CDR Consumer to choose the period over which the CDR Data will be collected and used by enabling the CDR Consumer to actively select whether the CDR Data would be collected on a single occasion and used over a specified period of time, or collected and used over a specified period of time;

15.24.3 ask for the CDR Consumer's express consent for the Accredited Data Recipient to collect the specified CDR Data, to use the collected CDR Data, and to undertake any direct marketing;

15.24.4 if the request covers voluntary consumer data and the Data Holder charges a fee for disclosure (and intends to pass this fee onto the CDR Consumer):

(a) clearly distinguish between the required consumer data and voluntary consumer data; and

(b) allow the CDR Consumer to actively select whether to consent to the collection of that CDR Data; and

15.24.5 allow the CDR Consumer to make an election in relation to deletion of redundant data.

15.25 Additionally, the Accredited Data Recipient must give the CDR Consumer the following range of information:

15.25.1 its name;

15.25.2 its accreditation number;

15.25.3 how the collection and use of CDR Data indicated in paragraph 15.24 above complies with the data minimisation principle;

15.25.4 the amount of the fee and the consequences if the CDR Consumer does not consent to the collection of that CDR Data if the request covers voluntary consumer data, the Data Holder charges a fee for disclosure and the Accredited Data Recipient is intending to pass that fee onto the CDR Consumer;

15.25.5 information relating to de-identification as specified in the Draft Rules if the Accredited Data Recipient is asking for the CDR Consumer's consent to de-identify

some or all of the collected CDR Data for the purposes of disclosing (including by selling) the de-identified data;

15.25.6 if the CDR Data may be disclosed to an outsourced service provider (including one that is based overseas), the CDR Consumer must also be provided with:

(a) a statement of that fact;

(b) a link to the Accredited Data Recipient's CDR Policy; and

(c) a statement noting that the CDR Consumer can obtain further information about such disclosure from the CDR Policy, if required;

15.25.7 instructions for how the consent can be withdrawn, including a statement that provides that, at any time, the consent can be withdrawn, and any consequences (if any) to the CDR Consumer if they withdraw their consent; and

15.25.8 information about redundant data, including:

(a) a statement regarding the Accredited Data Recipient's intended treatment of redundant data;

(b) a statement outlining the CDR Consumer's right to elect that their redundant data be deleted; and

(c) instructions for how the election can be made.

Can CDR Consumers withdraw their consent?

15.26 A CDR Consumer may withdraw their consent at any time.

15.27 If the CDR Consumer notifies the Accredited Data Recipient in writing of the withdrawal of their consent, the Accredited Data Recipient must give effect to the withdrawal within 2 business days after receiving the communication and notify the Data Holder of this withdrawal in accordance with the Draft Data Standards.

15.28 If the CDR Consumer notifies the Accredited Data Recipient by using the Accredited Data Recipient's Consumer Dashboard, the Accredited Data Recipient must notify the Data Holder of this withdrawal in accordance with the Draft Data Standards.

15.29 Withdrawal of consent does not affect the ability of the CDR Consumer to elect, in accordance with the Draft Rules, that their collected CDR Data be deleted once it becomes redundant.

When do consents expire?

15.30 Consents in relation to CDR Data expire at the earliest of the following:

15.30.1 if consent was withdrawn by communicating the withdrawal to the Accredited Data Recipient in writing, the earlier of when the Accredited Data Recipient gave effect to the withdrawal or 2 business days after the Accredited Data Recipient received the written communication;

15.30.2 if consent was withdrawn using the Accredited Data Recipient's Consumer Dashboard, when consent was withdrawn;

15.30.3 when the Accredited Data Recipient is notified under the Draft Rules of the withdrawal of the authorisation for the Data Holder to disclose that CDR Data;

15.30.4 the end of the period of 12 months after the consent was given (or the end of any shorter period for the term of their consent which is specified by the CDR Consumer);

15.30.5 if the consent was for the collection of that CDR Data on one occasion, after the CDR Data has been collected; or

15.30.6 if the consent was for the collection of that CDR Data over a specified period of time, the end of that period of time.

15.31 If an Accredited Data Recipient's accreditation is revoked or surrendered in accordance with the Draft Rules, all consents for the Accredited Data Recipient to collect and use CDR Data expire when the revocation or surrender takes effect.

Can consent be varied?

15.32 In the initial implementation of the CDR regime, it is not possible for a CDR Consumer to vary their consent. If a CDR Consumer wishes to vary their consent, they must first withdraw their consent (as specified above at paragraphs 15.26 to 15.29). The CDR Consumer can then re-provide the Accredited Data Recipient with a new consent.

When can an Accredited Data Recipient use or disclose CDR Data?

15.33 In accordance with the Draft Rules, CDR Data can be used or disclosed if it is a permitted use or disclosure. A permitted use or disclosure includes:

15.33.1 using the CDR Consumer's CDR Data to provide goods or services requested by the CDR Consumer (in accordance with the data minimisation principle and the CDR Consumer's current consent);

15.33.2 directly or indirectly deriving CDR Data from the collected CDR Data for that purpose;

15.33.3 disclosing, to the CDR Consumer, any of their CDR Data;

15.33.4 disclosing the CDR Consumer's CDR Data to an outsourced service provider for the purposes of doing things specified in paragraphs 22.19.2(a) to 22.19.2(c) above, and to the extent reasonably needed to do those things; and

15.33.5 disclosing (by sale or otherwise), to any person, CDR Data that has been de-identified in accordance with the CDR Data de-identification process.

When must CDR Data be de-identified or deleted?

15.34 CDR Data becomes redundant data when the Accredited Data Recipient no longer needs any of that CDR Data for the purpose permitted under the Draft Rules or the purpose for which the Accredited Data Recipient is able to use or disclose it in accordance with the CDR Act.

15.35 Accredited Data Recipients must de-identify or delete that redundant data in accordance with the CDR Data de-identification process and the CDR Data deletion process provided for in the Draft Rules.[21]

[21] The Draft Rules provide further detail and information in relation to the treatment of redundant data, and the processes for de-identification and deletion under the CDR regime.

15.36 Under the Draft Rules, an Accredited Data Recipient must tell a CDR Consumer whether it has a general policy of:

15.36.1 deleting redundant data;

15.36.2 de-identifying redundant data; or

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

15.37 The effect of the CDR legislative framework is that in certain circumstances, Accredited Data Recipients must delete CDR Data. Depending on the situation, this may include when:

15.37.1 in accordance with the CDR Data de-identification process, an Accredited Data Recipient cannot de-identify CDR Data that becomes redundant; and

15.37.2 a CDR Consumer has elected for their CDR Data, when it becomes redundant, to be deleted.

15.38 Further, if an Accredited Data Recipient has provided any of its outsourced service providers with the redundant data, the outsourced service provider must return the redundant data to the Accredited Data Recipient or delete the redundant data (and notify the Accredited Data Recipient of the deletion).

15.39 De-identification must be undertaken in accordance with the process in the Draft Rules, including the *De-identification Decision-Making Framework,* published by the OAIC and Data61.[22]

15.40 We note that if an Accredited Data Recipient wants to de-identify a CDR Consumer's CDR Data for the purposes of disclosing (including by selling) the de-identified data, it must:

15.40.1 obtain the CDR Consumer's consent to do so; and

15.40.2 provide the CDR Consumer with additional information about the process for de-identification, proposed disclosures, and that the CDR Consumer would not be able to elect to have their de-identified data deleted once it becomes redundant data (as discussed in paragraphs 15.41 and 15.42 below).

Can a CDR Consumer elect for their redundant data to be deleted?

15.41 A CDR Consumer who gave a consent to collect and use particular CDR Data may elect that the collected CDR Data, and any data derived from it, be deleted when it becomes redundant data, at the time of giving consent to the collection and use of the CDR Data or at any other time before the consent expires.

15.42 The CDR Consumer may make the election to delete the redundant data by communicating it to the Accredited Data Recipient in writing or by using the Accredited Data Recipient's Consumer Dashboard. We note that this does not apply if the Accredited Data Recipient informed the CDR Consumer when it obtained consent to collect and use CDR Data that it has a general policy of deleting CDR Data when it becomes redundant data.[23]

[22] The *De-identification Decision-Making Framework* is available at https://www.oaic.gov.au/privacy/guidance-and-advice/de-identification-decision-making-framework/.
[23] We note that the Draft Rules provide that if the derived CDR Data was de-identified in accordance with the CDR Data de-identification process before the collected CDR Data from which it was derived became redundant, it does not need to be deleted.

16. Information flows between the CDR Consumer and a Data Holder

Summary

16.1 The Data Holder will hold information about the CDR Consumer (the information may be held by the Data Holder themselves, or a third party on behalf of the Data Holder). This information may include CDR Data and non-CDR Data, and may be personal information or non-personal information. The information may have been provided to the Data Holder by the CDR Consumer, or otherwise collected or generated by the Data Holder.

16.2 The Data Holder must, in accordance with the Draft Rules, provide an online service that can be used by CDR Consumers to make requests for their CDR Data directly to the Data Holder (direct request service) and an online service that can be used by Accredited Data Recipients to make requests for CDR Data on behalf of CDR Consumers to the Data Holder (accredited person request service).

16.3 The CDR Consumer may use the direct request service to request that the Data Holder disclose their CDR Data directly to themselves. The Data Holder must then provide the requested CDR Data to the CDR Consumer (in human-readable form), unless the Data Holder refuses to disclose the CDR Data as permitted by the Draft Rules. These circumstances are those where the Data Holder considers the refusal to be necessary to prevent physical or financial harm or abuse, or as otherwise specified in the Draft Data Standards.

16.4 Alternatively, the CDR Consumer may have requested that an Accredited Data Recipient collect their CDR Data from the Data Holder (in accordance with the processes described in paragraph 15 of this **Part D [Project Description]**). Upon providing their consents to collect and use the CDR Data, the CDR Consumer will be redirected (in accordance with the single one time password process discussed in paragraph 13.4.1 of this **Part D [Project Description]**) to the Data Holder. The Data Holder will undertake their usual authentication processes to establish the identity of the CDR Consumer at this point (e.g., the CDR Consumer will enter their usual banking username and password, or other credentials).

16.5 The CDR Consumer must then authorise the Data Holder to disclose their CDR Data to the Accredited Data Recipient (using the Data Holder's systems).

16.6 Data Holders must also provide a Consumer Dashboard to allow CDR Consumers to manage their authorisation under the CDR regime (again, authorisation is not undertaken through the Consumer Dashboard, but the Consumer Dashboard will allow the CDR Consumer to see their current authorisations and to manage them, including by withdrawing an authorisation as required). The Data Holder will also verify the identity of the CDR Consumer when the CDR Consumer accesses the Consumer Dashboard, using their usual authentication processes. If a CDR Consumer withdraws their authorisation under the CDR regime, the Data Holder must notify the Accredited Data Recipient of this withdrawal of authorisation.

16.7 Further, the Data Holder's Consumer Dashboard must have a function that:

16.7.1 allows for withdrawal of authorisations to disclose CDR Data at any time;

16.7.2 is simple and straightforward to use;

16.7.3 is no more complicated to use than the process for giving the authorisation to disclose the CDR Data;

16.7.4 is prominently displayed; and

16.7.5 as part of the process for withdrawing authorisation, displays a message relating to the consequences of the withdrawal in accordance with the Data Standards.

Request by CDR Consumer for direct provision of CDR Data

16.8 CDR Consumers will be able to use the Data Holder's direct request service, to request the Data Holder disclose their CDR Data directly to the CDR Consumer.

16.9 Unless an exception specified in the Draft Rules applies, the Data Holder must disclose the requested CDR Data to the CDR Consumer.

Request by Accredited Data Recipient on behalf of the CDR Consumer

16.10 If an Accredited Data Recipient makes a request on behalf of a CDR Consumer, there is no current authorisation for the Data Holder to disclose the requested CDR Data and the Data Holder reasonably believes that the request was made by an Accredited Data Recipient on behalf of an eligible CDR Consumer, the Data Holder must ask the CDR Consumer to authorise the disclosure of the requested CDR Data to the Accredited Data Recipient. This must be done in accordance with the Division 4.4 of the Draft Rules (Authorisations to disclose CDR Data) and the Draft Data Standards.

16.11 The Draft Rules contain similar requirements in relation to authorisations to those for the consent process described in paragraph 15 above, including the requirements for:

16.11.1 the Data Holder's Consumer Dashboard;

16.11.2 the obtaining of the authorisation; and

16.11.3 the withdrawal and expiry of authorisations.

Can a Data Holder refuse to disclose CDR Data?

16.12 For completeness, a Data Holder may refuse to disclose CDR Data in response to a valid request if the Data Holder:

16.12.1 considers it necessary in order to prevent physical or financial harm or abuse; or

16.12.2 has reasonable grounds to believe that disclosure of some or all of that CDR Data would adversely impact the security, integrity or stability of the Accreditation Register or the Data Holder's information and communication technology systems.

16.13 The Data Holder may also refuse to disclose CDR Data in response to a valid request in circumstances set out in the Draft Data Standards.

16.14 If the Data Holder decides to refuse a valid request in accordance with the Draft Data Standards, the Data Holder must inform the Accredited Data Recipient. Additionally, a Data Holder may refuse a request in the circumstances set out in the Draft Data Standards. The Draft Data Standards provide for refusal to be given in certain circumstances, including during periods of time when the digital channels for the Data Holder are the target for a distributed denial of service or equivalent form of attack, or there is a significant increase in traffic from a poorly designed or misbehaving Accredited Data Recipient.

Joint banking Products

16.15 Under the Draft Rules, there are special requirements for joint bank account holders. These will mean that Data Holders must provide an ability for all joint account holders to jointly elect that each joint account holder will individually be able to make consumer data requests, give authorisations to disclose CDR Data and revoke those authorisations. However, each individual joint account holder must be able to individually revoke such an election.

16.16 If a Data Holder considers it necessary in order to prevent physical or financial harm or abuse, it is not required to update the Consumer Dashboard of a joint account holder, following disclosure of CDR Data in response to a consumer data request made by the other joint account holder.

17. Information flows involving the ACCC's broader ICT system for the CDR regime (including the Accreditation Register)

Summary

17.1 The Data Holder and Accredited Data Recipient will need to verify the identity and/or accreditation status of the other party before collecting or disclosing CDR Data. They will also need to obtain the necessary technical information to make the relevant request and/or provide or receive the requested CDR Data.

17.2 The Draft Rules provide that a database containing a list of Data Holders will form part of the Accreditation Register. This database will contain information about each Data Holder, including each brand name under which the Data Holder offers products and a hyperlink to the relevant web site address of the Data Holder and to their CDR Policy. We understand that Data Holders will also be required to undertake a process of testing to ensuring that their ICT systems include a direct request service and an accredited person request service, and will allow the transfer of CDR Data to Accredited Data Recipients, in accordance with the requirements of the Draft Rules and Draft Data Standards.[24]

17.3 The Accreditation Register will also hold information about Accredited Data Recipients who have completed the accreditation process. We understand that applicants seeking accreditation will need to undergo a process of testing to ensuring that their ICT systems will allow the making of requests to Data Holders, and for the receipt of CDR Data from Data Holders, in accordance with the requirements of the Draft Rules and Draft Data Standards.

17.4 Before an Accredited Data Recipient makes a request for the provision of CDR Data by a Data Holder, the Accredited Data Recipient will electronically obtain the technical information required to enable the Accredited Data Recipient to make that request from the ACCC's broader ICT system for the CDR regime. [25]

17.5 Before disclosing any CDR Data to an Accredited Data Recipient, the Data Holder will electronically confirm with the Accreditation Register that the Accredited Data Recipient is accredited, and obtain the necessary technical information from the Accreditation Register required to make the transfer of authorised CDR Data.[26]

[24] We note that the current version of the Draft Rules is silent about any requirements for testing for conformance with the Draft Rules and Draft Data Standards.
[25] We understand that, technically, the Accredited Data Recipient obtains information from the ACCC's broader ICT system for the CDR regime which enables it to register its software product with the Data Holder, and it is this registration that will subsequently allow the transfer of requests and CDR Data.
[26] As discussed in footnote 25 above, we understand that, technically, this occurs during the registration of the Accredited Data Recipient's software product.

17.6 All transactions between the Accreditation Register and/or the ACCC's broader ICT system for the CDR regime, will be made in a manner consistent with the Draft Rules and the technical requirements in the Draft Data Standards.[27]

What is the Accreditation Register?

17.7 The ACCC is currently developing the Accreditation Register as part of a broader specialist ICT system to implement the CDR regime, with the assistance of a third party contractor. The Accreditation Register is being developed using an agile methodology in anticipation of the commencement of the CDR regime, but as at 23 September 2019 the detailed design of the Register has not been finalised. The relevant contract contains provisions designed to ensure that the Register (and the contractor) complies with all legislative requirements of the CDR regime, including its privacy and security requirements.

17.8 We also understand that the ACCC is currently undertaking further work to determine the necessary requirements for:

17.8.1 the Accreditation Register API to be included in the Data Standards (i.e., the API that will allow CDR Participants to find the details of registered Data Holders and Accredited Data Recipients);

17.8.2 the business and technical design principles;

17.8.3 the security profile and certificate management aspects for access to the CDR ICT system (and the Accreditation Register); and

17.8.4 the caching and refreshing of metadata in the Accreditation Register.

17.9 The design of the Accreditation Register and the ACCC's broader ICT system for the CDR regime will also be relevant to its security and operation. For example, we understand that the Accreditation Register will undertake a process of authentication using a private key which can be verified by a Data Holder using a published public key, and that communication will also be transport encrypted.

How does an entity or person become an Accredited Data Recipient?

17.10 To become an "accredited person" under the CDR regime, an applicant must apply to the Data Recipient Accreditor, and provide all information stipulated under the Draft Rules. While an application may contain personal information (and be regulated by the Privacy Act), no CDR Data will be collected by the Data Recipient Accreditor. The Data Recipient Accreditor will consider the application in accordance with the accreditation criteria specified in the Draft Rules.

17.11 The Data Recipient Accreditor may, in processing an application:

17.11.1 request further information from the applicant;

17.11.2 consult with other Commonwealth, State or Territory authorities, including (but not limited to):

(a) the Information Commissioner;

(b) the Australian Securities and Investment Commission (**ASIC**);

(c) the Australian Prudential Regulation Authority (**APRA**); and

[27] We also note that the design of the ACCC's broader ICT system for the CDR regime may also be relevant (e.g. protocols governing calls *to* the system will be defined by the design of the system, but protocols governing calls *from* the system to the Data Holder will be in the Data Standards).

(d) the Australian Financial Complaints Authority (**AFCA**);

17.11.3 consult with similar authorities in foreign jurisdictions; and

17.11.4 interview the applicant.

17.12 Once a decision has been made in relation to the application, the Data Recipient Accreditor must:

17.12.1 if it decides to accredit the applicant, give the applicant a unique number by which it may be identified as an Accredited Data Recipient (i.e. their accreditation number); and

17.12.2 notify the applicant of the outcome, and provide the information prescribed under the Draft Rules.

17.13 An accreditation takes effect when the fact that the Data Recipient Accreditor has decided to accredit the applicant is included in the Accreditation Register.

17.14 At the time of accreditation, or at any time after accreditation, the Data Recipient Accreditor may impose conditions on the accreditation (which can be varied or removed at any time). However, before imposing or varying a condition, the Data Recipient Accreditor must inform the applicant or Accredited Data Recipient of the proposed imposition or variation of the condition/s and give them a reasonable opportunity to be heard in relation to the proposed condition (unless an exception in the Draft Rules applies).

Are there any obligations that apply to Accredited Data Recipients?

17.15 In the initial implementation of the CDR regime, there will only be a single level of accreditation, meaning that an Accredited Data Recipient must, in accordance with the Draft Rules, be accredited at the "unrestricted" level.

17.16 Accredited Data Recipients at the "unrestricted" level must meet a number of obligations, including that they must continue to:

17.16.1 be a fit and proper person to manage CDR Data;

17.16.2 protect the CDR Data from misuse, interference and loss, and unauthorised access, modification or disclosure by implementing particular requirements set out in Schedule 2 to the Draft Rules;

17.16.3 have internal dispute resolution processes that meet particular requirements;

17.16.4 be a member of a recognised external dispute resolution scheme in relation to CDR Consumer complaints (which we understand will initially be the AFCA for the banking Sector)[28];

17.16.5 have adequate insurance, or a comparable guarantee (although this will not apply for the initial implementation of the CDR regime in respect of Accredited Data Recipients who are authorised deposit-taking institutions (**ADIs**)); and

17.16.6 have an address for service (noting that if the Accredited Data Recipient is a foreign entity, it must have a local agent that has an address for service).

[28] We understand that, since the "point in time" established for the conduct of this PIA, under the *Competition and Consumer (External Dispute Resolution Scheme-Banking Sector) Instrument 2019*, AFCA has been recognised as the external dispute resolution scheme for the banking Sector, in accordance with section 56DA(1) in the CDR Act.

17.17 Further, Accredited Data Recipients must comply with the conditions of their accreditation. Schedule 1 to the Draft Rules require Accredited Data Recipients to comply with the default conditions on their accreditation, which includes provision of an attestation statement and an assurance report in accordance with the Draft Rules.

17.18 Additionally, there are a number of notification requirements that an Accredited Data Recipient must comply with. For example, an Accredited Data Recipient must notify the Data Recipient Accreditor within 5 business days of:

17.18.1 any material change in circumstances that could affect the Accredited Data Recipient's ability to comply with any of its obligations;

17.18.2 any matter that could be relevant to a decision as to whether the Accredited Data Recipient is a fit and proper person to manage CDR Data; and

17.18.3 a change to, or the Accredited Data Recipient becomes aware of an error in, any of the information provided to the Data Recipient Accreditor to be entered into the Accreditation Register.

17.19 The Data Recipient Accreditor must notify the Accreditation Registrar of any accreditation, change to a condition on an accreditation, surrender, suspension or revocation of an accreditation or if the Accredited Data Recipient has notified the Data Recipient Accreditor of a matter specified in paragraph 17.18.3 above.

17.20 In accordance with the Draft Rules, an accreditation cannot be transferred.

17.21 We note that Accredited Data Recipients will be bound both by the CDR regime in respect of CDR Data, and the obligations of an APP entity under the Privacy Act in respect of any non-CDR Data that is personal information (if the Accredited Data Recipient is an APP entity).

17.22 The CDR Act will insert a new subsection 6E(1)(d) into the Privacy Act. The effect of this new subsection will be that while a small business operator is accredited as an Accredited Data Recipient, it will be treated as an APP entity in respect of all personal information that is not CDR Data. This means that the APPs will apply to that personal information held by the Accredited Data Recipient.

Can an Accredited Data Recipient's accreditation end?

17.23 An Accredited Data Recipient's accreditation can be revoked, suspended or surrendered.[29] There are a number of grounds for revocation, suspension or surrender, as set out in the Draft Rules. These include if the Data Recipient Accreditor is no longer satisfied that the Accredited Data Recipient is a fit and proper person to manage CDR Data or the Accredited Data Recipient has contravened a range of relevant laws or data standards.

What happens if an Accredited Data Recipient's accreditation is suspended, revoked or surrendered?

17.24 If an Accredited Data Recipient's accreditation is suspended, revoked or surrendered, the Accredited Data Recipient must:

17.24.1 if the accreditation has been suspended:

(a) comply with its obligations as an Accredited Data Recipient; and

(b) not collect any further CDR Data;

[29] The Draft Rules are silent as to whether accreditation is granted only for a specific period of time. Accordingly, under the current version of the Draft Rules, accreditation will continue indefinitely, until it is revoked or surrendered.

17.24.2 if the accreditation has been revoked or surrendered:

(a) comply with Privacy Safeguards 6, 7 and 12 as if it were still an Accredited Data Recipient;

(b) not further collect, use or disclose any CDR Data; and

(c) delete or de-identify any CDR Data that it holds, unless it is required to retain the CDR Data by or under an Australian law or a court/tribunal order, or it relates to any current or anticipated legal proceedings or dispute resolution proceedings to which the Accredited Data Recipient is a party; and

17.24.3 if it has collected CDR Data, notify each CDR Consumer who has provided their consent to the Accredited Data Recipient's collection of their CDR Data that:

(a) their accreditation has been suspended, revoked or surrendered; and

(b) if the accreditation has been suspended, any consents to collect and to use CDR Data may be withdrawn by the CDR Consumer at any time and the effect of any withdrawal.

18. Information flows between the Data Holder and the Accredited Data Recipient

Summary

18.1 If a CDR Consumer consents to the Accredited Data Recipient collecting and using their CDR Data, and also authorises the Data Holder to disclose the relevant CDR Data, the Data Holder must transfer the requested CDR Data to the Accredited Data Recipient.

18.2 CDR Data disclosed by the Data Holder to the Accredited Data Recipient must be disclosed in machine-readable form, and the transfer must occur in accordance with the Draft Data Standards (which include a number of minimum requirements, including in relation to security).

18.3 Accredited Data Recipients will collect that CDR Data from the Data Holder in accordance with the consent provided by the CDR Consumer to collect that CDR Data, and may then use and disclose the collected CDR Data, but only in accordance with the consent to use it provided by the CDR Consumer.

19. Information flows between Accredited Data Recipients and their outsourced service providers

Summary

19.1 An Accredited Data Recipient may disclose the CDR Consumer's CDR Data to an outsourced service provider. An Accredited Data Recipient must disclose CDR Data in accordance with its CDR outsourcing arrangement, which must meet the requirements for such an arrangement as provided for in the Draft Rules.[30]

19.2 Any use or disclosure in accordance of that CDR Data by an outsourced service provider (whether or not in accordance with the CDR outsourcing arrangement) is taken to have been by the Accredited Data Recipient (irrespective of whether the CDR Data was disclosed to the

[30] This is further discussed in **Part E [Fundamental Concepts]** of this PIA report.

outsourced service provider by the Accredited Data Recipient, or directly through one or more further CDR outsourcing arrangements).

20. Dispute resolution and remedies for breach of the CDR regime

Dispute resolution

20.1 The Draft Rules include a number of dispute resolution provisions.

20.2 For example, the Draft Rules provide that Data Holders and Accredited Data Recipients *'must have internal dispute resolution processes that meet the internal dispute resolution requirements in relation to that sector'*. The Draft Rules state that Data Holders and Accredited Data Recipients in the banking Sector are considered to have met the internal dispute resolution requirements if their internal dispute resolution processes comply with particular provisions of Regulatory Guide 165 (**RG 165**). The Draft Rules set out a list of the provisions of RG 165 that must be complied with,[31] which include the provisions dealing with:

20.2.1 the guiding principles and standards that Data Holders and Accredited Data Recipients must meet in respect of their internal dispute resolution procedures;

20.2.2 the outsourcing of internal dispute resolution procedures;

20.2.3 the manner in which Data Holders and Accredited Data Recipients must acknowledge, respond to, and seek to resolve, complaints, including the relevant timeframes;

20.2.4 the tailoring and development of internal dispute resolution processes;

20.2.5 the documentation of internal-facing dispute resolution procedures; and

20.2.6 the establishment of links between internal dispute resolution and external dispute resolution procedures.

20.3 The Draft Rules also provide that all Data Holders and Accredited Data Recipients must be members of a recognised external dispute resolution scheme in relation to CDR Consumer complaints.

Remedies

20.4 The CDR Act activates a number of powers that can be exercised by the ACCC and the OAIC in their roles as regulators. This includes a number of civil penalty provisions and criminal offences:

20.4.1 Civil penalties will attach to:

(a) misleading or deceptive conduct;

(b) holding out that a person is an "accredited person"; and

(c) breaching particular requirements of the Privacy Safeguards.

20.4.2 Criminal offences, in certain circumstances, will also attach to:

[31] The Draft Rules state that Data Holders and Accredited Data Recipients must comply with RG 165 as if references in RG 165 were references to CDR Consumer complaints, and as if references to financial firms and financial service providers were references to Data Holders and Accredited Data Recipients.

(a) misleading or deceptive conduct; and

(b) holding out that a person is an "accredited person".

20.5 The Draft Rules provide that specified provisions of the Draft Rules are civil penalty provisions (within the meaning set out in the *Regulatory Powers (Standard Provisions) Act 2014* (Cth) (**Regulatory Powers Act**)).[32]

20.6 If a person is suspected of committing a criminal offence, contravenes a civil penalty provision, breaches a Privacy Safeguard, or a cause of action is otherwise identified (e.g. for breach of contract or negligence) (as the case may be):

20.6.1 CDR Consumers may:

(a) make a complaint to the Information Commissioner (complaints will be handled in accordance with Part V (Investigations etc.) of the Privacy Act);

(b) make a report to the ACCC; and/or

(c) commence a civil action for damages; and

20.6.2 the responsible regulators may, dependent on their respective standing and legislative authority, and the nature of the conduct:

(a) institute proceedings for a civil action;

(b) issue an infringement notice for a breach of a civil penalty provision;

(c) conduct an investigation and issue a determination;

(d) consider pursuing criminal charges for a suspected criminal offence;

(e) seek an enforceable undertaking (for example, each provision relating to the Privacy Safeguards is enforceable under Part 6 of the Regulatory Powers Act); and/or

(f) seek an injunction (for example, each provision relating to the Privacy Safeguards is enforceable under Part 8 of the Regulatory Powers Act).

20.7 We understand that the OAIC will be primarily responsible for regulation of compliance with the Privacy Safeguards, and the ACCC will be primarily responsible for any other breaches of the CC Act. The CDR Act enables information sharing between the OAIC and ACCC, which will facilitate joint regulation and cross-referral to the most appropriate body.

20.8 There will be a "no wrong door" approach to complaints, meaning that CDR Consumers can make a report to the ACCC or make a complaint to the OAIC, and the regulators will work together to ensure the issue is considered by the appropriate entity. We understand that the ACCC and the OAIC are developing processes to manage this workflow.

[32] Rule 9.8 sets out a full list of the civil penalty provisions.

Part E Fundamental Concepts

21. Introduction

21.1 The CDR Act, together with its interaction with the Open Banking Designation, the Draft Rules, and the Draft Data Standards, is very complex. We suspect that it may be difficult for some CDR Consumers, Data Holders and Accredited Data Recipients to comprehend.[33]

21.2 In this **Part E [Fundamental Concepts]**, we endeavour to further explain our understanding of some key concepts in the legislative framework, in order to provide further background to our analysis.

22. Further explanation of key concepts

(a) Who is a CDR Consumer?

22.1 Under section 56AI(3) in the CDR Act, a person will be a CDR Consumer for CDR Data, if:

22.1.1 the CDR Data relates to the person (or their associate) because the person was supplied goods or services; and

22.1.2 the CDR Data is held by:

(a) a Data Holder;

(b) an Accredited Data Recipient; or

(c) a person holding it for the Data Holder or Accredited Data Recipient; and

22.1.3 the person is identifiable, or reasonably identifiable, from the CDR Data or from other information which is held by the entity described in paragraph 22.1.2.

22.2 The effect of this definition is that:

22.2.1 a CDR Consumer does not need to be an individual (any "person", which includes corporations and other legal entities, can be a CDR Consumer);[34]

22.2.2 there must be CDR Data (see the discussion below about the meaning of "CDR Data") which must "relate" to the CDR Consumer because of goods or services that have been supplied to them (or their associate);

[33] As mentioned earlier in this PIA report, since our "point in time" analysis, the OAIC published a draft version of its "*Privacy Safeguard Guidelines*", which are designed to assist CDR Participants in understanding how the obligations under the APPs and the Privacy Safeguards operate. While we have not incorporated the contents of these draft guidelines into this document, we note that they provide useful guidance on many of the issues we have discussed in this PIA report. We understand that the OAIC also intends to publish further guidance on the CDR regime designed to assist CDR Consumers in the near future.

[34] Any corporation or other legal entity can be a CDR Consumer - the CDR regime does not have any financial or other threshold test for non-individuals to be a CDR Consumer (this is unlike the test for a "consumer" under some other regimes, such as the CC Act generally).

22.2.3 the CDR Data must be held by a Data Holder, an Accredited Data Recipient, or someone else holding the CDR Data on behalf of the Data Holder or Accredited Data Recipient (see the discussions below about the meaning of "Data Holder" and "Accredited Data Recipient"); and

22.2.4 the CDR Consumer must be able to be identified (either from the CDR Data itself, or through combining the CDR Data with other information held by the same entity that could reasonably re-identify the CDR Data).

(b) Who is an eligible CDR Consumer?

22.3 In accordance with clause 2.1 of Schedule 3 of the Draft Rules, a CDR Consumer is eligible in relation to a particular Data Holder, if:

22.3.1 the CDR Consumer is 18 years of age or older (if the CDR Consumer is an individual); and

22.3.2 the CDR Consumer has an account with the Data Holder that is open and can be accessed online (such as by using an internet browser or a mobile phone application).

(c) When is information CDR Data?

22.4 The effect of the definition of CDR Data (in section 56AI in the CDR Act) and the Open Banking Designation means that for the initial implementation of the CDR regime, information will only be CDR Data if it is:

22.4.1 **about a user of a Product** (see s5(1) and s6 of the Open Banking Designation): Effectively, this is information about the CDR Consumer who has been supplied with a Product (or whose associate has been supplied with a Product). It includes:

(a) information identifying the CDR Consumer or their associate;

(b) information relevant to the eligibility of the CDR Consumer or their associate to acquire or use a Product or a feature of a Product; and

(c) the contact details of the CDR Consumer or their associate;

22.4.2 **information about use of a Product** (see s5(1) and s7 of the Open Banking Designation): This is information about the CDR Consumer's use of the Product (or their associate's use of the Product), which includes:

(a) information identifying an account associated with the Product;

(b) each balance of an account associated with the Product;

(c) information about a transaction made by the CDR Consumer or their associate in connection with the Product; and

(d) information about an authorisation given by the CDR Consumer or their associate in connection with an account associated with the Product, including information about:

(i) who is authorised to use or access, or view information relating to, the account; and

(ii) a third party authorisation to make a payment;

(We note that even if information falls within this category, it will not be within the classes specified in the Open Banking Designation if it is "materially enhanced information" as described in s10 of the Open Banking Designation. This is information about use of a product that has been derived through the application of insight and analysis by or on behalf of the person holding the data, which rendered the information significantly more valuable.

We note that this definition may be somewhat difficult to apply in practice, as it will require Data Holders to make a judgement about whether data which has been manipulated in any way meets this test. Even if it does fall within the definition, Data Holders will also need to consider whether it is likely to be caught as information which is "wholly or partly" derived from other CDR Data for the purposes of section 56AI(1)(b) in the CDR Act.

Accordingly, we have recommended that further guidance be provided in order to further clarify for CDR Consumers and CDR Participants what is, and what is not, materially enhanced information (see **Recommendation 2**)).

22.4.3 **information about a Product** (see s5(1) and s8 of the Open Banking Designation);[35] and

22.4.4 **information which is wholly or partly derived** from any of the information in paragraphs 22.4.1 to 22.4.3 (section 56AI(b) in the CDR Act). Again, we suggest that there may be some difficulty in working out whether particular derived information will be "CDR Data".

22.5 However, even if the information falls within one of these categories, it will not be CDR Data if it is certain credit information which is already regulated under the Privacy Act (see sections 5 and 9 of the Open Banking Designation).

22.6 In addition, information will not be CDR Data for the initial implementation if it was collected before 1 January 2017 (which is the earliest holding day specified in section 5(3) of the Open Banking Designation in accordance with section 56AC(2)(c) in the CDR Act). This means that if the information was collected before 1 January 2017, the information will not be CDR Data and the person who holds it:

22.6.1 will not be a Data Holder of the CDR Data; and

22.6.2 will not be required to disclose it under the Draft Rules.

22.7 A further complication is that, under the Draft Rules applicable to the banking Sector, consumer data requests can be made in relation to "required consumer data" and "voluntary consumer data".[36]

22.8 Under Schedule 3 to the Draft Rules, for the initial implementation, required consumer data is limited to the classes of information in the Open Banking Designation (as specified in paragraph 22.4 above). Further, it must be "customer data", "account data", "transaction data" or "product specific data". Additionally, required consumer data must be held by the Data Holder in digital form. There are also further restrictions on what is considered to be required consumer data in relation to transaction data and account data, as provided for in clause 3.2(4) of Schedule 3 to the Draft Rules. A fee cannot be charged for the disclosure of required consumer data.

[35] As discussed in **Part C [Methodology]**.
[36] Some CDR Data will be neither required consumer data nor voluntary consumer data, as provided for in clause 3.2(3) of Schedule 3 to the Draft Rules.

22.9 A Data Holder may:

22.9.1 in response to a consumer data request made by a CDR Consumer, refuse to disclose required consumer data to that CDR Consumer if it considers it necessary to prevent physical or financial harm or abuse, or in circumstances (if any) set out in the Draft Data Standards. If it does so, the Data Holder must inform the CDR Consumer of the refusal in accordance with the Draft Data Standards; and

22.9.2 in response to a consumer data request made by an Accredited Data Recipient, refuse to disclose, or refuse to ask for an authorisation in relation to, required consumer data to an Accredited Data Recipient if it considers it necessary to prevent physical or financial harm or abuse, or has reasonable grounds to believe that the disclosure would adversely impact the security, integrity or stability of the Accreditation Register, or the Data Holder's information and communication technology systems. If it does so, the Data Holder must inform the Accredited Data Recipient of the refusal in accordance with the Draft Data Standards.

22.10 Voluntary consumer data is CDR Data for which there is a CDR Consumer, and where the CDR Data is not required consumer data. A fee may be charged for the disclosure of voluntary consumer data.

22.11 We note that the application of the above means that it is particularly difficult to determine the scope of the applicable CDR Data.

(d) When is a person a Data Holder?

22.12 For the initial implementation, a person will be a Data Holder (under section 56AJ in the CDR Act) if:

22.12.1 the CDR Data falls within one of the classes of information in the Open Banking Designation (see paragraphs 22.4 to 22.5 of this **Part E [Fundamental Concepts]**), or is "directly or indirectly derived" from the data (as discussed above, the Draft Rules applicable to the banking Sector initially restrict operation of the CDR regime to CDR Data which does not include any wholly or partly derived data);

22.12.2 and either:

(a) the person is an authorised deposit taking institution (as defined in the *Banking Act 1959*) (**ADI**) and:

(i) the person did not receive the CDR Data from anyone under the Draft Rules; or

(ii) the person did not receive other CDR Data under the Draft Rules which it then used to derive the CDR Data (section 56AJ(2) in the CDR Act); or

(b) the person is an Accredited Data Recipient, and it did not receive that CDR Data (or any other CDR Data from which it then used to derive the CDR Data) under the Draft Rules (section 56AJ(3) in the CDR Act).

(e) Can an Accredited Data Recipient become a Data Holder?

22.13 We note that under section 56AJ(4) in the CDR Act, the Draft Rules may set out particular conditions where an Accredited Data Recipient becomes a Data Holder for CDR Data and any CDR Data that is directly or indirectly derived from that CDR Data (relevant CDR Data) after it has received that CDR Data from another Data Holder under the Draft Rules. For the initial implementation of the CDR regime, this will occur if:

22.13.1 the person is an ADI;

22.13.2 the CDR Consumer has acquired a Product from the person;

22.13.3 the person:

(a) reasonably believes that the relevant CDR Data is relevant to its provision of the Product to the CDR Consumer;

(b) has asked the CDR Consumer to agree to the person being a Data Holder, rather than an Accredited Data Recipient, of the relevant CDR Data;

(c) has explained to the CDR Consumer:

(i) that, as a result, the Privacy Safeguards would no longer apply to the person in relation to the relevant CDR Data;

(ii) the manner in which it proposes to treat the relevant CDR Data; and

(iii) why it is entitled to provide the CDR Consumer with this option; and

(d) has outlined the consequences, to the CDR Consumer, of not agreeing to this; and

22.13.4 the CDR Consumer has agreed to the person being a Data Holder, rather than an Accredited Data Recipient, of the relevant CDR Data.

22.14 Importantly, if an Accredited Data Recipient becomes a Data Holder, the Draft Rules provide that:

22.14.1 any consents to collect CDR Data under the consumer data request expire; and

22.14.2 any authorisations to disclose CDR Data in relation to the consumer data request expire.

(f) When is an accredited person an Accredited Data Recipient?

22.15 An "accredited person" is a person who holds an accreditation under section 56CA(1) in the CDR Act.

22.16 Under section 56CA(1) in the CDR Act, the Data Recipient Accreditor (for the initial implementation, this will be the ACCC), may, in writing, accredit a person if the Data Recipient Accreditor is satisfied that the person meets the criteria for accreditation specified in the Draft Rules.

22.17 The legislative framework draws a distinction between an "accredited person", and an "accredited data recipient". For the initial implementation, a person will only be an "accredited data recipient" of CDR Data (under section 56AK in the CDR Act) if:

22.17.1 the person is an accredited person;

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

22.17.3 the CDR Data was disclosed to the person under the Draft Rules; and

22.17.4 the person is not a Data Holder for the first-mentioned CDR Data (including because of the operation of section 56AJ(4) in the CDR Act). As discussed in paragraph 22.13 above, although it is possible for an Accredited Data Recipient to become a Data Holder in certain situations, the Draft Rules are currently silent about whether there are any conditions in the Draft Rules which trigger the operation of section 56AJ(4) in the CDR Act.

22.18 We note the effect of this is that a person who has received accreditation under the CDR Act, but has not yet received any CDR Data from another Data Holder, will be an "accredited person" but not an "accredited data recipient" (and such entities will also be Data Holders in relation to any CDR Data that they hold themselves). However, for convenience, we have (unless otherwise specified) used "Accredited Data Recipient" in this PIA report to refer to an accredited person who either has, or may, receive CDR Data under the CDR regime.

(g) Can an Accredited Data Recipient who has received CDR Data further disclose that CDR Data?

22.19 Under PS 6, an Accredited Data Recipient must not disclose CDR Data, unless:

22.19.1 the disclosure is required under the Draft Rules in response to a valid request from a CDR Consumer;

22.19.2 the Draft Rules otherwise authorise use or disclosure. For the initial implementation of the CDR regime, the Draft Rules provide that an Accredited Data Recipient is only authorised to use or disclose CDR Data if it is a permitted use or disclosure (Rule 7.7). A permitted use or disclosure includes:

(a) using the CDR Consumer's CDR Data to provide goods or services requested by the CDR Consumer (in accordance with the data minimisation principle and the CDR Consumer's current consent);

(b) directly or indirectly deriving CDR Data from the collected CDR Data for that purpose;

(c) disclosing, to the CDR Consumer, any of their CDR Data;

(d) disclosing the CDR Consumer's CDR Data to an outsourced service provider for the purposes of doing things specified in paragraphs 22.19.2(a) to 22.19.2(c) above, and to the extent reasonably needed to do those things; and

(e) disclosing (by sale or otherwise), to any person, CDR Data that has been de-identified in accordance with the CDR Data de-identification process; or

22.19.3 the disclosure is required or authorised by or under another Australian law or a court/tribunal order, and the Accredited Data Recipient makes a written note of the disclosure.

22.20 As specified in paragraph 22.19.2(d) above, an Accredited Data Recipient may disclose the CDR Consumer's CDR Data to an outsourced service provider. Under Rule 1.10, an outsourced service provider is a person to whom an Accredited Data Recipient discloses CDR Data under a CDR outsourcing arrangement.

22.21 A CDR outsourcing arrangement is a written contract between the discloser of CDR Data and the recipient of CDR Data. Under a CDR outsourcing arrangement:

22.21.1 the recipient will provide goods or services using CDR Data to the discloser; and

22.21.2 the recipient is required to comply with the following requirements in relation to any CDR Data disclosed to it by the discloser:

(a) the recipient must take the steps in Schedule 2 to protect that CDR Data as if it were an Accredited Data Recipient;

(b) the recipient must not use or disclose any such CDR Data other than in accordance with a contract with the discloser;

(c) the recipient must return, delete, provide records about deletion of, CDR Data, and it must direct any other person to which it has disclosed CDR Data to take such steps, when directed to do so by the discloser; and

(d) the recipient must only disclose any such CDR Data to another person under a CDR outsourcing arrangement and must ensure that the other person complies with the requirements of the CDR outsourcing arrangement.

22.22 In accordance with Rule 7.6, if the Accredited Data Recipient discloses CDR Data it has collected to another person (including an outsourced service provider) under a CDR outsourcing arrangement, any use or disclosure of that CDR Data by the other person (whether or not in accordance with the CDR outsourcing arrangement) is taken to have been by the Accredited Data Recipient (irrespective of whether the CDR Data was disclosed to the other person by the Accredited Data Recipient, or directly through one or more further CDR outsourcing arrangements).

22.23 Importantly, under Rule 4.12, an Accredited Data Recipient is restricted from asking a CDR Consumer to give consent to use or disclose their CDR Data for the purposes of:

22.23.1 selling the CDR Data (unless the CDR Data is de-identified in accordance with the CDR Data de-identification process); or

22.23.2 using or aggregating data for the purpose of identifying, compiling insights in relation to or building a profile in relation to any identifiable person who is not the CDR Consumer for that data and who did not make the consumer data request.

22.24 The effect of the above is that, for the initial implementation, an Accredited Data Recipient may further disclose CDR Data received from a Data Holder to its outsourced service providers. As specified in Rule 1.10(2)(iv), the outsourced service provider may disclose the CDR Data to another person under a CDR outsourcing arrangement, and it must ensure that the other person complies with the requirements of the CDR outsourcing arrangement.

Part F Analysis of APP Application and Compliance

23. Introduction

23.1 The OAIC Guide explains the need for PIAs to consider whether, and if so how, the relevant project complies with the APPs and with any other applicable privacy legislation.

23.2 In the CDR regime, that other applicable privacy legislation is the CDR legislative framework itself, including the Privacy Safeguards.

23.3 The implementation of the CDR regime will mean that for information which is CDR Data, the applicable privacy protections will depend on the relevant Sector, nature of the person or other entity holding that CDR Data and their role in the CDR regime. For example:

23.3.1 for some information held by some entities, the APPs will not apply at all (even if that entity is otherwise an APP entity) but the Privacy Safeguards will apply;

23.3.2 for the same information held by other entities, only some of the Privacy Safeguards will apply, and some, or all, or none of the APPs may also apply (depending on whether the participant is an APP entity); and

23.3.3 for the same information held by other entities, neither the Privacy Safeguards or the APPs may apply (but other protections in the CDR legislative framework may apply, e.g., contractual requirements for outsourced service providers).

23.4 Further complexity is added because the Privacy Safeguards apply to a broader range of entities and information than the APPs. Examples include that:

23.4.1 the information captured by the Privacy Safeguards (i.e. "CDR Data") has a different scope to "personal information"; and

23.4.2 the Privacy Safeguards afford protections to "CDR Consumers", which includes both individuals and businesses.

23.5 In addition, the CDR Act imposes obligations on small business operators once they become accredited under the CDR regime, which includes applying the Privacy Act to any personal information (that is not CDR Data) a small business operator holds as if the small business operator were an "organisation" under the Privacy Act.

23.6 This means that not all information held by a particular entity about, in relation to, or in connection with, a particular CDR Consumer can be treated in the same way, because different privacy protections may be required under the CDR legislative framework.[37]

[37] We note that definition of "personal information" under the Privacy Act requires that information be "about" an individual in order to be personal information. This differs from some formulations in the Privacy Safeguards (and from relevant provisions in other jurisdictions such as the GDPR). Our comment here is intended to be general, and not specific to a particular piece of legislation.

23.7 For this reason, it is not helpful to undertake a "normal" PIA analysis, where each of the APPs is considered in turn, with an analysis conducted as to whether or not the requirements of the APPs will be met if the project is implemented as intended. Rather, we have in this **Part F [Analysis of APP Application and Compliance]**:

23.7.1 considered when each of the APPs and/or Privacy Safeguards will apply to particular information generally; and

23.7.2 for each of the privacy concepts encapsulated by the APPs, determined whether the APPs and/or Privacy Safeguards apply to each of the Data Holder and/or Accredited Data Recipient.

24. Consideration of when the Australian Privacy Principles (APPs) and when the Privacy Safeguards (PSs) apply

24.1 The CDR regime imposes obligations on a broad range of entities. These entities include Accredited Data Recipients and Data Holders. The Privacy Safeguards and the APPs will apply to the entity depending on whether the entity is an Accredited Data Recipient (including whether it has received the relevant CDR Data, or has only been accredited as an "accredited person") and/or a Data Holder (see paragraph 24.4 for discussion on when these obligations apply to Accredited Data Recipients and paragraph 24.5 for discussion on when these obligations apply to Data Holders).

24.2 A starting point is to recognise that the APPs only apply to "personal information" as defined in the Privacy Act. To meet this definition, information must:

24.2.1 be about an individual – this means that the APPs will not apply to the handling of any CDR Data which is about a business rather than an individual (noting that the APPs may apply to a CDR Consumer which is a sole trader trading under the relevant individual's name);

24.2.2 identify an individual, or be such that an individual is reasonably identifiable – this means that the APPs will not apply to any CDR Data which is properly de-identified (and we note the potential for re-identification needs to be carefully considered when deciding whether information is, in fact, de-identified); [38] and

24.2.3 be held by an APP entity – this means that APPs will not apply to CDR Data which is held by, for example, a small business that is not an "APP entity" under the Privacy Act.[39]

24.3 The Privacy Safeguards are expressed to apply to, or in relation to, CDR Data, where there are one or more CDR Consumers for that data. This means that the definition of 'CDR Data' must be met (see discussion about the definition of "CDR Data" in **Part E [Fundamental Concepts]** of this PIA report). This in turn means that the Privacy Safeguards will not apply if the identity of the relevant CDR Consumer cannot be ascertained from the information.

24.4 If a person is an Accredited Data Recipient of CDR Data (see the discussion about the definition of "Accredited Data Recipient" in **Part E [Fundamental Concepts]** of this PIA report):

24.4.1 it does not need to comply with the APPs in relation to that CDR Data (section 56EC(4)(a) in the CDR Act);

[38] We note for completeness that the Privacy Safeguards will not apply to information that is properly de-identified either, as the information will no longer be a CDR Consumer's CDR Data.
[39] We note that the amendments to the Privacy Act have expanded the scope of the APP entities to include small business operators who are accredited as Accredited Data Recipients.

24.4.2 it does need to comply with the Privacy Safeguards in relation to that CDR Data; and

24.4.3 it does need to comply with the APPs (if it is an APP entity) for any other information it holds that is personal information but not CDR Data.[40]

24.5 If a person is a Data Holder (see the discussion about the definition of "Data Holder" in **Part E [Fundamental Concepts]** of this PIA report):

24.5.1 it needs to comply with the APPs in relation to any personal information it holds which is not CDR Data (if it is an APP entity);

24.5.2 it needs to comply with those Privacy Safeguards that are expressed to apply to Data Holders (e.g. PS 1) for all CDR Data (section 56EC(5) in the CDR Act); and

24.5.3 for CDR Data which is also personal information, it will also need to comply with all of the APPs (if it is an APP entity) except that:

(a) if PS 11(1) applies to disclosure of CDR Data (quality of data), APP 10 will not apply (section 56EC(4)(a) in the CDR Act); and

(b) if PS 13 applies in relation to the CDR Data (correction), APP 13 will not apply (section 56EC(4)(b) in the CDR Act).

24.6 We also note that outsourced service providers of Accredited Data Recipients are not required to comply with the Privacy Safeguards, although they will be required to comply with the APPs in respect of CDR Data that is also personal information (if they are an APP entity). Outsourced service providers will also be contractually required to comply with the security requirements in Schedule 2 to the Draft Rules.

24.7 We consider that the above complexity means that there is a risk that CDR Consumers (as well as Data Holders and Accredited Data Recipients) will not understand:

24.7.1 what the CDR regime is and how it operates in practice;

24.7.2 what constitutes CDR Data;

24.7.3 how the APPs and the Privacy Safeguards apply to each person (and hence, what rights they have, and what protections are afforded to their information);

24.7.4 what obligations they are subject to;

24.7.5 when CDR Data is governed by the APPs and the Privacy Safeguards; and

24.7.6 how the APPs and the Privacy Safeguards interact.

24.8 Stakeholders in their submissions also indicated that they would welcome particular guidance in additional areas, including:

24.8.1 the OAIC and the ACCC's approach to handling complaints under the CDR regime (the Australian Banking Association recommended updating the OAIC's *"Guide to privacy regulatory action"* to include information about how complaints will be handled by both the OAIC and the ACCC under the CDR regime;

[40] We note that the amendments to the Privacy Act have expanded the scope of the APP entities to include small business operators who are accredited as Accredited Data Recipients.

24.8.2 how outsourced service providers must handle CDR Data (noting that Accredited Data Recipients will, under the Draft Rules, retain responsibility for any uses or disclosures by outsourced service providers);

24.8.3 the uses or disclosures (as listed in Rule 4.12(3)(b)) where consent cannot be sought from CDR Consumers;

24.8.4 the requirement for destruction of CDR Data under PS 4, noting that there may be situations where Data Holders cannot destroy unsolicited information as it is not technically possible to irretrievably destroy the relevant CDR Data;

24.8.5 the grounds on which a Data Holder can refuse to disclose CDR Data in response to a valid request; and

24.8.6 the procedure for when CDR Data is intercepted by a malicious attack during the transfer of the CDR Data from the Data Holder to the Accredited Data Recipient, including the responsibilities of both Data Holders and Accredited Data Recipients.

24.9 We have recommended that all of the above are areas where further clarity and guidance is required, including to ensure CDR Consumers, Data Holders and Accredited Data Recipients are able to understand which set(s) of privacy protections apply, and in what circumstances they apply (see **Recommendation 2**).[41]

24.10 Stakeholders providing submissions strongly agreed with **Recommendation 2**, and the need for further guidance. Some stakeholders endorsed our view that consumer education is not, by itself, likely to be sufficient to mitigate against identified privacy risks, and that this is particularly so for vulnerable CDR Consumers. Some stakeholders, while still endorsing this view, did recognise the value of guidance for Data Holders and Accredited Data Recipients: "*In general, guidance is only useful for industry. However as it is important that industry comply with all standards, detailed guidance may assist*" (Submission by the Australian Privacy Foundation).

25. Analysis of the APPs and Privacy Safeguards

25.1 In the following table, we set out, for each Australian Privacy Principle (**APP**) and the associated Privacy Safeguard (**PS**):

25.1.1 a brief analysis of the differences between them;

25.1.2 how they will apply to Data Holders and Accredited Data Recipients participating in the CDR regime; and

25.1.3 any comments we have in relation to the differences (these are in bold italics in the third column).

[41] As mentioned in footnote 33, the OAIC has published draft "*Privacy Safeguard Guidelines*", which when finalised will provide useful guidance on many of the issues we have discussed in this PIA report (although we have not incorporated the contents of those draft guidelines into this document as they were published after our "point in time" analysis).

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
APP 1 – open and transparent management of personal information		
PS 1[42] – open and transparent management of CDR data		
Application	As expressed in the note at section 56EC(5) in the CDR Act, a Data Holder[43] must comply with both APP 1 and PS 1 (this means that a Data Holder must have both an APP Privacy Policy and a CDR Policy, and the Draft Rules require the two policies to be distinct from each other). An Accredited Data Recipient of CDR Data[44] must comply with PS 1 but is not required to comply with APP 1 in respect of CDR Data.	
Form of policy	While there are generally similar obligations in both APP 1 and PS 1 in relation to the open and transparent management of applicable information, there are differences in the requirement for an available policy about that management. PS 1 requires a CDR entity's CDR Policy about the management of CDR Data to be in a form approved in accordance with the Draft Rules (Rule 7.2 provides that the Commissioner may approve a form for a CDR Policy). APP 1 does not require use of a particular form for a privacy policy (there are requirements for it to be clearly expressed, and to contain specific information). Rule 7.2 provides further detail on the form of the CDR Policy. This information will be relevant for both Data Holders and Accredited Data Recipients in their provision of their CDR Policy.	

[42] For ease of reference, we have used the Privacy Safeguard number in the CDR Act section heading, rather than the applicable section of the CC Act in the CDR Act (e.g. to "PS 11(1)", rather than "section 56EN(1) in the CDR Act").
[43] In this table, we have assumed that the Data Holder is also an APP entity for the purposes of the Privacy Act, who handles CDR Data that is also personal information.
[44] In this table, "An Accredited Data Recipient of CDR Data" refers to an Accredited Data Recipient who has received CDR Data from a Data Holder.

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
Information to be in the policy	Due to the nature of the CDR regime, PS 1 sets out the coverage of each policy for a Data Holder and an Accredited Data Recipient separately, whilst APP 1 sets out the coverage of the policy for any APP entity. There are additional requirements imposed on Accredited Data Recipients which are not imposed on APP entities under APP 1. This includes the Accredited Data Recipient having to contain in its policy: • the consequences if the CDR Consumer withdraws their consent to collect and use CDR Data; • the circumstances in which the Accredited Data Recipient may disclose CDR Data to a person who is not an accredited person (which may include an outsourced service provider); • the events about which the Accredited Data Recipient will notify the CDR Consumers of their CDR Data; • the circumstances in which the Accredited Data Recipient must delete or de-identify CDR Data in accordance with a request given by a CDR Consumer for the CDR Data under the Draft Rules. The Draft Rules provide further information about this requirement (including information about de-identification of CDR Data that is not redundant and use of that de-identified data; information about the deletion of redundant data; information about de-identification of redundant data; and how the CDR Consumer can elect to delete their CDR Data); and • information about whether it intends to store CDR Data outside of Australia, and if so, the countries in which it proposes to store CDR Data. There are also additional requirements imposed on Data Holders which are not imposed on APP entities under APP 1. This includes the Data Holder having to contain in its policy: • whether it accepts requests for voluntary consumer data (and voluntary product data) and if so, associated information about fees it charges. Both Accredited Data Recipients and Data Holders must also include information about internal dispute resolution processes and complaint mechanisms.	***The application of PS 1, and the requirement for the provision of additional information about management of CDR Data, is a privacy-enhancing strategy.***
Availability of policy	APP 1 requires the policy to be made available in an appropriate form, whilst PS 1 specifically requires the policy to be made available through each online service that a	As above, this means that Accredited Data Recipients and Data Holders may, if they wish, adopt different mechanisms to

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
	Data Holder or an Accredited Data Recipient ordinarily uses to deal with the CDR Consumer.	make their APP Privacy Policy and their CDR Policy available. ***This may make it harder for CDR Consumers to locate the applicable policies.*** ***See Recommendation 2.***
APP 2 – anonymity and pseudonymity		
PS 2 – anonymity and pseudonymity		
Application	PS 2 (and Rule 7.3) applies to Accredited Data Recipients of CDR Data only. APP 2 does not apply to Accredited Data Recipients in respect of CDR Data, but will apply to Data Holders. Under PS 2 (and Rule 7.3), an Accredited Data Recipient must give a CDR Consumer the option of using a pseudonym, or not identifying themselves, unless dealing with identified CDR Consumers is required or authorised by law/court or tribunal order, or it is otherwise impracticable in relation to particular CDR Data.	For most CDR Data, it is likely that the exception in Rule 7.3 will apply (as it will be impractical for the Accredited Data Recipient to deal with a CDR Consumer that has not been identified in the context of the banking Sector (which has specific requirements for identity verification etc.)).
APP 3 – collection of solicited personal information		
PS 3 – soliciting CDR data from CDR participants		
Application	PS 3 only applies to "accredited persons".[45] APP 3 does not apply to Accredited Data Recipients in respect of CDR Data, but will apply to Data Holders.	
Sensitive information	APP 3 draws distinctions between collecting sensitive information and other personal information which is not sensitive information, whilst PS 3 does not draw any distinction between different types of CDR Data.	

[45] See discussion at paragraph 22.18 of **Part E [Fundamental Concepts]** (all Accredited Data Recipients must be an "accredited person" but not all accredited persons may have received CDR Data and therefore be an "accredited data recipient").

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
Collection	APP 3 specifies that an APP entity must only collect personal information if the information is reasonably necessary for one or more of the entity's functions or activities. PS 3 specifies that an accredited person must only collect CDR Data under the Draft Rules from the Data Holder of the CDR Data, if the CDR Consumer of the CDR Data has validly requested this in accordance with the Draft Rules, and the accredited person complies with all other requirements in the Draft Rules in relation to collection of CDR Data from the Data Holder.	***PS 3 provides added protections to CDR Consumers by requiring compliance with the privacy-enhancing requirements in the Draft Rules. These protections also include that under PS 3, accredited persons must receive a valid request (i.e. consent must be given) from CDR Consumers before they can seek to collect CDR Data.***
APP 4 – dealing with unsolicited personal information		
PS 4 – dealing with unsolicited CDR data from CDR participants		
Application	PS 4 only applies to "accredited persons".[46] APP 4 does not apply to Accredited Data Recipients in respect of CDR Data, but will apply to Data Holders.	
Destruction or de-identification	Under APP 4, if an APP entity determines that personal information it has received was not solicited by the entity, it must determine whether the entity could have collected the information under APP 3. If the answer is no (and the information is not contained in a Commonwealth record), the entity must destroy the information or ensure that the information is de-identified, but only if it is lawful and reasonable to do so. Under PS 4, if an accredited person collects CDR Data not as a result of seeking to collect that CDR Data, and it is not required to retain the CDR Data by or under an Australian law or a court/tribunal order, the accredited person must destroy that CDR Data.	***PS 4 requires destruction of the relevant information, rather than either destruction or de-identification. In our view, this is a privacy-enhancing protection for CDR Data.***

[46] See footnote 45 above.

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
APP 5 – notification of the collection of personal information		
PS 5 – notifying of the collection of CDR data		
Application	PS 5 (and Rule 7.4) only applies to "accredited persons".[47] APP 5 does not apply to Accredited Data Recipients in respect of CDR Data, but will apply to Data Holders.	
Timing of notification	Under APP 5, an APP entity must, at or before the time or, if that is not practicable, as soon as practicable after, notify the individual of collection of personal information including the matters listed in APP 5.2 or otherwise ensure the individual is aware of the matters listed in APP 5.2. These matters include the identity of the APP entity, the purposes for collection of the personal information, the consequences for the individual if all or some of the personal information is not collected, which other entities, bodies or people information of that kind is usually disclosed to, information about the APP Privacy Policy and if the APP entity is likely to disclose the personal information to overseas recipients. Under PS 5, an accredited person must give the CDR Consumer a notification of collection of CDR Data at or before the time specified in the Draft Rules (Rule 7.4 requires the notice to be given by updating the Consumer Dashboard as soon as practical after collection, to indicate what CDR was collected, when it was collected and the Data Holder of the CDR Data).	***The Consumer Dashboard does not need to include all of the APP 5 matters (for example, whether the accredited person is likely to disclose the CDR Data to an overseas entity - i.e. an outsourced service provider). However, given that the CDR Consumer will receive multiple notifications of the matters relating to collection, use and disclosure of their CDR Data (such as for the purposes of Rules 4.18 and 4.20), we consider that the Consumer Dashboard does not need to repeat information already provided to CDR Consumers.***

[47] See footnote 45 above.

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
APP 6 – use or disclosure of personal information		
PS 6 – use or disclosure of CDR data by accredited data recipients or designated gateways		
Application	PS 6 applies to Accredited Data Recipients of CDR Data only. APP 6 does not apply to Accredited Data Recipients in respect of CDR Data, but will apply to Data Holders.	
Use and disclosure	APP 6 states that if an APP entity has personal information that was collected for a primary purpose, it must not be used or disclosed for a secondary purpose, unless exceptions apply. These exceptions include if the individual would reasonably expect the APP entity to use or disclose the information for the secondary purpose, the use or disclosure is authorised by or under an Australian law, or permitted situations exist. PS 6 requires Accredited Data Recipients to only use or disclose CDR Data in response to a valid request from the CDR Consumer, or if that disclosure or use of CDR Data is required or authorised under the Draft Rules, or if the use or disclosure is required or authorised by or under another Australian law. Use or disclosure of CDR Data will be authorised under the Draft Rules if it is for a "permitted use or disclosure". These are listed in Rule 7.5.	In the initial implementation of the CDR regime, the effect of PS 6 will be to prohibit uses or disclosures of CDR Data by Accredited Data Recipients unless: • the disclosure of CDR Data is required under the Draft Rules in response to a valid request from a CDR Consumer for the CDR Data; • the use or disclosure of CDR Data is otherwise required, or authorised under the Draft Rules in accordance with one of the listed permitted uses or disclosures under Rule 7.5; and • the use or disclosure of CDR Data is required or authorised by or under another Australian law or a court/tribunal order, and the Accredited Data Recipient makes a written note of the use or disclosure. (See **Part E [Fundamental Concepts]** of this PIA report for further discussion about further use or disclosure of CDR Data by Accredited Data Recipients.)

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
Exceptions	APP 6 does not apply to the use or disclosure of personal information for the purpose of direct marketing or government related identifiers. PS 6 does not apply to the use or disclosure of CDR Data for the purposes of direct marketing.	There is no mention of government related identifiers as an exception to PS 6 (we are unsure of the policy reasons behind this difference).
APP 7 – direct marketing		
PS 7 – use or disclosure of CDR Data for direct marketing by accredited data recipients or designated gateways		
Application	PS 7 applies to Accredited Data Recipients of CDR Data only. APP 7 does not apply to Accredited Data Recipients in respect of CDR Data, but will apply to Data Holders.	
Exceptions to use or disclose for direct marketing	Under APP 7, personal information may be used or disclosed if the organisation collected the information from the individual, the individual would reasonably expect the organisation to use/disclose the information for that purpose and the individual is provided with a simple way to opt out of receiving direct marketing from the organisation. Further, personal information may be used/disclosed for the purpose of direct marketing if the individual has consented to the use/disclosure. Sensitive information may be used or disclosed for the purpose of direct marketing if the individual has consented to the use/disclosure of the information for that purpose. Under PS 7, CDR Data must only: • be disclosed if the disclosure is required under the Draft Rules in response to a valid request from a CDR Consumer; or • be disclosed or used if the disclosure or use is authorised under the Draft Rules in accordance with a valid consent of a CDR Consumer. The Draft Rules provide that the use or disclosure of CDR Data for the purposes of direct marketing is authorised if it is a "permitted use or disclosure" that relates to direct marketing, as provided for in Rule 7.5(3).	***There are fewer exceptions under which Accredited Data Recipients can use or disclose CDR Data for the purposes of direct marketing (effectively, the consent of the CDR Consumer, obtained in accordance with the Draft Rules, will be required, and the use or disclosure will have to be a "permitted use or disclosure" of CDR Data for the purposes of direct marketing, in accordance with Rule 7.5(3)).*** ***We consider that this is a privacy-enhancing feature of PS 7.***

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
APP 8 – cross-border disclosure of personal information		
PS 8 – overseas disclosure of CDR data by accredited data recipients		
Application	PS 8 applies to Accredited Data Recipients of CDR Data only. APP 8 does not apply to Accredited Data Recipients in respect of CDR Data, but will apply to Data Holders.	
Liability of making overseas disclosure	APP 8 provides that APP entities must take certain steps before disclosing personal information to an entity located overseas, unless an exception applies. In certain circumstances, an act done by the overseas recipient is taken, under section 16C of the Privacy Act [Acts and practices of overseas recipients of personal information], to have been done by the APP entity and to be a breach of the APPs. PS 8 prohibits disclosure of CDR Data by an Accredited Data Recipient to a new recipient (i.e. the recipient is not in Australia and not a CDR Consumer for that CDR Data), unless: • the new recipient is themselves an accredited person; • the Accredited Data Recipient has taken reasonable steps to ensure that any act or omission by the new recipient will not breach PS 1(3) or another PS penalty provision; • the Accredited Data Recipient reasonably believes that the new recipient is subject to a law or binding scheme similar to the CDR regime and a CDR Consumer for the CDR Data will be able to enforce those protections; or • the conditions specified in the Draft Rules are met (but no such conditions are specified in the Draft Rules). Like APP 8, an act or omission by the new recipient may in some circumstances be taken to be an act or omission by the Accredited Data Recipient.	PS 8(1) can be reconciled with the effective restrictions on further disclosure in PS 6 and the Draft Rules, as it permits disclosure to an overseas outsourced service provider who is either themselves accredited, or where another condition in PS 8(1)(d) to (f) is met. PS 8 does not contain an exception which allows overseas disclosure with the consent of the CDR Consumer (as is the case under APP 8) – this avoids the possibility of the CDR Consumer being pressured into signing a broad consent permitting such disclosures – the Accredited Data Recipient is required to take other steps to ensure appropriate privacy treatment of the CDR Data by the overseas recipient. ***In our view, this is a privacy-enhancing feature.*** Please see analysis at Step 7C in the table in **Part G [Analysis of Risks Associated with Information Flows in the CDR Regime]** of this PIA report, which provides further discussion on the risks and current mitigation strategies in relation to situations where an Accredited

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
		Data Recipient may disclose CDR Data to its outsourced service providers.
APP 9 – adoption, use or disclosure of government related identifiers		
PS 9 – adoption or disclosure of government related identifiers by accredited data recipients		
Application	PS 9 applies to Accredited Data Recipients of CDR Data only. APP 9 (other than APP 9.3, which is applied by PS 9) does not apply to Accredited Data Recipients in respect of CDR Data, but will apply to Data Holders.	
Scope	APP 9 provides a range of situations in which an organisation may adopt, use or disclose a government related identifier, including if it considers that the use or disclosure of the identifier is reasonably necessary for the organisation to verify the identity of the individual for the purposes of the organisation's activities or functions. PS 9 states that adoption or use or disclosure of government related identifiers may only be permitted if the adoption, use or disclosure is required or authorised by or under an Australian law other than the Draft Rules or a court/tribunal order, or APP 9.3 applies (which states situations where regulations prescribe the adoption, use or disclosure of government related identifiers).	The requirements for the adoption, use or disclosure of government related identifiers will be largely consistent between Accredited Data Recipients and Data Holders.

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
N/A		
PS 10 – notifying of the disclosure of CDR data		
Application	PS 10 (and Rule 7.9) applies to both Accredited Data Recipients of CDR Data and Data Holders.	
Notification	The effect of PS 10 (and Rule 7.9) is to require Data Holders to, as soon as practicable, update a CDR Consumer's Consumer Dashboard to indicate that CDR Data has been disclosed to an Accredited Data Recipient (with what CDR Data was disclosed, when it was disclosed and who it was disclosed to). Although PS 10 also requires Accredited Data Recipients to take steps in the Draft Rules to notify CDR Consumers about disclosures of CDR Data, no such steps have been specified.	***Accredited Data Recipients are not required to update the Consumer Dashboard in relation to permitted disclosures of CDR Data to outsourced service providers. Accredited Data Recipients are not permitted to disclose CDR Data other than in accordance with the Draft Rules. For the initial implementation of the CDR regime, under Rule 7.7, a permitted use or disclosure includes disclosure to outsourced service providers under a CDR outsourcing arrangement. A CDR outsourcing arrangement is a written contract that requires an outsourced service provider to comply with several requirements, including to take the steps in Schedule 2 to protect CDR Data. A list of outsourced service providers must be included in the Accredited Data Recipient's CDR Policy and an Accredited Data Recipient must make a CDR Consumer aware of the fact that their CDR Data may be disclosed to an outsourced service provider.*** ***We query whether it would be practical for Accredited Data Recipients to***

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
		notify CDR Consumers of every single instance of a permitted disclosure of CDR Data to its outsourced service providers.
APP 10 – quality of personal information		
PS 11 – quality of CDR Data		
Application	PS 11 applies to both Accredited Data Recipients of CDR Data and Data Holders. If PS 11(1) applies to a Data Holder, APP 10 does not apply.	
Steps	APP 10.1 states that an APP entity must take such steps (if any) as are reasonable in the circumstances to ensure that the personal information it collects is accurate, up to date and complete. Similarly, APP 10.2 requires an APP entity to take such steps (if any) as are reasonable in the circumstances**,** to ensure personal information they disclose is, having regard to the purpose of the use or disclosure, accurate, up-to-date, complete and relevant. Under PS 11(1) and (2), Data Holders and Accredited Data Recipients who disclose CDR Data (as permitted by the Draft Rules) must take reasonable steps having regard to the purpose for which the CDR Data is held, to ensure that the CDR Data is, accurate, up to date and complete.	***We understand the difference between the applicable tests in APP 10 and PS 11 (see italics in column 2) is intended to reflect that Data Holders and Accredited Data Recipients may hold the same CDR Data for different purposes, and the quality of the CDR Data may not be required to be the same (having regard to that purpose).***
Incorrect CDR Data and correction	PS 11 places an obligation on Data Holders and Accredited Data Recipients to notify the CDR Consumer within 5 business days (as required by Rule 7.10) if they have disclosed CDR Data and then later become aware some or all of the CDR Data was incorrect, because, it was inaccurate, out of date or incomplete. Rule 7.10 prescribes what a Data Holder must include in its written notice to CDR Consumers if it is found that some or all of the CDR Data disclosed was incorrect. Further, if the CDR Consumer then requests for the Data Holder or Accredited Data Recipient (as relevant) to fix this by disclosing to the recipient the corrected CDR Data, it must do this.	***The requirement to notify the CDR Consumer of any provision of information that is later determined to be inaccurate etc (and to take steps to correct this if required) is a privacy-enhancing feature.***

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
APP 11 – security of personal information		
PS 12 – security of CDR data and destruction or de-identification of redundant CDR data		
Application	PS 12 applies to Accredited Data Recipients of CDR Data only. APP 11 does not apply to Accredited Data Recipients in respect of CDR Data, but will apply to Data Holders.	
Steps to protect information	APP 11 requires an APP entity to take such steps as are reasonable in the circumstances to protect the personal information it holds from misuse, interference and loss, and from unauthorised access, modification or disclosure. PS 12 requires Accredited Data Recipients to take the steps specified in the Draft Rules to protect the CDR Data from misuse, interference and loss, and from unauthorised access, modification or disclosure. Under the Draft Rules, Accredited Data Recipients must comply with Schedule 2 to the Draft Rules (as specified in Rule 7.11), which are the steps for PS 12 – security of CDR Data held by Accredited Data Recipients. Given the detail provided in Schedule 2 to the Draft Rules, there are very strict (and comprehensive) steps the Accredited Data Recipient must take to ensure that CDR Data is protected.	***The specification of the particular security requirements in Schedule 2 to the Draft Rules provides a higher degree of certainty for Accredited Data Recipients (and CDR Consumers) about the required security protections. This is a privacy enhancing feature.***

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
Steps after information is no longer needed	Under APP 11, if the APP entity holding the personal information no longer needs the information, the information is not contained in a Commonwealth record and the entity is not required by an Australian law to retain the information, an APP entity must take such steps as are reasonable in the circumstances to destroy the personal information, or to ensure that the information is de-identified. Data Holders will be required to take such steps as are reasonable in the circumstances to destroy or de-identify any personal information they hold in relation to CDR Consumers. Under PS 12, subject to the exceptions specified in PS 12(2) (e.g. the CDR Data does not relate to any legal/dispute resolution proceedings and the Accredited Data Recipient is not required by an Australian law to retain the CDR Data), the Accredited Data Recipient must take the steps specified in the Draft Rules to destroy redundant data or ensure the redundant data is de-identified. Accredited Data Recipients must comply with PS 12, and with Rule 7.12 and Rule 7.13. Rule 7.12 sets out the steps an Accredited Data Recipient must follow to de-identify redundant data. If Rule 7.12 does not apply, the Accredited Data Recipient must delete redundant data in accordance with Rule 7.13. The Draft Rules also specify the CDR Data de-identification process and CDR Data deletion process (in Rule 1.17 and Rule 1.18).	***Specification of the required de-identification and deletion processes in the Draft Rules provides a higher degree of certainty for Accredited Data Recipients (and CDR Consumers) about the treatment of redundant data. This is a privacy enhancing feature.***

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
APP 12 – access to personal information		
N/A		
Application	APP 12 will not apply to Accredited Data Recipients in relation to CDR Data (even if it is personal information). This means that CDR Consumers who are individuals will not have rights of access under APP 12 to their CDR Data which is personal information. However, APP 12 will apply to Accredited Data Recipients (who are APP entities) in relation to personal information that is not CDR Data (as discussed in paragraph 17.22 of **Part D [Project Description],** the Privacy Act (including the APPs) applies to personal information which is not CDR Data and is held by Accredited Data Recipients). APP 12 will apply to Data Holders, meaning that CDR Consumers will have rights of access to that personal information which is held by the Data Holder.	***It is not clear as to the policy reasons why the Privacy Safeguards do not include a right for CDR Consumers to access their CDR Data whilst it is in the hands of the Accredited Data Recipient.*** ***See Recommendation 4.***
APP 13 – correction of personal information		
PS 13 – correction of CDR Data		
Application	PS 13 (and Rule 7.15) applies to both Accredited Data Recipients of CDR Data and Data Holders. If PS 13(1) applies to a Data Holder, APP 13 will not apply to the Data Holder.	Therefore, if a Data Holder is not requested to correct the CDR Data by the CDR Consumer, it must continue to comply with APP 13, and take such steps as are reasonable to correct any personal information it is satisfied is out of date, incomplete, irrelevant or misleading.
Scope	APP 13 is broader than PS 13, in that APP 13 also requires an APP entity to take correction steps even if there is no request by the individual for correction. APP 13 states that an APP entity must take such steps (if any) as are reasonable in the circumstances to correct personal information if it is either satisfied that the information is out of date, incomplete, irrelevant or misleading, or the individual requests to correct the information, so as to ensure that the information is accurate, up to date, complete, relevant and not misleading. APP 13 also includes taking such steps (if any) as are	Accredited Data Recipients will be required to comply with PS 13.

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
	reasonable in the circumstances to notify any other APP entities the personal information has been previously disclosed to of the correction. In relation to Data Holders, PS 13 states that if a CDR Consumer requests the Data Holder to correct the CDR Data and the Data Holder was earlier required or authorised under the Draft Rules to disclose the CDR Data, it must respond to the request to correct the CDR Data by taking such steps as specified in the Draft Rules. In relation to Accredited Data Recipients, PS 13 states that if a CDR Consumer requests the Accredited Data Recipient to correct the CDR Data, it must respond to the request to correct the CDR Data by taking such steps as specified in the Draft Rules.	
Timing to respond to a request	APP 13.5 provides that an agency (as defined in the Privacy Act) must respond to a request to correct personal information within 30 days after the request is made, and an organisation (as defined in the Privacy Act) must respond within a reasonable period after the request is made. PS 13 provides that, as specified in Rule 7.15(a), the Data Holder or Accredited Data Recipient (as relevant) must acknowledge receipt of the request to correct CDR Data as soon as practicable.	If PS 13 (1) does not apply, Data Holders must respond to a request to correct personal information in accordance with APP 13(5) (depending on whether the Data Holder is an agency or organisation). If PS 13(1) applies, Data Holders must acknowledge receipt of the request as soon as practicable. Accredited Data Recipients must acknowledge receipt of the request as soon as practicable.
Steps to take when responding to a correction request	APP 13.2 provides that if an APP entity has corrected personal information about an individual that has been previously disclosed to another APP entity, and the individual requests the APP entity to notify the other APP entity of the correction, the APP entity must take such steps as are reasonable in the circumstances to give that notification (unless it is impracticable or unlawful to do so). Under APP 13.3, if the APP entity refuses to correct the personal information as requested by the individual, the APP entity must give the individual a written notice including the reasons for the refusal and the mechanisms available to complain about the refusal. Further, if the APP entity refuses to correct the personal information, and the individual requests the APP entity to associate with the information a statement that the	The requirements in relation to steps to take when responding to a correction request and the matters to be dealt with in responding to such a request must be complied with by Data Holders if PS 13(1) applies, and must be complied with by Accredited Data Recipients.

Table of comparison between Australian Privacy Principles (APPs) and Privacy Safeguards (PSs)		
	information is inaccurate, out of date, incomplete, irrelevant or misleading, the APP entity must take such steps as are reasonable in the circumstances to do so, so as to make the statement apparent to users of the information. PS 13 provides that, as specified in rule 7.15, the recipient of a request to correct CDR Data must, within 10 business days after receipt of the request, and to the extent it considers appropriate, correct the CDR Data, or must include a statement with the CDR Data ensuring it is accurate, up to date, complete and not misleading and attach an electronic link to a digital record of the CDR Data. The recipient must also give the requester (CDR Consumer) a written electronic notice that indicates what actions the recipient took in response to the request, an explanation if the recipient did not think it appropriate to take a step provided for in the paragraph above, and set out the complaint mechanism available to the requester (see Part 6 – Rules relating to dispute resolution of the Draft Rules).	

Part G Analysis of Risks Associated with Information Flows in the CDR Regime

26. Introduction

26.1 In this **Part G**, we have analysed risks that we have identified as being associated with particular information flows in the CDR regime.

26.2 To assist in identifying those information flows, we have identified the following steps:

Pre-operation of the CDR regime

26.2.1 **Step 0** (Information is provided to the Data Holder, including by the CDR Consumer.[48] This step occurs in the ordinary course of the Data Holder's business and before any request is made by the CDR Consumer for access to their CDR Data).

Direct requests

26.2.2 **Step 1A**[49] (Direct request by CDR Consumer. In this step, the CDR Consumer makes a direct request for their CDR Data to the Data Holder, and is provided with that CDR Data by the Data Holder).

Accredited Data Recipient Requests

26.2.3 **Step 1B** (CDR Consumer gives consent to Accredited Data Recipient to collect and use their CDR Data).

26.2.4 **Step 2** (Accredited Data Recipient obtains technical information from the ACCC's CDR ICT system to send request for CDR Data to the Data Holder).

26.2.5 **Step 3** (Accredited Data Recipient sends a request to the Data Holder on behalf of the CDR Consumer. Accredited Data Recipient then redirects the CDR Consumer to the Data Holder's system).

26.2.6 **Step 4** (CDR Consumer authorises the Data Holder to release their CDR Data to the Accredited Data Recipient).

26.2.7 **Step 5** (Data Holder confirms that the Accredited Data Recipient is accredited).

26.2.8 **Step 6** (Data Holder transfers the CDR Data to the Accredited Data Recipient; and Accredited Data Recipient collects that CDR Data).

26.2.9 **Step 7A**[50] (Accredited Data Recipient uses CDR Data to provide goods or services requested by the CDR Consumer).

[48] We note that this information may have been provided before commencement of the CDR regime, in which case the individual or business providing the information would not have been a "CDR Consumer", and the information would not have been "CDR Data", when the information was provided.
[49] Please note that Steps "1A" and "1B" happen independently, and not sequentially. We have given them numbers for identification purposes only.
[50] Please note that Steps "7A" to "7B" may happen in any order or concurrently, and not all Accredited Data Recipients will necessarily undertake all of these Steps. We have given the Steps numbers for identification purposes only.

26.2.10 **Step 7B** (Accredited Data Recipient discloses CDR Data to the CDR Consumer (may not apply to all Accredited Data Recipients)).

26.2.11 **Step 7C** (Accredited Data Recipient discloses CDR Data to an outsourced service provider (may not apply to all Accredited Data Recipients)).

26.2.12 **Step 7D** (Accredited Data Recipient de-identifies CDR Data and discloses the de-identified data to third parties (may not apply to all Accredited Data Recipients)).

26.2.13 **Step 8** (CDR Consumer withdraws their consent or their consent expires).

26.2.14 **Step 9** (CDR Consumer withdraws their authorisation or their authorisation expires).

26.2.15 **Step 10** (Accredited Data Recipient's accreditation is suspended, revoked, or surrendered).[51]

26.3 For each step, we have created a diagram illustrating the relationships and information flows involved. A reference to the relevant diagram in **Attachment 2** to this PIA report is included for each step below.

26.4 We have described and considered the information flows and privacy risks associated with each of those steps in the tables below. We have identified some of the key existing mitigation strategies that have been included in the legislative framework, together with our analysis of any identified gaps.

26.5 For each identified gap, we have then considered whether any additional mitigation strategies could be implemented, to further protect the privacy of individuals. These recommendations are referenced in this **Part G [Analysis of Risks Associated with Information Flows in the CDR Regime]**, but more fully discussed in **Part B [Executive Summary]**.

26.6 Given that the CDR Act has now been passed and royal assent given, we have taken into account that further legislative reforms are unlikely to be a viable option for enhancing privacy in the short-term. For example, some stakeholders in their submissions expressed the view that there should be a single set of privacy protections that apply to information which is CDR Data (irrespective of whether it is held by a Data Holder, an Accredited Data Recipient, or a third party). We understand that such a "closed system" does not reflect the policy intent behind the CDR legislative framework (that is, the CDR regime is not intended to replace the current privacy framework applicable to the holding of personal information, but is designed to promote further protections around disclosure of CDR Data). However, we have recommended that further guidance should be provided given the complexity of the CDR legislative framework (see **Recommendation 2**).

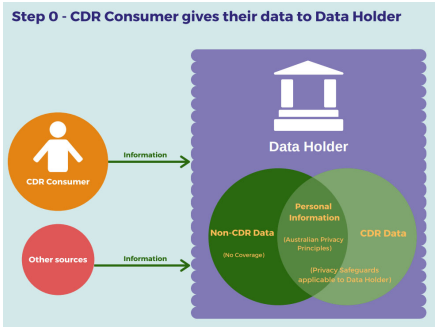
[51] Please note that Step 10 could occur at any time and may not occur at all for a particular Accredited Data Recipient (i.e., this Step is not sequential, but we have given it a number for identification purposes).

Step 0. CDR Consumer gives their data to Data Holder

Summary of step:

The CDR Consumer provides information to the Data Holder. This step occurs before operation of any requests for provision of CDR Data (note that the definitions of "CDR Consumer" and "CDR Data" and "Data Holder" must be met).

Relevant Diagram in Attachment 2:



STEP 0 – CDR CONSUMER GIVES DATA TO DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**Data Holder does not properly identify and apply the appropriate privacy protections[52] to CDR Data and non CDR Data, and between personal information and non-personal information**	The CDR Act sets out when the APPs will not apply to CDR Data held by a Data Holder (see section 56EC(4) in the CDR Act and also the analysis in **Part F [Analysis of APP Application and Compliance]** of this PIA report). Where information is not CDR Data but is personal information about an individual CDR	The complexity of the CDR regime makes it difficult for both CDR Participants and CDR Consumers to properly navigate when and where CDR regime and/or APP protections apply to the different types of data held by the Data Holder.

[52] This is not intended to imply that all of the privacy protections in the CDR regime will all initially apply to data held by Data Holders (other than the requirements for a CDR policy, a Data Holder's obligations are generally triggered by a consumer data request (or product data request) for disclosure of CDR Data).

STEP 0 – CDR CONSUMER GIVES DATA TO DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	To determine which category or categories of information particular data may fall within will require careful analysis by the Data Holder. In addition, we understand that the initial Data Holders may hold the various categories of information in and across many different components of their ICT systems. The complexity and overlapping nature of the various categories increases the risk that information will be incorrectly categorised and the appropriate protections will not be applied. If information is not properly classified by Data Holders, there is a risk that without clarity and guidance, CDR Consumers may have data disclosed that does not fall within the protections of the CDR regime.	Consumer, the APPs will apply (if held by an APP entity).	There is currently a lack of clarity or specific guidance for CDR Consumers and other CDR Participants about: 1. when data will be defined as CDR Data; 2. when CDR Data is captured by the Privacy Act; and 3. at what point the CDR Data is captured by the CDR regime and no longer falls within the protections of the APPs. To address this gap, we have recommended the provision of guidelines by the OAIC, and other activities to promote the understanding and acceptance of the Privacy Safeguards, and educational programs to protect CDR Data. We understand that the OAIC currently intends to issue such guidelines and to undertake other activities (see **Recommendation 2**).

STEP 0 – CDR CONSUMER GIVES DATA TO DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
2.	**CDR Consumers do not understand how CDR Data will be managed** CDR Consumers do not know or understand how the Data Holder will manage CDR Data that they provide to a Data Holder.	Data Holders must have an available CDR Policy which informs CDR Consumers about their management of CDR Data. The Information Commissioner may approve a form for a CDR Policy (Rule 7.2(1)). The policy is to be readily available to CDR Consumers.	We query whether the provision of a CDR policy is likely to be sufficient (and whether CDR Consumers are likely to closely examine such policies, if at all, before providing CDR Data to a Data Holder). To address this gap, it will be important that CDR Consumers understand the protections that do, and do not, apply to their CDR Data (see **Recommendation 2**).
3.	**CDR Data held by a Data Holder is subject to malicious attacks, resulting in theft of information about the CDR Consumer** Data Holders are not required to comply with PS 12, which provides the procedures for ensuring the security of CDR Data and the destruction or de-identification of redundant CDR Data. There is a risk that as the Data Holder's systems are not required to have the same security safeguards as Accredited Data Recipients (or their outsourced service providers), as required by Schedule 2 to the Draft Rules,	The Privacy Act, including the requirements of APP 11, will apply in relation to personal information held by Data Holders who are APP entities. (We have noted some stakeholders' concerns about the adequacy of the level of protection under the APPs.)	APP 11 does not have protections which are as clear and strong as those in PS 12. In addition, the APPs only apply to CDR Data which is also personal information and which is held by an APP entity. This means that CDR Data may have a higher level of protection when received by an Accredited Data Recipient, than when the same information is held by a Data Holder. The Data Holder listing process (in Rule 5.25 of the Draft Rules) does not expressly involve any testing processes, or collection or assessment of information which would ensure an appropriate level of security protections by Data Holders (although we note that the Accreditation Registrar may collect "other information" if required for requests to be processed in accordance with the Draft Data Standards,

STEP 0 – CDR CONSUMER GIVES DATA TO DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	there may be an increased risk of malicious attacks.		which could potentially include security-related information). We have therefore recommended that the ACCC consider whether any process for testing a Data Holder's compliance with the Draft Data Standards should be included in the Draft Rules (including when, how and how often testing will occur), and whether that process does, or should, include assessment of a Data Holder's security in relation to the transmission of CDR Data (see **Recommendation 3**). In general, stakeholders who provided submissions broadly supported the need for increased clarity about ongoing testing (including testing for compliance with security requirements) for all CDR Participants. However, one stakeholder submitted that any extension to the Draft Rules "*should recognise the requirements already imposed upon many Data Holders in relation to security obligations*" (Submission by the Australian Retail Credit Association). We consider this to be a valid point that should be taken into account if **Recommendation 3** is implemented.

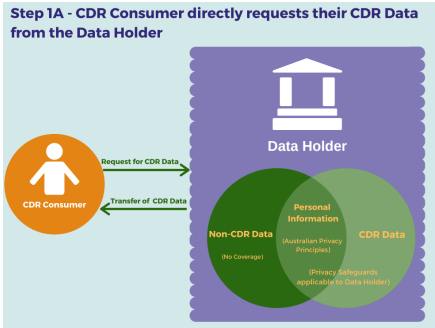
STEP 0 – CDR CONSUMER GIVES DATA TO DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
4.	**A CDR Consumer requests a Data Holder to destroy/de-identify their CDR Data** CDR Consumers do not have a right under the CDR legislative framework to require that a Data Holder destroy or de-identify their CDR Data. (See also section 56BD(3) in the CDR Act which prohibits the Draft Rules from including matters about destruction of CDR Data by Data Holders.)	Pursuant to the Draft Rules, Data Holders must provide a CDR Policy which informs CDR Consumers on the management of their CDR Data. Where information is not CDR Data but is personal information about an individual CDR Consumer, APP 11.2 will apply (if held by an APP entity).	APP 11.2 only applies to personal information, not all CDR Data, and only applies if the Data Holder is an APP entity. Given the intention of the CDR Act (including as reflected in section 56BD(3)), we consider that it will be important that CDR Consumers understand the protections that do, and do not, apply to their CDR Data (see **Recommendation 2**).

Step 1A. CDR Consumer makes a direct request to the Data Holder for their CDR Data

Summary of step:

The CDR Consumer makes a direct request to a Data Holder for their CDR Data. The Data Holder releases that CDR Data in human-readable form directly to the CDR Consumer.

Relevant Diagram in Attachment 2:



STEP 1A – CDR CONSUMER DIRECTLY REQUESTS CDR DATA FROM DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**CDR Consumers do not understand the different access rights available to them under the CDR regime** CDR Consumers may be unaware that they can directly request the Data Holder to release their CDR Data to them.	Data Holders must have an available CDR Policy which informs CDR Consumers about the management of their CDR Data. The Information Commissioner may approve a form for a CDR Policy (Rule 7.2(1)). The policy is to be available to CDR Consumers using specified mechanisms.	We query whether the provision of a CDR Policy is likely to be sufficient. It is important that CDR Consumers understand their available options (see **Recommendation 2**), but noting our additional comments about the limitations of consumer education.

STEP 1A – CDR CONSUMER DIRECTLY REQUESTS CDR DATA FROM DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
2.	**Form of CDR Data** CDR Data is provided by the Data Holder in a form that cannot be used by the CDR Consumer.	The CDR Data must, in accordance with Rule 1.13(1)(a)(iii), be provided in human-readable form. CDR Data must be provided in accordance with the Draft Data Standards (Rule 3.4(3)).	
3.	**CDR Consumer provides CDR Data to a third party outside the CDR regime** If the CDR Consumer provides their CDR Data that it has received from a Data Holder, to a third party, the privacy protections afforded to that CDR Data under the CDR regime will not apply. Third parties may try to circumvent the privacy protections of the CDR regime by requiring CDR Consumers to elicit CDR Data directly from Data Holders.	The Privacy Act, including the requirements of APP 11, will apply in relation to personal information held by Data Holders who are APP entities. (We have noted some stakeholders' concerns about the adequacy of the level of protection under the APPs.) The CDR Data will be provided in human-readable form as opposed to machine-readable form. There appears to be some debate amongst stakeholders as to whether this represents a mitigation strategy designed to protect CDR Consumers if they then choose to provide their CDR Data to a third party outside the CDR regime. Some stakeholders indicated that any such protection is somewhat illusory, given technologies available to translate human-readable data into machine-readable form. However, others considered that because human-readable data will not be as structured and able to be manipulated as machine-readable data, it will not be as "useful" to those third parties compared	The protections afforded in the APPs will only apply to CDR Consumers where the third party is an APP entity. CDR Data may have a lower level of protection when received by a third party, than when the same information is held by a Data Holder or Accredited Data Recipient. There is no requirement for CDR Consumers to be "warned" that the protections of the CDR regime (and possibly the APPs) will not apply if they share the CDR Data provided with a third party. We note the view of some stakeholders that a warning by itself is unlikely to be sufficient, stating that a "*warning may very well prevent a large proportion of people from engaging in risky behaviour but it will be the vulnerable consumer, the consumer experiencing financial hardship that will be most at risk under the CDR regime as currently designed*" (Submission by the Financial Rights Legal Centre). Stakeholders

STEP 1A – CDR CONSUMER DIRECTLY REQUESTS CDR DATA FROM DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		to CDR Data which was sought by an Accredited Data Recipient.	suggested that additional strategies should be employed to address this risk which would provide "*more effective interventions to guide consumers away from sharing information with third parties outside the CDR regime*" (Submission by the Australian Privacy Foundation), including: • amending the Privacy Act and the APPs; • requiring any entity handling CDR Data (including Data Holders) to be accredited in a similar manner to accreditation of Accredited Data Recipients; • ensuring third party recipients have clear obligations about the handling of CDR Data they receive by, for example, extending the application of the Privacy Safeguards to apply to third party data recipients of CDR Data; and/or • banning screen-scraping and similar unsafe data access, transfer and handling technologies. It seems likely that legislative reforms would be required to employ such additional strategies (noting our comments in paragraph 26.6 above). We consider that it is important that CDR Consumers understand their available options (see **Recommendation 2**), but note our

STEP 1A – CDR CONSUMER DIRECTLY REQUESTS CDR DATA FROM DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			additional comments about the limitations of consumer education. Accordingly, we suggest that the ACCC should consider whether the Draft Rules should require a Data Holder to provide information to a CDR Consumer when disclosing their CDR Data pursuant to their consumer data request (see **Recommendation 3**). In determining its response to this recommendation, the Department may wish to consider the following: • Although most stakeholders supported this **Recommendation 3**, we note the view of one stakeholder [FinTech Australia], that such an additional warning is unnecessary and likely to lead to greater consumer confusion, as there are number of disclosures, prompts and warnings, and this could instead mislead to the consumer thinking they are engaging in "high risk behaviour". • Another stakeholder [the Australian Banking Association] noted that if this part of **Recommendation 3** is implemented, guidance and examples from the OAIC on what form such disclosures (or warnings) will take should be provided. We agree that this would be useful.

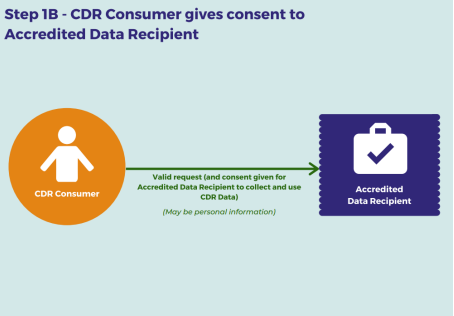
STEP 1A – CDR CONSUMER DIRECTLY REQUESTS CDR DATA FROM DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			• We also understand that the Data Standards Body is considering whether additional controls are required when specifying standards in relation to data being in "human readable form". We would support including this consideration of the ability to translate human-readable data into machine-readable form.

Step 1B. CDR Consumer gives consent to Accredited Data Recipient

Summary of step:

CDR Consumer gives consent to Accredited Data Recipient to collect CDR Data on their behalf for the use of a specific product or service.

Relevant Diagram in Attachment 2:



STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**Consent given by CDR Consumers is not voluntary** There is a risk that a CDR Consumer gives consent that is not voluntarily provided (for example, because it is effectively a requirement by the Accredited Data Recipient for provision of its goods and services).	Division 4.3 of the Draft Rules is designed to ensure that consent given by a CDR Consumer to use CDR Data is voluntary and express. For example, Rule 4.11(1)(c) requires the CDR Consumer's express consent (so that it cannot be inferred or implied).	Although most stakeholders did not disagree with this risk, a view was expressed that this is a theoretical risk, and "*in the absence of fraud or duress, it is difficult to see how such consent could be regarded as not having been provided voluntarily*" (Submission by FinTech Australia). Nevertheless, we consider that this remains a legitimate risk for consumers who may feel pressured to provide their consent.

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
2.	**CDR Consumers are asked to provide consent which is too broad to be a valid consent** There is a risk that CDR Consumers will be asked to consent to broad uses of their CDR Data, which are not sufficiently specific (e.g. a consent to use the CDR Data *"for our business purposes"*). There is a risk that CDR Consumers will be asked to provide consent that will allow their CDR Data to be on-sold in an identifiable form or used to create a profile of someone else. There is a risk that CDR Consumers will not be adequately informed about the specific purpose(s) for which their CDR Data will be collected and used.	Division 4.3 of the Draft Rules are designed to ensure that consents provided by CDR Consumers are "specific as to purpose" (Rule 4.9 (d)), and "informed" (Rule 4.9(c)). An Accredited Data Recipient may only ask a CDR Consumer for consent to collect and use their CDR Data where the CDR Consumer has requested the Accredited Data Recipient to provide goods and services, and access to their CDR Data is needed in order to provide those goods and services (Rule 4.3). This is also contained in Rule 4.12(2), in that consent cannot be asked for unless it would comply with the data minimisation principle. The Draft Rules contain protections in the processes that an Accredited Data Recipient must use to ask a CDR Consumer for consent (Rule 4.10). These include that the processes must comply with the Draft Data Standards, and that the Accredited Data Recipient must have regard to any CX Guidelines developed by the Data Standards Body, in order to be as easy to understand as practicable. This reflects the extensive consumer research that has been conducted by the Data Standards Body for the CDR regime about the ways in which consumers understand consent, and how it can be made accessible and easy to comprehend.	Although an Accredited Data Recipient is required to "have regard" to the CX Guidelines, the CX Guidelines themselves are not binding upon Accredited Data Recipients (as they are not incorporated as part of the Draft Rules or binding Draft Data Standards). It may be unclear to Accredited Data Recipients what they must do in order to comply with the requirements of Rule 4.10(a)(ii). In our view, implementation of **Recommendation 2** will assist in mitigating this risk, but the ACCC may wish to consider whether the Draft Rules will provide sufficient clarity on this aspect and will allow the regulators to take action if broad consents are sought by Accredited Data Recipients.

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		For example, the CX Guidelines suggest that the consent flow should provide CDR Consumers with a 'Product value proposition' before asking for consent. This is intended to provide CDR Consumers with the opportunity to fully understand the 'specific purpose' for which their CDR Data will be used. Consents may not be bundled or other documents included or referenced so as to reduce comprehensibility (Rule 4.10(b)). When asking for consent, an Accredited Data Recipient must allow the CDR Consumer to actively select or otherwise clearly indicate the specific uses for which they consent (Rules 4.11(1)(a)(ii) and 4.11(1)(c)(ii)). The Accredited Data recipient must not present pre-selected options to the CDR Consumer (Rule 4.11(2)). Further, if an Accredited Data Recipient asks CDR Consumers to provide their consents to allow their CDR Data to be on-sold in an identifiable form or used to create a profile of someone else, this will be in contravention of Rules 4.12(3) and 4.12(3)(b), which will assist in mitigating against this risk.	
3.	**A CDR Consumer does not have legal capacity to provide a valid consent**	Only *eligible CDR Consumers* will be able to make consumer data requests. For the initial implementation, the CDR regime will only apply to an individual CDR Consumer if he or she is over	

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	There is a risk that consent will be provided by CDR Consumers who do not have legal capacity to consent.	18 years of age (avoiding the need to assess whether children may provide valid consent). Similarly, eligible CDR Consumers in the initial implementation will only include CDR Consumers who have an account with the Data Holder which is open and that they are able to access online (i.e. using an internet browser or mobile phone application). This will effectively require the CDR Consumer to have the legal and mental capacity to have and operate the relevant account (avoiding the need to assess their capacity).	
4.	**The CDR Consumer is not adequately informed before giving consent** There is a risk that consent will be provided by CDR Consumers who are not adequately informed before giving consent.	Division 4.3 of the Draft Rules are designed to ensure that consents provided by CDR Consumers are "informed" (Rule 4.9(c)). This is reflected in Rule 4.11(3), which sets out a comprehensive list of specific information that must be given to CDR Consumers when asking for their consent. As discussed above, Accredited Data Recipients must make the consents "as easy to understand as practicable", including by using concise language and potentially visual aids (Rule 4.10).	It is not easy to identify which of the Draft Data Standards[53] (if any) would assist in ensuring that CDR Consumers are adequately informed and are binding upon Accredited Data Recipients. The CX Guidelines are not binding upon Accredited Data Recipients (as they are not incorporated as part of the Draft Rules or binding Draft Data Standards).[54] However, Accredited Data Recipients must, when asking for consent, have regard to the CX Guidelines so as to ensure that its consent process is as

[53] We understand that the new version of the Draft Data Standards subsequently been published by the Data Standards Body (version 1.0.0), may address some of the issues raised for this risk, but as it was published after the "point in time" established for the conduct of this PIA, these have not been detailed in this PIA report.
[54] Although we have not considered versions of the Draft Data Standards published after the "point in time" for this PIA, we understand that some aspects of the CX Guidelines have subsequently been included as binding requirements in the further version of the Draft Data Standards (for example, requirements for accessibility of content).

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		The Data Standards Body has conducted consumer research into matters concerning vulnerable CDR Consumers to ensure that genuine consent is obtained. The consumer research and the CX Guidelines contain some guidance about making the consent process comprehensible for vulnerable consumers. The CX Guidelines refer to aspects of consent requirements as "mandatory" (e.g. of the Web Content Accessibility Guidelines (WCAG) which address accessibility and readability of web content; and data language standards that must be used when asking consumers for consent, including the permission language that must be used to obtain consent).	easy to understand as practicable (Rule 4.10(a)(ii)). We have recommended that the Draft Data Standards be recast into language that will allow CDR Participants to easily distinguish which parts of the Draft Data Standards are binding legal requirements. In addition, we suggest that there needs to be adequately detailed version control (which appears to be currently absent) to allow for easy identification of any changes to the Draft Data Standards. This is because otherwise there is a risk that the Draft Data Standards will not be implemented consistently by all CDR Participants (see **Recommendation 5**). The majority of stakeholders who provided submissions strongly agreed with this **Recommendation 5**. Some stakeholders went further, suggesting that that the Draft Data Standards should *only* contain binding requirements. For example, Legal Aid Queensland submitted that it does "*not support a two-tiered system of enforceability for Data Standards. The Data Standards in their entirety should be enforceable otherwise there will be little incentive for the industry to comply with non-binding obligations. If, however, some Data Standards are recast as non-legally binding they should be clearly articulated as such with clear statements as to*

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			the effect and limitations of a non-binding standard." The Financial Rights Legal Centre also stated that "*This distinction between binding and non-binding [standards] inevitably will lead to regulatory arbitrage and provide significant scope to industry stakeholders to design interfaces that serve themselves well, and serve consumers poorly. We therefore recommend that rather than merely distinguishing between binding and non-binding requirements – that all guidelines be binding and enforceable.*" Many stakeholders also requested further clarity around the status of the CX Guidelines, with many stating that they should also be binding, because currently "*references to screen-reader accessibility remain solely within the CX Guidelines*" and as such "*remain suggestions rather than mandatory"* (Submission by the Australian Communications Consumer Action Network). One stakeholder stated that as "*uncertainty in the Data Standards will lead to increased costs and complexity of developing systems*", it supports "*the Data Standards being written in an industry standard format, as this would facilitate efficient parsing of the scheme and end-points"* (Submission by FinTech Australia).

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			We suggest that the Data Standards Body should be asked to also consider these views. Finally, we note the view of one stakeholder [the Australian Retail Credit Association] that the ACCC should consider developing standardised consents that Accredited Data Recipients must provide to CDR Consumers, and this should be done in consultation with industry and relevant stakeholders. We consider that there may be merit in the suggestion of developing standard consents for specific situations, which Accredited Data Recipients could choose to use if they wished, as this would provide a level of certainty that the form of consent meets the requirements of the CDR legislative framework.
5.	**Consent is not sufficiently current to be a valid consent** There is a risk that consent will be provided by CDR Consumers that is not sufficiently current.	The maximum duration of a consent provided by a CDR Consumer is 12 months (after which time the consent will expire and must be re-obtained if the Accredited Data Recipient wishes to continue to collect and/or use the CDR Data) (Rule 4.12(1)).	
6.	**The CDR Consumer is not aware of the consent(s) they have provided**	The Accredited Data Recipient is required to provide CDR Consumers with a *"CDR receipt"*, as soon as practicable after they have given consent to an Accredited Data Recipient collecting their	The Draft Rules do not require the CDR receipt to provide advice about what the CDR Consumer should do if the consent(s) recorded do not match their understanding of the

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	There is a risk that CDR Consumers are not aware of the consent(s) they have provided.	CDR Data (Rule 4.18). The CDR receipt must set out information about the consent, and be provided other than through the Consumer Dashboard. The CDR receipt should assist CDR Consumers to identify if consent has been provided fraudulently or errors have been made. The Accredited Data Recipient is also required to make available a Consumer Dashboard which includes details about consents provided, and update this to reflect expiry of consents.	consent(s) that have been given, nor do the Draft Rules require the CDR receipt to provide information on what the consequences are (e.g. whether the consent is then rendered void). The ACCC may wish to consider whether this level of detail should be specified in the Draft Rules (see **Recommendation 3**).
7.	**Genuine consent is not obtained from vulnerable CDR Consumers** There is a risk that vulnerable cohorts of CDR Consumers may not be able to engage with the consent processes (e.g. individuals for whom English is a second language).	Accredited Data Recipients must make the consents "as easy to understand as is practicable", with the ability to use aids to enhance comprehensibility, and are prohibited from including documents that reduce comprehensibility (Rule 4.10). The Data Standards Body has conducted consumer research into matters concerning vulnerable CDR Consumers to ensure that genuine consent is obtained. This consumer research has involved consultation with vulnerable consumers, including people with accessibility needs, varying levels of English, digital, and financial literacy, and a range of other characteristics/experiences. The CX Guidelines contain some guidance about making the consent process comprehensible for vulnerable consumers. This includes:	The CX Guidelines are not binding upon Accredited Data Recipients (as they are not incorporated as part of the Draft Rules or binding Draft Data Standards). We have recommended that the Draft Data Standards be recast into language that will allow CDR Participants to easily distinguish which parts of the Draft Data Standards are binding legal requirements (see **Recommendation 5**). The Data Standards Body has noted that further consultation/research with vulnerable consumers and advocacy groups would be valuable, and that it has also considered approaches such as "visual aids" (including "comic contracts") to address English literacy issues.

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		• "Mandatory" Accessibility guidance for all of the WCAG-based accessibility guidelines and considerations (see page 22). • "Recommended" guidance 2.4.2 which says "CDR information should have full translation functionality and be fully screen-reader accessible". However, we note that the Data Standards Body is not planning to provide translations for consent language (see page 40).	

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
8.	**Non-accredited persons pose as Accredited Data Recipients to obtain CDR Data** CDR Consumers may be 'lured' to give consent to collection of their CDR Data by non-accredited persons posing as Accredited Data Recipients.	It is an offence for a person to hold out that it is an accredited person if it is not (section 56CC in the CDR Act). It is a civil penalty provision for a person to solicit CDR Data from a CDR Consumer unless the CDR Consumer has provided a valid request under the Draft Rules. A valid request can only be made directly to a Data Holder or by an Accredited Data Recipient. Additionally, a Data Holder will need to confirm the accreditation and identity of the Accredited Data Recipient with the Accreditation Register before sending CDR Data to the Accredited Data Recipient in accordance with the Draft Data Standards (with identity verification providing some protection against provision of CDR Data to non-accredited persons).	We note the view of one stakeholder [the Australian Banking Association] that the ACCC (and the Department, and perhaps Accredited Data Recipients) should provide consumer education to CDR Consumers on how to identify genuine Accredited Data Recipients. While this seems to us to be a worthy endeavour, we suspect that consumer education by itself is unlikely to be sufficient. We consider that an effective monitoring and enforcement regime will be of more use in reducing the likelihood of the inappropriate behaviour, than any requirement for consumer education.
9.	**Joint account holders** There is a risk that where there are joint account holders: • one account holder may be forced into giving the other account holder control over the CDR Data; or	For the initial implementation of the CDR regime in the banking Sector, joint accounts have special conditions in Part 4 of Schedule 3 to the Draft Rules. Generally, before CDR Data that relates to a joint account can be disclosed under the CDR regime, joint account holders must have jointly elected that each individual account holder can make requests for information that relates to the joint account (and provide or withdraw authorisations	We recognise that the treatment of joint accounts needs to be considered in the light of the need to balance privacy protections of individual joint account holders with other policy considerations (such as the need to protect victims of family violence). We note that there is no ability for the Data Holder or Accredited Data Recipient to apply an exception to the general rules for joint account holders to *permit* the release of CDR Data for

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	• one account holder may not want the other account holder to know of their request for CDR Data (for example, in instances of family violence).	for such requests), but that each joint account holder can revoke such an election. This ensures that the privacy of one joint account holder is not compromised by disclosure of their joint data to another joint account holder. However, Rule 7.9 of the Draft Rules (notifying about disclosure of CDR Data) does not apply if the Data Holder considers this is necessary to prevent physical or financial harm or abuse. In addition, a Data Holder can refuse to disclose CDR Data generally if it considers this necessary to prevent physical or financial harm or abuse (Rule 4.7)(1)(b)).	joint account holders. For example, exceptions may be needed if the Data Holder or Accredited Data Recipient is aware that there are circumstances in which it is not safe or possible for a joint account holder to obtain the election or consent from the other joint account holder, but the joint account holder needs the CDR Data in order to escape from family violence. We understand that many of the initial Data Holders already have procedures and policies in place for dealing with such situations, however these are not reflected in the legislative framework. We understand that the ACCC has undertaken extensive consultation with stakeholders involved in preventing family violence in preparing the Draft Rules, but we recommend that the ACCC satisfy itself that the Draft Rules represent an appropriate balance in the circumstances (see **Recommendation 6**). The majority of stakeholders who provided submissions broadly agreed with this **Recommendation 6** and agreed that the Department should carefully consider the application of the CDR legislative framework in relation to joint account holders. Several stakeholders requested further guidance about how Data Holders should deal with joint account holders, especially those in vulnerable circumstances. Several asked for

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			specific guidance about the level of evidence required for a conclusion that there was a risk of 'physical or financial harm or abuse'. For example, Legal Aid Queensland submitted that "*it is unclear what evidence the Data Holder requires to come to a view that in order to prevent physical or financial harm or abuse, they will not update the joint account holder's Consumer Dashboard"* (as provided for in Rule 4.6(b)). Further, it submitted that such evidential requirements should not be onerous, and that it is "*important that consistent criteria are developed to ensure there is a balance between those circumstances where there is a need for disclosure to potential victims and other circumstances where there should be non-disclosure to perpetrators of domestic violence.*" Another stakeholder made a similar submission, stating that "*there is little guidance on the level of evidence required for the Data Holder or Accredited Data Recipient to not update the joint account holder's Consumer Dashboard"* (Submission by the Financial Rights Legal Centre). It also expressed concern about the inclusion of a physical address of CDR Consumers in the CDR Data. Several stakeholders appeared to indicate a view that the current treatment of joint account holders under the Draft Rules should not yet be treated as settled. For example, the Australian Retail Credit Association suggested that "*consideration [should] be given to changing the*

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			current fundamental approach to joint account holders. That is, consideration should be given to allowing a joint account holder to authorise the sharing of the CDR Data without the consent or knowledge of the other joint account holder." Another stakeholder submitted that there "*must be a balance between protecting and empowering people*". It submitted that if one joint account holder changes their consent and election provided in accordance with the Draft Rules, in cases of domestic abuse, the other joint account holder should not be notified on this change. As discussed above, there is no ability for CDR Participants to apply an exception to the general rules for joint account holders to permit the release of CDR Data for joint account holders. This stakeholder supported this observation, and submitted that there "*should be an ability to permit the release of CDR Data for a joint account [holder] in circumstances where the person seeking the data is a person experiencing domestic abuse*" (Submission by the Redfern Legal Centre). Further, it submitted that there is a risk that in domestic violence situations, perpetrators of domestic violence may access their victim's Consumer Dashboard to manage and control their consents and authorisations (and inflict financial abuse) using the personal identification information they know about the victim (such as

STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			banking credentials, phone number, email address etc.). The Australian Privacy Foundation submitted that "*to ensure privacy rights are safeguarded, joint account data should not be portable unless consent is obtained from both account holders…the disclosure of personal information without consent could be challenged at law. Even if that challenge is not successful, the provision of that data to a third party without consent remains a serious breach of privacy.*" This stakeholder submitted that our previous draft of **Recommendation 6** did not go far enough, and that, given the complexities and sensitivities surrounding the issue of joint account holders, the CDR regime should not apply to joint account holders at all until all policy considerations have been fully and properly considered. We have recommended that the Department consider issuing a public statement explaining how the competing privacy and policy issues in relation to the treatment of joint account holders were considered and balanced (see **Recommendation 6**). This may go some way to alleviating stakeholders' concerns. Alternatively, the Department may wish to consider whether the CDR regime should initially not apply to joint account holders at all, until such time as the policy considerations have been fully considered and balanced.

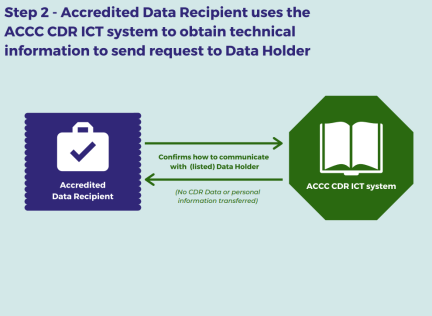
STEP 1B – CDR CONSUMER GIVES CONSENT TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			We do support the view of Australian Communications Consumer Action Network, which submitted that the Department should continue to have discussions with domestic and family violence specialists when considering issues such as joint account holders.
10.	**Collection of personal information** We understand that in this Step 1B, Accredited Data Recipients will collect personal information from the CDR Consumer (this will occur when the CDR Consumer provides the Accredited Data Recipient with details to create a user ID and password). There may be a risk that the Accredited Data Recipient does not handle this personal information in accordance with the APPs under the Privacy Act.	If Accredited Data Recipients are APP entities, then the APPs will apply to the personal information they collect from CDR Consumers. 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.	

Step 2. Accredited Data Recipient uses the ACCC CDR ICT system to obtain technical information to send request to Data Holder

Summary of step:

Before the Accredited Data Recipient makes a request to a Data Holder for the provision of CDR Data from the Data Holder, the Accredited Data Recipient will obtain from the ACCC's CDR ICT system the technical information required to subsequently make requests to that Data Holder.[55]

Relevant Diagram in Attachment 2:



STEP 2 – ACCREDITED DATA RECIPIENT USES ACCC CDR ICT SYSTEM			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**The Data Holder does not seek listing and undertake the ICT testing regime** The Accreditation Registrar must maintain a database with a list of Data Holders and associated information (Rule 5.25(1)). Data Holders must, if requested by the Accreditation Registrar, provide the requested	Data Holders are required to have both a direct request service, and an accredited data recipient request service. Data Holders are required to receive consumer data requests, and to provide requested CDR Data, in compliance with the Draft Data Standards.	The Draft Rules do not specify that Data Holders must proactively identify themselves to the Accreditation Registrar for listing, or undergo any testing regime to ensure compliance with the Draft Data Standards (see **Recommendation 3**).

[55] We understand that, technically, the Accredited Data Recipient obtains information from the ACCC's broader ICT system for the CDR regime which enables it to register its software product with the Data Holder, and it is this registration that will subsequently allow requests to be made to the Data Holder. The Draft Data Standards will contain requirements about this process and the storage and use of the technical information received from the ACCC's CDR ICT system.

STEP 2 – ACCREDITED DATA RECIPIENT USES ACCC CDR ICT SYSTEM			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	information for inclusion in the database. However, there is currently no obligation on Data Holders to actively seek such listing and undergo any testing for compliance with the Draft Data Standards or compatibility with the ACCC's broader CDR ICT system, in order to facilitate CDR Consumer requests through an Accredited Data Recipient. If a Data Holder does not undertake the listing and ICT testing regime, there is a risk that CDR Consumers will not be able to access their CDR Data as contemplated by the legislative framework.		
2.	**Pathway security between the Accredited Data Recipient and ACCC CDR ICT system is compromised** There is a risk that the pathways used by the Accredited Data Recipient to communicate with the ACCC	The Draft Data Standards include requirements in relation to an Information Security Profile. API technical conformance testing will ensure systems can communicate securely in accordance with the Draft Data Standards. We understand that PKIs will be used to authenticate the identities of the Accredited Data Recipients for communications.	

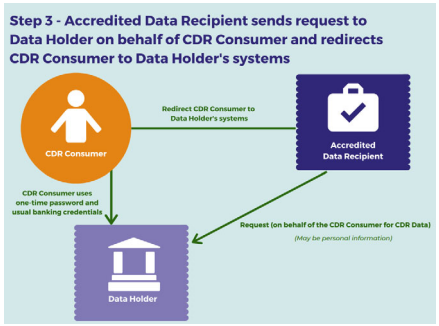
STEP 2 – ACCREDITED DATA RECIPIENT USES ACCC CDR ICT SYSTEM			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	CDR ICT system could be compromised.	The contract for the design and build of the ACCC CDR ICT system contains requirements for it to comply with minimum security and privacy requirements (including the Draft Data Standards). No CDR Data will be transferred between the Accredited Data Recipient and the ACCC CDR ICT system during any Step in the CDR regime, including this Step 2.	

Step 3. Accredited Data Recipient sends request to Data Holder on behalf of CDR Consumer and redirects CDR Consumer to the Data Holder's systems

Summary of step:

The Accredited Data Recipient sends a request for CDR Data to the Data Holder on behalf of the CDR Consumer. The Accredited Data Recipient then redirects the CDR Consumer to the Data Holder's systems using a one-time password provided to the CDR Consumer. The CDR Consumer is authenticated by the Data Holder (using its usual authentication processes).

Relevant Diagram in Attachment 2:



STEP 3 – ACCREDITED DATA RECIPIENT SENDS REQUEST TO DATA HOLDER ON BEHALF OF CDR CONSUMER

No.	Risk	Existing mitigation strategies	Gap analysis and Recommendations
1.	**Malicious attacks** There is a risk of malicious attacks occurring as part of CDR Consumer redirection to Data Holder systems, resulting in theft of information about the CDR Consumer. A redirection is also inherently counter to traditional consumer education programs in relation to the banking Sector (including, for example, education in regards to not clicking on foreign/unknown	Using existing banking credentials for a redirected Data Holder's page would go against consumer education currently provided by the banking Sector to consumers, and increase risks of CDR Consumers ignoring the consumer education in other circumstances and therefore exposing themselves to risk of malicious attacks. The implementation of a one-time password (provided to the CDR Consumer through an alternative contact point, e.g. via mobile phone) is designed to address this risk and increase confidence that the re-direction is valid. This will reduce (but cannot eliminate) the risk of malicious attacks. Further, the Data Holder will only authenticate the identity of the CDR Consumer using one aspect of their usual banking credentials (their customer	The CX Guidelines are not binding upon CDR Participants (as they are not incorporated as part of the Draft Rules or binding Draft Data Standards). We have recommended that the Draft Data Standards be recast into language that will allow CDR Participants to easily distinguish which parts of the Draft Data Standards are binding legal requirements (see **Recommendation 5**).

STEP 3 – ACCREDITED DATA RECIPIENT SENDS REQUEST TO DATA HOLDER ON BEHALF OF CDR CONSUMER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	links or entering passwords into such links).	number, which may, for some CDR Consumers, be one of their bank account numbers). The CDR Consumer will not be asked for (or provide) their usual banking password, but must enter the one-time password issued by their Data Holder. The CX Guidelines provide "mandatory" guidelines for the CDR Consumer authentication stage, including prohibiting Data Holders from including a forgotten password link in the redirect screen (Component 3.1.1 of the CX Guidelines). Component 3.2 and 3.3 of the CX Guidelines also outline "mandatory" guidelines for the one time password. There is also a "mandatory" guideline in component 3.1.2 that consumer education material consistently emphasise the message that consumers should never enter their banking password except in their bank's website or mobile app. We understand that the ACCC also intends to implement consumer education about this message. Other specific points in the CX Guidelines that we understand are intended to assist include a "recommended" guideline 2.3.1 (p. 38) about inclusion of ACCC-provided trust mark, and an -ability for CDR Consumers to verify accreditation of their Accredited Data Recipient (possibly through an accreditation identity verified on the ACCC list).	

STEP 3 – ACCREDITED DATA RECIPIENT SENDS REQUEST TO DATA HOLDER ON BEHALF OF CDR CONSUMER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
2.	**Data Holder refuses to accept the request** There is a risk that Data Holders may not grant access to CDR Data, citing security or other concerns. The CDR Consumer may not be given a proper explanation for why the Accredited Data Recipient was not granted access.	The Draft Rules and the Draft Data Standards provide the instances where a Data Holder can refuse a request. The Draft Rules provide that a Data Holder may refuse to disclose CDR Data in response to a valid request, if the Data Holder considers that refusal is necessary to prevent physical or financial harm or abuse, there are reasonable grounds to believe that disclosure would adversely impact the security, integrity or stability of the Accreditation Register or the Data Holder's ICT systems, or the circumstances permitted by the Draft Data Standards (Rule 4.7). The Draft Data Standards provide for refusal to be given in certain circumstances, including during periods of time when the digital channels for the Data Holder are the target for a distributed denial of service or equivalent form of attack, or there is a significant increase in traffic from a poorly designed or misbehaving Accredited Data Recipient. If a request is refused, the Data Holder must notify the Accredited Data Recipient in accordance with the Draft Data Standards. We understand that these mean that an error code will be sent back, but these error messages may not identify the precise reasons as to why the request has been rejected.	There does not appear to be any requirement for CDR Consumers to be notified of reasons why a request for CDR Data was refused. We understand that the ACCC has considered whether CDR Consumers should be told why their request has been refused. We understand that the approach in the Draft Rules has been adopted because it was considered that, if the Draft Rules provided that CDR Consumers should be generally told the reason why their request was refused, except in limited circumstances (for example, in family violence situations), this would potentially allow perpetrators of family violence to conclude, by deduction, the reason for any refusal of their request, which could itself potentially result in harm to their victims. The ACCC has advised that it balanced this risk against full transparency and also took into account the relatively well-established mechanisms in the banking Sector for dealing with family violence situations. One stakeholder [Redfern Legal Centre] submitted that if a request is refused on the grounds of physical or financial harm or abuse, the Draft Rules should expressly state that the grounds for refusal must not be provided to CDR Consumers, because of the potential for serious harm. While we consider that this may have merit, we also think that the risk could be addressed by the issuing of appropriate

STEP 3 – ACCREDITED DATA RECIPIENT SENDS REQUEST TO DATA HOLDER ON BEHALF OF CDR CONSUMER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			guidance for Data Holders and Accredited Data Recipients, about the potential for disclosure of the reasons for refusal to provide CDR Data to impact on those suffering financial or physical harm or abuse (see **Recommendation 2**).
3.	**Pathway security between the Accredited Data Recipient and Data Holder is compromised** There is a risk that the pathways used by the Accredited Data Recipient to communicate with the Data Holder could be compromised.	The Draft Data Standards include requirements in relation to an Information Security Profile. API technical conformance testing will ensure systems can communicate securely in accordance with the Draft Data Standards. We understand that PKIs will be used to authenticate the identities of the Data Holder and Accredited Data Recipients for communications. The contract for the design and build of the ACCC CDR ICT system contains requirements for it to comply with minimum security and privacy requirements (including the Draft Data Standards). Data will be encrypted during transit.	The Draft Rules do not specify that Data Holders must proactively identify themselves to the Accreditation Registrar for listing, or undergo any testing regime to ensure compliance with the Draft Data Standards (see **Recommendation 3**).[56]

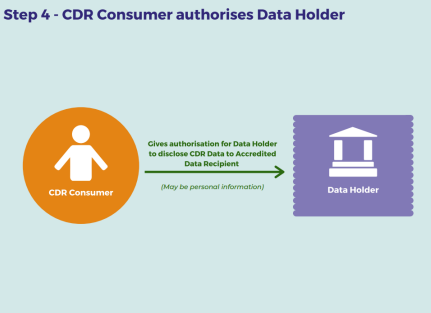
[56] We note that the functions of the Accreditation Registrar include maintaining the security, integrity and stability of the Accreditation Register, including undertaking or facilitating any testing for that purpose (Rule 5.30). The Accreditation Registrar also has powers to request a Data Holder to provide information to the Accreditation Registrar (Rule 5.25(2) or to do a specified thing in order to ensure the security, integrity and stability of the Accreditation Register (Rule 5.31). These rely on a request being issued by the Accreditation Registrar.

Step 4. CDR Consumer authorises Data Holder

Summary of step:

The CDR Consumer authorises the Data Holder to release their CDR Data to the Accredited Data Recipient.

Relevant Diagram in Attachment 2:



STEP 4 – CDR CONSUMER AUTHORISES DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**Authorisation does not match initial consent provided by the CDR Consumer** There is a risk that the authorisation provided by the CDR Consumer to the Data Holder will not match the consent the CDR Consumer originally gave to the Accredited Data Recipient.	The Draft Data Standards provide the technical specifications for the CDR Participants to communicate through the technical data flows. This will effectively ensure that the consent for collection given by the CDR Consumer to the Accredited Data Recipient will match the request for authorisation which is given to the CDR Consumer by the Data Holder.	

STEP 4 – CDR CONSUMER AUTHORISES DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
2.	**The authorisation provided by the CDR Consumer is not genuine** *[Please see risks identified in Step 1B relation to the provision of consent, which also apply to the provision of authorisation.]*	Authorisation must be given in accordance with Division 4.4 of the Draft Rules, and in accordance with the Draft Data Standards (Rule 4.5(2)). These include similar protections as for seeking consent. *[Please see analysis at Step 1B in relation to the provision of consent – similar mitigation strategies are included in the Draft Rules for authorisation.]* Further, Rule 4.23 requires the Data Holder to provide the CDR Consumer with information about the authorisation, including the name of the Accredited Data Recipient who has made the request to the Data Holder, the period of time relating to the request for the CDR Data by the Accredited Data Recipient, the types of CDR Data to be disclosed and if the authorisation is being sought for the disclosure of CDR Data on a single occasion or over a period of time. Some of this information repeats the information that the CDR Consumer must receive from Accredited Data Recipients when they seek consent under Division 4.3 of the Draft Rules. This provides additional assurance that the consent provided by the CDR Consumer aligns with the information that the Accredited Data Recipient has requested from the Data Holder. Rule 4.24 also prohibit the Data Holder from providing or requesting additional information from the CDR Consumer, or offering additional or	The consumer research did not appear to place as much emphasis on the authorisation component compared to the initial consent component of the information flow (e.g. to analyse if there are any differences between these components). In the CX Guidelines, the requirements for authorisation are listed as “recommended” rather than “mandatory”. (See the discussion in relation to Step 1B, Risk 4).

STEP 4 – CDR CONSUMER AUTHORISES DATA HOLDER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		alternative services, as part of seeking authorisation.	

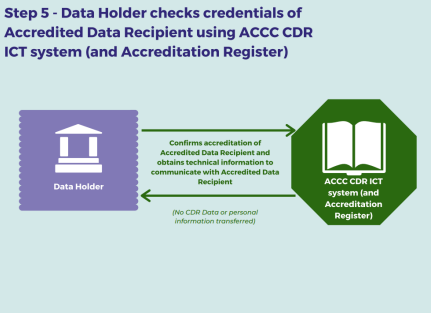
Step 5. Data Holder checks credentials of Accredited Data Recipient using ACCC CDR ICT system (and Accreditation Register)

Summary of step:

The Data Holder confirms with the Accreditation Register that the Accredited Data Recipient that has requested a CDR Consumer's CDR Data is accredited,[57] and obtains from the ACCC's broader ICT system for the CDR regime other technical information required to transfer the CDR Data to the Accredited Data Recipient.[58]

For technical reasons and in accordance with the Draft Data Standards, elements of this Step 5 may occur immediately after, or as part of, Step 2.

Relevant Diagram in Attachment 2:



STEP 5 – DATA HOLDER CONFIRMS CREDENTIALS OF ACCREDITED DATA RECIPIENT USING ACCC CDR ICT SYSTEM (AND ACCREDITATION REGISTER)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**CDR Data is transferred to a non-accredited person** There is a risk that the Data Holder will not verify the accreditation status of the Accredited Data Recipient.	All Accredited Data Recipients are required to be registered under the legislative framework, and be included on the Accreditation Register. It is in the interests of Data Holders to check that an Accredited Data Recipient is accredited (in order to comply with the requirements of the CDR legislative framework for disclosure). The ACCC's ICT system has been designed so that a Data Holder's ICT system can obtain up to date	Although not directly related to this risk, one stakeholder [the Australian Banking Association] did raise the issue that there is no mechanism in the Draft Rules for Data Holders to make complaints or raise concerns in relation to an accredited person (for example, if they believe that person may not be a "fit and proper person", as required for accreditation at the "unrestricted level"), or any ability of a Data Holder to withhold disclosure of .CDR Data to that person until the

[57] We understand that this Step 5 involves the Data Holder's system regularly checking cached information obtained from the ACCC's CDR ICT system. The Draft Data Standards will require cached information to be regularly refreshed from the ACCC's CDR ICT system many times a day.
[58] We understand that, technically, this occurs during the registration of the Accredited Data Recipient's software product.

STEP 5 – DATA HOLDER CONFIRMS CREDENTIALS OF ACCREDITED DATA RECIPIENT USING ACCC CDR ICT SYSTEM (AND ACCREDITATION REGISTER)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		information about the accreditation status of the Accredited Data Recipient before transferring CDR Data.	regulator has resolved those complaints or concerns. We note that the legislative framework for the CDR regime is based upon the Data Recipient Accreditor's assessment of a number of criteria, including that the Accredited Data Recipient is a "fit and proper person", with the ability to suspend or revoke an Accredited Data Recipient's accreditation if it considers that criterion is no longer met. In assessing the fit and proper person criteria in relation to it making a decision about accreditation, the Data Recipient Accreditor may take into account "any other relevant matter" (Rule 1.9(1)(g)), which may include any information provided by f a Data Holder. Further, the Data Recipient Accreditor has the ability to suspend, on urgent grounds, an Accredited Data Recipient's accreditation, and any information provided by a Data Holder may be relevant to an urgent suspension (Rule 5.21). Additionally, as provided for in Rule 4.7, a Data Holder can refuse to disclose CDR Data if it considers that refusal is necessary to prevent physical or financial harm or abuse, there are reasonable grounds to believe that disclosure would adversely impact the security, integrity or stability of the Accreditation Register or the Data

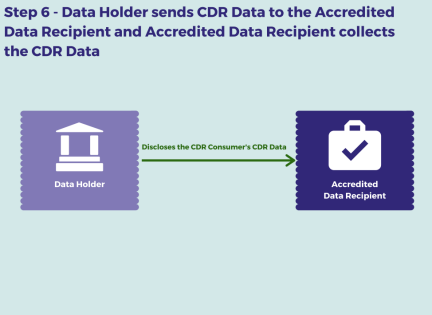
STEP 5 – DATA HOLDER CONFIRMS CREDENTIALS OF ACCREDITED DATA RECIPIENT USING ACCC CDR ICT SYSTEM (AND ACCREDITATION REGISTER)			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			Holder's ICT systems, or the circumstances permitted by the Draft Data Standards.
2.	**Pathway security between the Data Holder and the Accredited Data Recipient is compromised** As with Step 3, there is a risk that the pathways used by the Data Holder to communicate with the Data Holder could be compromised.	All Accredited Data Recipients are required to be registered. We understand that the accreditation process will involve a testing regime, to ensure conformance with the requirements of the Draft Data Standards (which include minimum security requirements). PS 12 will apply to Accredited Data Recipients, requiring the maintenance of minimum security requirements. Data will be encrypted during transit.	The Draft Rules do not clearly provide for a testing regime as part of the accreditation or listing process. PS 12 does not apply to Data Holders. See **Recommendation 3**, which recommends that the ACCC consider whether any process for testing a Data Holder's compliance with the Draft Data Standards should be included in the Draft Rules, and whether that process does, or should, include assessment of a Data Holder's security in relation to the transmission of CDR Data.

Step 6. Data Holder sends CDR Data to the Accredited Data Recipient (and Accredited Data Recipient collects that CDR Data)

Summary of step:

The Data Holder sends the CDR Consumer's CDR Data to the Accredited Data Recipient. The Accredited Data Recipient collects that CDR Data.

Relevant Diagram in Attachment 2:



STEP 6 – DATA HOLDER SENDS CDR DATA TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**Incorrect Accredited Data Recipient** There is a risk that CDR Data is sent to the incorrect Accredited Data Recipient.	PS 4 requires an Accredited Data Recipient that receives unsolicited CDR Data to destroy it as soon as practicable. Step 6 requires that Data Holders obtain technical information from the ACCC's CDR ICT system needed to send CDR Data to the Accredited Data Recipient. Further, we understand that the current design of the ACCC's CDR ICT system will involve an authentication process using PKIs to establish the identity of the correct Accredited Data Recipient.	

STEP 6 – DATA HOLDER SENDS CDR DATA TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
2.	**CDR Data is sent to a non-accredited person** There is a risk that the Data Holder sends CDR Data to a non-accredited person instead of the Accredited Data Recipient.	Step 6 requires that Data Holders obtain technical information from the ACCC's CDR ICT system needed to send CDR Data to the Accredited Data Recipient. Further, we understand that the current design of the ACCC's CDR ICT system will involve an authentication process using PKIs to establish the identity of the correct Accredited Data Recipient. If the CDR Data incorrectly provided is personal information, APP 4 will apply if the non-accredited person is an APP entity (requiring de-identification or destruction of the unsolicited information).	PS 4 only applies to accredited persons (not persons outside the CDR regime). APP 4 will only apply if the non-accredited person receiving the unsolicited data is an APP entity and the CDR Data is personal information. However, we understand that the technical measures that will be put in place mean that it is extremely unlikely that CDR Data will be sent to a non-accredited person in error.
3.	**Malicious attacks** CDR Data is intercepted by malicious attack during the transfer between the Data Holder and the Accredited Data Recipient.	The Draft Data Standards themselves contain requirements in relation to the transfer of CDR Data which protects the security of the transfer. PS 12 provides strict guidelines for the required security systems for the Accredited Data Recipient. Further, there is an obligation for CDR Consumers to be notified if there are any eligible data breaches in relation to their CDR Data (section 56ES in the CDR Act applies Part IIIC of the Privacy Act to an Accredited Data Recipient that holds a CDR Consumer's CDR Data). In order to become an accredited person, the accreditation applicant must have taken the steps	PS 12 only applies to Accredited Data Recipients (not Data Holders). However, if **Recommendation 3** is implemented, there will be further comfort that the Data Holders' security arrangements are sufficient.

STEP 6 – DATA HOLDER SENDS CDR DATA TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		outlined in Schedule 2 to the Draft Rules, which relate to protecting the CDR Data from misuse, interference and loss, and unauthorised access, modification and disclosure. The Draft Data Standards will require CDR Data to be encrypted during transit.	
4.	**System issues** Lack of system inter-operability or other technical issues prevents successful transfer of CDR Data (either not transferred at all, or transferred so that the CDR Data is incomplete and/or inaccurate upon receipt by the Accredited Data Recipient)	Both Data Holders and Accredited Data Recipients will have to undertake testing to ensure conformance with the Draft Data Standards (including requirements for APIs) before accreditation/being listed. The Draft Data Standards are designed to ensure appropriate and accurate transfer of the CDR Data. PS 11 requires that Data Holders and Accredited Data Recipients take reasonable steps to ensure that the CDR Data is accurate, up to date and complete. This is a civil penalty provision. PS 13 provides for correction of CDR Data by a Data Holder and Accredited Data Recipient.	The process for requiring testing is not currently in the legislative framework (see **Recommendation 3**).
5.	**Scope of CDR Data released by Data Holder does not match the consents and authorisations obtained by Accredited Data Recipient**	CDR Consumers will be provided with Consumer Dashboards by both the Data Holder and Accredited Data Recipient (and can check that consents and authorisations match with their understanding about what they have provided).	CDR Consumers may not actively check the relevant Consumer Dashboards, and are therefore unaware of any misalignment (noting that the CDR receipt under Rule 4.18 only provides information relating to consents, but not authorisations (see **Recommendation 3**)).

STEP 6 – DATA HOLDER SENDS CDR DATA TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	There is a risk that the CDR Data that is transferred from the Data Holder to the Accredited Data Recipient does not align with the consents and authorisations given by the CDR Consumer.	PS 10 requires the CDR Consumer to be notified through the Consumer Dashboard, of disclosures (so they can then check that this aligns with their consents and authorisations provided). Components 4.3, 4.4 and 4.5 of the CX Guidelines provide clear guidance on how CDR Consumers should be informed.	The CX Guidelines are not binding upon CDR Participants (as they are not incorporated as part of the Draft Rules or binding Draft Data Standards).
6.	**Disclosure of third party individuals' information** There is a risk that CDR Data is disclosed which includes information about transactions involving third party individuals (who are not associates of the CDR Consumer or joint account holders). We understand that the CDR Data which may be disclosed by a Data Holder, may include information about third party individuals. For example, CDR Data could include details about deposits into, or withdrawals from, a Product account by a third party individual.	CDR Data must be used and disclosed in accordance with the Draft Rules. The Accredited Data Recipient cannot use the third party individual's information to identify, compile insights in relation to, or build a profile about, that third party individual from the CDR Data. However, this is limited in that the Draft Rules make it clear that this restriction does not apply to Accredited Data Recipients deriving information about a third party individual's interactions with the CDR Consumer in order to provide the requested goods and services to the CDR Consumer (Rules 4.12(3) and 4.12(4)).	The third party individual will not have provided any consents (and will be unlikely to be aware) that their information has been disclosed by the Data Holder to the Accredited Data Recipient, and that information will be used by the Accredited Data Recipient. We understand that this issue has been carefully considered by the Department, including by considering how this issue is treated in other jurisdictions (e.g. under the GDPR). We understand that it is intended that the position that has been reached represents a balancing of interests, between the privacy rights of the third party individual against the utility for CDR Consumers to access and use their information. Although this use will be permitted by law, we still expect that the Australian community may have privacy concerns about this. We therefore recommend that the responsible agencies

STEP 6 – DATA HOLDER SENDS CDR DATA TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			publish information to support this law, including a clear description of the benefits for CDR Consumers and how this is balanced against the potential concerns third party individuals may have (including the reasons why personal information in relation to third party individuals is not required to be redacted by the Data Holder before release) (see **Recommendation 7**). We note that although most stakeholders who provided submissions broadly agreed with **Recommendation 7**, one stakeholder [FinTech Australia] submitted that the identified risk is not problematic as most transaction payments are made by or to companies rather than individuals. While we are not in a position to comment on the proportions of third party transaction payments that are made by or to companies in comparison to those made by or to individuals, we expect at least some of those payments will be made by third party individuals and accordingly consider it necessary to consider this risk and the potential mitigation strategies. Some stakeholders suggested that we should recommend additional strategies in relation to such third party data of individuals. For example, the Financial Rights Legal Centre submitted that "*requirements should be imposed upon Accredited [Data] Recipients (and Data Holders) to delete or de-identify [third party data] after it is used or that this data be reconfigured to*

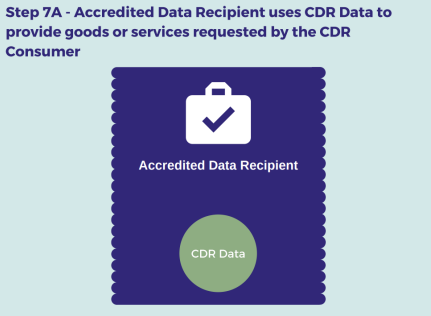
STEP 6 – DATA HOLDER SENDS CDR DATA TO ACCREDITED DATA RECIPIENT			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			maintain the utility of such data but remove the risks." The Australian Privacy Foundation expressed the view that it is unclear why the consent of the third party is not required and that "*third party information must be redacted. It cannot be shared with a third party without consent.*" It noted that such disclosure of third party personal information creates a culture where individuals think they do not have control over their data (which may have broader implications, such as loss of trust for the Australian Government). If **Recommendation 7** is implemented, the explanation may assist stakeholders in understanding how the competing privacy interests have been considered and balanced.

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

Summary of step:

Accredited Data Recipient collects and uses CDR Data to provide the specific goods or services to which the CDR Consumer consented (including directly or indirectly deriving CDR Data from the collected CDR Data).

Relevant Diagram in Attachment 2:



STEP 7A – ACCREDITED DATA RECIPIENT COLLECTS AND USES CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**Accredited Data Recipient collects and uses CDR Data outside the scope of the consent** There is a risk that the Accredited Data Recipient will collect and use the CDR Data outside the scope of the original consent provided by the CDR Consumer.	PS 6 effectively prevents the collection or use of CDR Data by an Accredited Data Recipient which is not a "permitted use". This is defined in Rule 7.5 as including use in compliance with the data minimisation principle to provide goods or services requested by the CDR Consumer. Use outside of the scope of the applicable consents for those goods and services will not be a "permitted use". *[For the other permitted uses, see Steps 7B to 7D below.]* To obtain and retain status as an Accredited Data Recipient, the accreditation applicant must be a fit	

STEP 7A – ACCREDITED DATA RECIPIENT COLLECTS AND USES CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		and proper person. This assists in ensuring only persons who are likely to comply with the requirements of the CDR regime will be able to be accredited.	
2.	**Use for prohibited consents** There is a risk that an Accredited Data Recipient could use CDR Data for a use for which it is not permitted to ask for consent (e.g. for on-selling non-de-identified CDR Data) and using it to build a profile of an identified third party) .	As above.	
3.	**Security of CDR Data held by Accredited Data Recipient** CDR Data is not securely held by the Accredited Data Recipient, resulting in theft of the CDR Consumer's CDR Data.	The accreditation process will involve testing to ensure compliance with the Draft Data Standards (which include minimum security requirements for ICT systems handling CDR Data). PS 12 (and Rule 7.11) require Accredited Data Recipients to maintain minimum security requirements. CDR Consumers must, in accordance with section 56ES in the CDR Act, be notified of any eligible data breaches of CDR Data.	CDR Consumers will only become aware of a security breach if notification is issued in accordance with the mandatory data breach notification scheme, as applied by the CDR Act (or if they independently become aware of misuse of their CDR Data by other means). However, this is no different to the position under the Privacy Act.

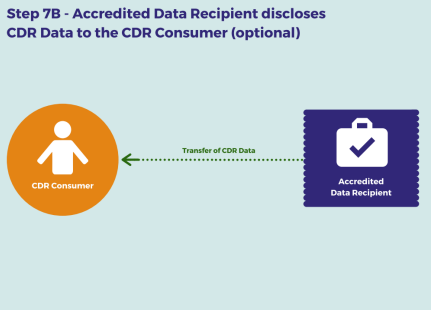
STEP 7A – ACCREDITED DATA RECIPIENT COLLECTS AND USES CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
4.	**Accredited Data Recipient does not treat derived data as CDR Data** Like the similar risk for Data Holders in Step 0, Accredited Data Recipients will need to carefully analyse whether derived data falls within the definition of 'CDR Data', and apply the correct privacy protections to it.	The CDR Act contains definitions about when data is 'CDR Data' *[See also our also the analysis in **Part F [Analysis of APP Application and Compliance]** of this PIA report]*.	To address this gap, we have recommended the provision of guidelines by the OAIC, and other activities to promote the understanding and acceptance of the Privacy Safeguards, and educational programs to protect CDR Data. We understand that the OAIC currently intends to issue such guidelines and to undertake other activities (see **Recommendation 2**).

Step 7B. Accredited Data Recipient discloses CDR Data to the CDR Consumer (optional)

Summary of step:

The Accredited Data Recipient may disclose CDR Data to the CDR Consumer.

Relevant Diagram in Attachment 2:



STEP 7B – ACCREDITED DATA RECIPIENT DISCLOSES CDR DATA TO THE CDR CONSUMER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**Right to request CDR Data** CDR Consumers do not have a *right* under the CDR regime to request an Accredited Data Recipient to provide their CDR Data to them.	Only Data Holders are required to disclose CDR Data under the CDR regime.	Currently, the CDR regime does not afford similar rights to CDR Consumers as is provided for under APP 12. To address this gap, we have recommended that it should be considered whether a right for CDR Consumers to access their CDR Data whilst it is held by Accredited Data Recipients should be included in the CDR regime (see **Recommendation 4**). The majority of stakeholders providing submissions supported this **Recommendation 4**. For example: • Legal Aid Queensland stated that "*such a right is particularly useful so that the CDR Consumer can check the accuracy of CDR Data held by the Accredited Data Recipient*

STEP 7B – ACCREDITED DATA RECIPIENT DISCLOSES CDR DATA TO THE CDR CONSUMER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			or seek confirmation that the Accredited Data Recipient has deleted information if consent to hold the information has been withdrawn by the CDR Consumer." • The Financial Rights Legal Centre stated that "*if it is empowering for consumers to be able to access their financial data from Data Holders – which is the entire raison d'être of the reform – then it is equally empowering for consumers to be able to access this information from [Accredited] Data Recipients.*" • The Australian Privacy Foundation stated that CDR Consumers "*must be able to access their own personal information from any participant in the system which holds that information*" and that this access should be easy and provided free of charge. However, alternative views were expressed by some stakeholders who provided submissions: • FinTech Australia noted that **Recommendation 4** would need to be balanced against the resources of Accredited Data Recipients, and that if it is adopted by the Department, stakeholders should be consulted. • The Australian Retail Credit Association did not agree with **Recommendation 4**, and submitted that there are risks associated

STEP 7B – ACCREDITED DATA RECIPIENT DISCLOSES CDR DATA TO THE CDR CONSUMER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			with providing CDR Consumers with the right to request their CDR Data from Accredited Data Recipients, including that the CDR Data held by Accredited Data Recipients may not be up to date, and implementing such a right may impose costs on Accredited Data Recipients. However, we remain of the view that access to one's own data is an important privacy right, and one that should be considered by the Department in relation to CDR Data held by an Accredited Data Recipient.
2.	**Accredited Data Recipient may become a Data Holder** There is a risk that CDR Consumers will not understand that an Accredited Data Recipient can become a Data Holder, which will change the entity's obligations in relation to handling CDR Data, and the protections under the Privacy Safeguards that will be afforded to their CDR Data.	The CDR Act allows an Accredited Data Recipient to be a Data Holder only in the circumstances set out in the Draft Rules. For the banking Sector, the Draft Rules set out a process for certain Accredited Data Recipients to request the CDR Consumer's agreement to become a Data Holder for the relevant CDR Data, rather than an Accredited Data Recipient (Schedule 3, section 7.2). This includes providing the CDR Consumer with information that explains: • that the Privacy Safeguards will no longer apply, and the consequences to the CDR Consumer of not agreeing to the entity not being a Data Holder; and	It is important that CDR Consumers understand their available options (see **Recommendation 2**), but noting our additional comments about the limitations of consumer education. We note that the protections in the CDR regime for the provision of consent do not apply to this agreement. We consider that there is scope for vulnerable consumers to be pressured into agreeing to this change (which will result in the loss of the additional protections for the CDR Data afforded by the Privacy Safeguards). This risk will be increased if CDR Consumers are, for example, told "We want to become your Data Holder, and the Privacy Act will apply to your personal information" – this is technically correct, but may lead CDR Consumers to believe that their CDR Data will have equivalent,

STEP 7B – ACCREDITED DATA RECIPIENT DISCLOSES CDR DATA TO THE CDR CONSUMER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		• how the CDR Data will be treated by the entity. The CDR Consumer is required to agree to the entity being a Data Holder for that CDR Data.	or greater, protections than under the CDR regime (despite being given the information which is required under the Draft Rules). We therefore recommend that the ACCC consider whether the Draft Rules should incorporate additional protections about *how* the Accredited Data Recipients may seek that agreement from the CDR Consumer, similar to the protections currently afforded to how consent may be sought (see **Recommendation 8**). Many stakeholders who provided submissions strongly agreed with this **Recommendation 8**. For example, the Financial Rights Legal Centre stated that "*we strongly support rules being introduced to ensure Accredited Data Recipients seek agreement from the [CDR] Consumer for them to become a Data Holder. The risk identified in the PIA goes directly to the issue of the complexity and inconsistency of consumer rights and protections at different stages and contexts of the data flow. This case demonstrated clearly that there are different protections in place for what essentially seems like the same thing to a consumer.*" Another stakeholder submitted that "*the ACCC should consider whether the Draft Rules need to include additional protections to manage the transition of an entity from an Accredited Data Recipient to a Data Holder*" (Submission by the Australian Communications Consumer Action

STEP 7B – ACCREDITED DATA RECIPIENT DISCLOSES CDR DATA TO THE CDR CONSUMER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			Network). It further stated that, given the difficulty CDR Consumers will have in understanding the privacy protections available under the CDR regime, it is vital that "*the overarching privacy protections within the CDR regime are reassessed and made more comprehensive to ensure that the privacy of CDR Consumers is appropriately protected in all scenarios".*

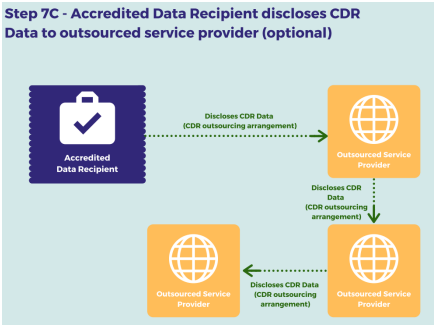
STEP 7B – ACCREDITED DATA RECIPIENT DISCLOSES CDR DATA TO THE CDR CONSUMER			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
3.	**If the Accredited Data Recipient discloses CDR Data and the CDR Consumer provides that CDR Data to a third party outside the CDR regime** If the CDR Consumer provides their CDR Data that it has received from an Accredited Data Recipient to a third party, the privacy protections afforded to that CDR Data under the CDR regime will not apply.	The Privacy Act, including the requirements of APP 11, will apply in relation to personal information held by Data Holders who are APP entities. (We have noted some stakeholders' concerns about the adequacy of the level of protection under the APPs.)	The protections afforded in the APPs will only apply to CDR Consumers where the third party is an APP entity. CDR Data may have a lower level of protection when received by a third party, than when the same information is held by a Data Holder or Accredited Data Recipient. There is no requirement for CDR Consumers to be "warned" that the protections of the CDR regime (and possible the APPs) will not apply if they share the CDR Data provided with a third party (see **Recommendation 3**). It is important that CDR Consumers understand their available options (see **Recommendation 2**), but noting our additional comments about the limitations of consumer education. The ACCC should consider whether the Draft Rules should require an Accredited Data Recipient to provide information to a CDR Consumer when disclosing their CDR Data pursuant to their consumer data request (see **Recommendation 3**).

Step 7C. Accredited Data Recipient discloses CDR Data to outsourced service provider (optional)

Summary of step:

The Accredited Data Recipient may disclose CDR Data to its outsourced service providers.

Relevant Diagram in Attachment 2:



STEP 7C – ACCREDITED DATA RECIPIENT DISCLOSES CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**CDR Consumers are unaware that their CDR Data is being handled by an outsourced service provider of the Accredited Data Recipient** Under Rule 7.5, an Accredited Data Recipient may disclose information to an outsourced service provider so that the outsourced service provider can provide goods and services.	PS 1 requires a CDR Policy to state whether CDR Data may be disclosed to an outsourced service provider (and to include a list of such service providers, including the applicable countries if outside Australia (Rule 7.2(4)(d)). Under Rule 4.11(f), an Accredited Data Recipient is required to provide the CDR Consumer with the fact that their CDR Data may be disclosed to an outsourced service provider (including one that is based overseas) and with a link to the Accredited Data Recipient's CDR Policy. The permitted use by an outsourced service provider is limited to the extent that the disclosure is reasonably needed for that entity to do the things that the Accredited Data Recipient is	The CDR Consumer is not required to be told *which* outsourced service provider their CDR Data will be disclosed to, or whether those outsourced service providers are based in Australia or overseas. The CDR Act provides that Accredited Data Recipients must take the steps specified in the Draft Rules to notify a CDR Consumer of a disclosure. The Draft Rules do not stipulate any notification requirements for disclosures to outsourced service providers. We are conscious of the risk that CDR Consumers may suffer "information overload" if presented with too much information.

STEP 7C – ACCREDITED DATA RECIPIENT DISCLOSES CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		permitted to do under Rule 7.5 (other than to disclose de-identified data).	We have also taken into account the views expressed by stakeholders to date, and that, in our view, most Australians today are likely to expect that outsourced ICT arrangements will be used. We therefore consider that, on balance, the protections in the CDR regime are likely to be sufficient to mitigate the identified risk.
2.	**CDR Consumers are unaware of disclosures by the Accredited Data Recipient to an outsourced service provider located overseas** CDR Consumers may have additional concerns where their CDR Data is stored outside Australia (including in countries with lesser privacy protections than Australia).	*[As in paragraph 1 above.]* In addition, under PS 8, the Accredited Data Recipient must only disclose the CDR Data to an overseas entity where it is an accredited person, or the Accredited Data Recipient reasonably believes that the overseas entity will provide substantially similar protections for the CDR Data. If an Accredited Data Recipient has disclosed CDR Data in accordance with a CDR outsourcing arrangement (as required under Rule 1.10), it will remain responsible for use and disclosure of for CDR Data by the recipient. This includes further disclosures in an outsourcing 'chain' (Rules 7.6(2) and 7.6(3)).	*[As in paragraph 1 above.]*

STEP 7C – ACCREDITED DATA RECIPIENT DISCLOSES CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
3.	**Security breach in relation to CDR Data held by an outsourced service provider** There is a security breach in relation to CDR Data held by an outsourced service provider of the Accredited Data Recipient.	Rule 1.10 effectively requires the contract between the Accredited Data Recipient and the outsourced service provider (the "CDR outsourcing arrangement") to require the outsourced service provider to comply with Schedule 2 to the Draft Rules. Schedule 2 to the Draft Rules relates to security of CDR Data. The Accredited Data Recipient is responsible for ensuring compliance with the requirements of Schedule 2 to the Draft Rules (Rule 1.16).	The outsourced service provider is not itself required by the legislative framework to comply with the Privacy Safeguards, even though it may hold CDR Data. We note the view of one stakeholder [the Australian Privacy Foundation] that any entity that will receive or hold CDR Data (which includes all outsourced service providers and their outsourced service providers) should be members of a recognised dispute resolution scheme in relation to CDR Consumer complaints. Another stakeholder [the Financial Rights Legal Centre] had a similar view, that in order to hold CDR Data, the entity receiving the CDR Data should be accredited (similar to the requirement imposed on Accredited Data Recipients). We agree that such measures may warrant further consideration, and may provide additional protections in practice. We do note that the protections in Rule 1.16 legally mitigate the identified risk, and an effective monitoring and compliance regime will assist in ensuring the legal obligations of the Accredited Data Recipient in relation to any outsourced service providers are enforced (see **Recommendation 9**).

STEP 7C – ACCREDITED DATA RECIPIENT DISCLOSES CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
4.	**Outsourced service provider itself discloses CDR Data to its outsourced service provider (which may in turn, disclose CDR Data to its outsourced service provider)** The risk is that the Accredited Data Recipient will not be responsible for uses and disclosures of CDR Data by outsourced service providers at the end of a 'chain' of such providers.	An outsourced service provider may only disclose CDR Data to a further outsourced service provider under a "CDR outsourcing arrangement". This is defined in Rule 1.10, and requires: • a written contact; • the outsourced service provider to take the steps in Schedule 2 (which will provide minimum security protections); • restriction on use or disclosure of the CDR Data other than in accordance with the contract; • requirements to return or delete CDR Data as required by the discloser of the CDR Data; • a requirement to ensure any further disclosure is only done in accordance with a CDR outsourcing arrangement; and • a requirement to ensure the recipient complies with the CDR outsourcing arrangement (also in Rule 1.16). If an Accredited Data Recipient has disclosed CDR Data in accordance with a CDR outsourcing arrangement, it will remain responsible for the use and disclosure of CDR Data by the recipient. This includes further disclosures in an outsourcing 'chain' (Rules 7.6(2) and 7.6(3)).	

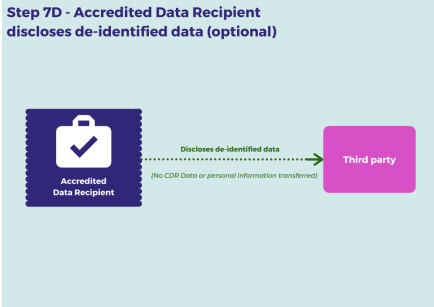
STEP 7C – ACCREDITED DATA RECIPIENT DISCLOSES CDR DATA			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
5.	**Data Holder uses an outsourced service provider to handle CDR Data** The outsourced service provider will not be subject to the privacy protections afforded to CDR Consumers under the CDR regime. *[Please see additional risks identified in paragraphs 1-3 above.]*	The APPs will apply to personal information held by the outsourced service provider if the CDR Data is personal information and the outsourced service provider is an APP entity (including APP 8, if the outsourced service provider is located overseas).	Unlike outsourced service providers of Accredited Data Recipients, the CDR regime does not impose restrictions on outsourced service providers of Data Holders handling the same CDR Data. However, we understand that this is consistent with the intention of the CDR Act (including as reflected in section 56BD(3)).

Step 7D. Accredited Data Recipient de-identifies CDR Data and discloses the de-identified data to third parties (optional)

Summary of step:

The Accredited Data Recipient may de-identify CDR Data and disclose the de-identified data to third parties in accordance with the CDR Data de-identification process.

Relevant Diagram in Attachment 2:



STEP 7D – ACCREDITED DATA RECIPIENT DISCLOSES DE-IDENTIFIED DATA TO THIRD PARTIES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**CDR Consumer not aware or does not understand implications of de-identification** The CDR Consumer does not know that their information has been de-identified and then disclosed to third parties, or does not understand how the de-identified data will be used.	When seeking the consent to collect and use CDR Data, the Accredited Data Recipient must give the CDR Consumer specified information if the Accredited Data Recipient is asking for the CDR Consumer's consent to de-identify some or all of the collected CDR Data for the purpose of disclosing (including by selling) the de-identified data. This information includes: • what the de-identification process is; • who it will disclose that data to (class of persons) and why; and	The CDR Consumer will still be unaware of the point at which the Accredited Data Recipient has de-identified their CDR Data so that the right of deletion is no longer applicable. One stakeholder [the Australian Privacy Foundation] expressed the view that CDR Consumers may select de-identification without understanding the risks (proper de-identification is a difficult process and it is relatively easy to re-identify de-identified data).[59]

[59] Although we generally agree with this statement, we do note that the ease with which data may be re-identified will vary depending on many factors, including the nature of the data itself, the nature and availability of other data used for re-identification, and the de-identification method(s) used.

STEP 7D – ACCREDITED DATA RECIPIENT DISCLOSES DE-IDENTIFIED DATA TO THIRD PARTIES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		• that the CDR Consumer would not be able to elect to have the de-identified data deleted once it becomes redundant data. Under PS 1, an Accredited Data Recipient's CDR Policy must contain information about their de-identification processes (Rule 7.2). Even though the concept of de-identification is technically complex, and there is a risk that CDR Consumers will not understand it and how it works, we do not consider that providing a level of technical detail to CDR Consumers about the de-identification process is necessary, noting that it may result in 'information overload'.	We also note that one stakeholder [the Financial Rights Legal Centre] voiced that there is nothing in the Draft Rules as they are currently drafted to prevent Accredited Data Recipients providing CDR Consumers with a reward or incentive if they provide their consent for the Accredited Data Recipient to de-identify some or all of the collected CDR Data for the purposes of disclosing (including by selling) the de-identified data (in accordance with Rule 4.11(3)(e)). This should be noted in light of another submission by another stakeholder [the Australian Privacy Foundation] that data which is collected and de-identified is likely to be more valuable to the Accredited Data Recipient than any payment for services provided to the CDR Consumer.
2.	**CDR Data not properly de-identified** There is a risk that CDR Data is not properly de-identified, meaning that the CDR Consumer can be identified from the data. This could be because Accredited Data Recipients may not appreciate the significant complexity and risk involved with attempting to de-identify data derived from CDR Data to the extent	CDR Data must only be de-identified in accordance with the CDR de-identification process specified in Rule 1.17. We understand that this has been informed by the OAIC and Data61's *De-identification Decision-Making Framework* .	We note that the technical requirements under the CDR regime for de-identification are not identical to the requirements under the Privacy Act. For this reason, it will be important that appropriate guidance is provided to Accredited Data Recipients (see **Recommendation 2**). One stakeholder [the Australian Privacy Foundation] held a strong view that *"de-identification does not work"*, and the only way to protect CDR Consumers is to make it a requirement that any CDR Data that becomes redundant must only be deleted (rather than de-identified).

STEP 7D – ACCREDITED DATA RECIPIENT DISCLOSES DE-IDENTIFIED DATA TO THIRD PARTIES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	technically required under the Draft Rules.		Although we accept that in an ideal world, from a privacy perspective, deletion of redundant data is a safer option for CDR Consumers as the data would be afforded stronger privacy protections than it would receive through de-identification (given the risks associated with de-identification), we note that this consideration needs to be balanced against the value of de-identified data and any associated implications (which may not be privacy issues). If de-identification is to be allowed in the CDR regime, we note that there are strategies in place in the CDR legislative framework, including that de-identification must be done in accordance with the Draft Rules. Such requirements include that: • the CDR Data de-identification process must be followed (Rule 1.17), including *The De-Identification Decision-Making Framework* published by the OAIC and Data61 (Rule 1.17(5)); • when an Accredited Data Recipient is asking for a CDR Consumer's consent, it must ask the CDR Consumer for consent to de-identify some or all of their CDR Data for the purpose of disclosing the de-identified data (Rule 4.11(3)(e)), including additional information relating to de-identification (Rule 4.15);

STEP 7D – ACCREDITED DATA RECIPIENT DISCLOSES DE-IDENTIFIED DATA TO THIRD PARTIES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			• an Accredited Data Recipient must provide a CDR Consumer with their general policy for de-identifying redundant data (if applicable), as well as the associated information about the de-identification (Rule 4.17); • an Accredited Data Recipient must include information about de-identification of CDR Data that is not redundant data in its CDR Policy (Rule 7.2(4)(e)) and of CDR Data that becomes redundant data (Rule 7.2(4)(g)); and • PS 12 must be followed, including Rule 7.12.

Step 8. CDR Consumer withdraws their consent or their consent expires

Summary of step:

The CDR Consumer's consent is either withdrawn from the Accredited Data Recipient (using the CDR Consumer's Consumer Dashboard) or the consent expires. The Accredited Data Recipient must stop using the CDR Data and inform the Data Holder that the CDR Consumer's consent has been withdrawn or has expired. The Data Holder must stop providing the CDR Data as it is no longer authorised to do so.

Relevant Diagram in Attachment 2:

STEP 8 – CDR CONSUMER WITHDRAWS CONSENT OR CONSENT EXPIRES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**Accredited Data Recipient continues to use the CDR Data** There is a risk that the Accredited Data Recipient will continue to use the CDR Data after the consent ends, and does not de-identify or destroy that CDR Data as required.	PS 6 limits use of CDR Data by Accredited Data Recipients. PS 12(2) (and Rule 7.12 and Rule 7.13) require destruction/de-identification of redundant CDR Data in accordance with the CDR Data de-identification process (Rule 1.17) or the CDR Data deletion process (Rule 1.18) (or if an Accredited Data Recipient is not required to destroy or de-identify the data, then the applicable Privacy Safeguards will continue to apply to that CDR Data).	

STEP 8 – CDR CONSUMER WITHDRAWS CONSENT OR CONSENT EXPIRES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
2.	**CDR Consumer wants their redundant CDR Data to be deleted, rather than de-identified (because of the risks associated with de-identification)** There is increasing community concern about the risk of de-identified data being re-identified through linkage with other data.[60]	CDR Consumers may elect that the collected CDR Data, and any data derived from it, be deleted when it becomes redundant data. This election can be made when giving consent, or at any other time before the consent expires (Rule 4.16). When asking for consent to collect and use, an Accredited Data Recipient must allow the CDR Consumer to make an election in relation to deletion of redundant data (Rule 4.11(1)(e)). It must also give specified information about the treatment of redundant data (including a statement that the CDR Consumer has the right to elect to delete redundant data) (Rules 4.11(h) and 4.17). Consumer Dashboards made available by Accredited Data Recipients must have a function that allows a CDR Consumer to elect to delete redundant data (i.e. data that is no longer required for the purposes for which is was collected) (Rule 1.14).	The right to deletion does not apply if the information has already been de-identified. However, there are mitigation strategies in relation to the de-identification of CDR Data (discussed in Step 7D above).
3.	**CDR Consumer is unaware that their consent has expired**	Under Rule 4.20, an Accredited Data Recipient is required to notify the CDR Consumer each 90 days that the consent is still current (but only if the CDR Consumer has not provided consent, or	

[60] See, for example, recent media and commentary around the Office of the Victorian Information Commissioner's report into the disclosure of myki travel information (https://ovic.vic.gov.au/wp-content/uploads/2019/08/Report-of-investigation_disclosure-of-myki-travel-information.pdf).

STEP 8 – CDR CONSUMER WITHDRAWS CONSENT OR CONSENT EXPIRES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
	There is a risk that the CDR Consumer will not know that their consent has expired, and that the Accredited Data Recipient has ceased collecting and/or using their CDR Data from the Data Holder.	used their Consumer Dashboard or been sent a notification by the Accredited Data Recipient). Under Rule 4.19, Accredited Data Recipients are required to update the CDR Consumer's Consumer Dashboard as soon as practicable after the information required to be included on the Consumer Dashboard (which includes information about consents) changes.	
4.	**CDR Consumer wishes to withdraw their consent (either to collect, or to use, their CDR Data)** There is a risk that Accredited Data Recipients will make it difficult for CDR Consumers to withdraw their consent.	The Draft Rules expressly require that consents to collect and use CDR Data must be able to be easily withdrawn (Rules 4.9). When asking for consent, an Accredited Data Recipient must give the CDR Consumer a statement that consent can be withdrawn at any time, and instructions on how to withdraw consent, and the consequences if consent is withdrawn (Rule 4.11(3)(g)). CDR Consumers are able to withdraw their consent to the collection and use of their CDR Data in accordance with Rule 4.13. The Consumer Dashboard must have a functionality to withdraw consents to collect and use CDR Data (Rule 1.14).	The CDR Act and the Draft Rules are silent about whether the protections in the legislative framework can be affected by a legally binding agreement between relevant parties. For example, there is no provision in the Draft Rules which expressly states that an Accredited Data Recipient must not include, in other contractual arrangements, a clause that is inconsistent with the right of the CDR Consumer to withdraw their consent to collect or to use CDR Data, or which imposes additional conditions or requirements on that right. We note that a contract cannot permit an action which is illegal, and that there is a general principle of law that a contractual provision which defeats or circumvents a statutory purpose or policy will not be enforceable.

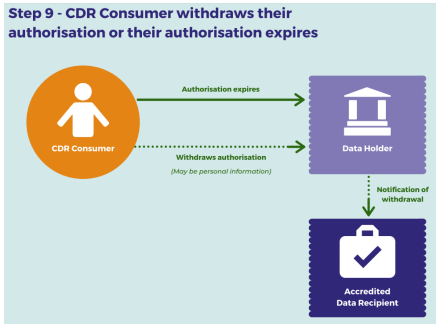
STEP 8 – CDR CONSUMER WITHDRAWS CONSENT OR CONSENT EXPIRES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
			Despite this, our engagement with stakeholders indicated that at least some entities had noted the absence of any prohibition on "contracting out" and were considering the implications of this. Accordingly, the ACCC may wish to consider whether the Draft Rules should expressly ensure that contractual clauses with a CDR Consumer cannot override rights and protections provided to CDR Consumers by the legislative framework (see **Recommendation 3**). We note that **Recommendation 3** also implements a suggestion in a submission by the Australian Privacy Foundation that the Draft Rules should give the ACCC the power to make a determination about whether a contractual clause with a CDR Consumer overrides their rights and protections.

Step 9. CDR Consumer withdraws their authorisation or their authorisation expires

Summary of step:

The CDR Consumer withdraws their authorisation from the Data Holder to continue disclosing their CDR Data, or the authorisation expires.

Relevant Diagram in Attachment 2:



STEP 9 – CDR CONSUMER WITHDRAWS AUTHORISATION OR AUTHORISATION EXPIRES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**No notification of withdrawal of authorisation** Data Holder does not notify the Accredited Data Recipient of the CDR Consumer's withdrawal of authorisation, so the Accredited Data Recipient continues to use the CDR Data.	Under Rule 4.25(2), a Data Holder must notify the Accredited Data Recipient of the CDR Consumer's withdrawal of authorisation, and the Draft Data Standards specify how this will occur technically. Further, under Rule 4.14(1)(c), upon an Accredited Data Recipient being notified of the withdrawal of authorisation, the associated consent to collect and use the CDR Data expires. We understand that the Draft Data Standards require an "automatic notification" from a Data Holder to an Accredited Data Recipient upon	

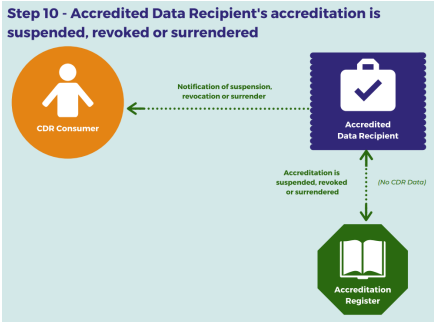
STEP 9 – CDR CONSUMER WITHDRAWS AUTHORISATION OR AUTHORISATION EXPIRES			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		withdrawal of authorisation (and vice versa upon withdrawal of consent).	
2.	**CDR Consumer is unaware of expiry of authorisation** CDR Consumer is unaware that their authorisation has expired, and the Accredited Data Recipient is no longer collecting and/or using their CDR Data.	Under Rule 4.27, Data Holders are required to update the CDR Consumer's Consumer Dashboard as soon as practicable if they receive an authorisation to disclose or if such an authorisation expires. This means that the CDR Consumer has the ability to check whether their consent has also expired as a result of their withdrawal of their authorisation.	

Step 10. Accredited Data Recipient's accreditation is suspended, revoked, or surrendered

Summary of step:

The Accredited Data Recipient's accreditation is suspended, revoked, or surrendered.

Relevant Diagram in Attachment 2:



STEP 10 – ACCREDITATION ENDS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
1.	**Data Holder continues to send CDR Data to a previously Accredited Data Recipient** There is a risk that Data Holders could continue to send CDR Data to a previously Accredited Data Recipient in cases where the accreditation has been revoked or surrendered.	The Data Holder must confirm the accreditation status of the Accredited Data Recipient before each disclosure of CDR Data (see Step 7 above). PS 6, PS 7 and PS 12 continue to apply even after the Accredited Data Recipient's accreditation ends (Rule 5.23). As consents to collect, use and disclose CDR Data will have expired upon revocation or surrender of the accreditation, the Accredited Data Recipient is not authorised to collect, use or disclose CDR Data under the CDR regime. APP 4 will apply to any unsolicited personal information if the previously Accredited Data	

STEP 10 – ACCREDITATION ENDS			
No.	**Risk**	**Existing mitigation strategies**	**Gap analysis and Recommendations**
		Recipient is an APP entity (requiring de-identification or destruction of the unsolicited information).	
2.	**CDR Data is released to a suspended Accredited Data Recipient** There is a risk that a Data Holder could send CDR Data to an Accredited Data Recipient in cases where the Accredited Data Recipient's accreditation has been suspended.	All the obligations provided in the legislative framework of the Accredited Data Recipient continue for the period of the suspension, including PS 4.	
3.	**CDR Consumer is unaware of the accreditation status of the Accredited Data Recipient** There is a risk that the CDR Consumer does not know that the previously Accredited Data Recipient's accreditation has ended.	There are requirements for the Accredited Data Recipient to notify the CDR Consumer under Rule 5.23(3)(b) in circumstances where their accreditation has been surrendered, suspended or revoked, together with a reminder that their consent can be withdrawn (in the case of the accreditation being suspended).	

Part H Other Privacy Risks

27. Introduction

27.1 In this **Part H**, we discuss some further privacy risks that have not been discussed in detail in other Parts of this PIA report.

28. Discussion of further risks

Resources

28.1 The privacy protections in the CDR regime will not be effective if:

28.1.1 Data Holders, Accredited Data Recipients, and CDR Consumers are not aware, or do not understand, those protections; or

28.1.2 the protections are not effectively monitored and enforced by the appropriate regulators.

28.2 In our view, and as discussed in **Part D [Project Description]** of this PIA report, the OAIC and ACCC, as the relevant regulators, will have critical roles to play in ensuring that these risks are appropriately addressed, through the provision of suitable guidance and other educational material, and the implementation of effective monitoring and enforcement regimes.

28.3 We have not investigated, or been provided with, any information about current or future funding levels for these agencies, but recommend that the Department consider whether the OAIC and ACCC will have the necessary funding and resources to provide appropriate guidance material, and to implement effective monitoring and enforcement regimes (**Recommendation 9**).

28.4 We note that almost all stakeholders who provided submissions strongly agreed that the Department should consider whether the OAIC and ACCC are appropriately funded and have the appropriate resources to provide suitable guidance and education material, as well as have effective monitoring and enforcement regimes.

28.5 One stakeholder submitted that this **Recommendation 9** is especially relevant for other Sectors because for the initial implementation in the banking Sector, there is an established external dispute resolution scheme (AFCA) whilst this might not be the case for other Sectors. It stated that "*if other Sectors will have access to CDR Data in the future, the OAIC and the ACCC may need significant resources before they can assess whether to approve an external dispute resolution scheme and monitor its performance*" (Submission by Legal Aid Queensland).

28.6 Another stakeholder expressed the view that, in addition to **Recommendation 9**, it is important that "*the level of resourcing appropriately reflect[s] the need for consumer input into, and testing of, these resources and educational activities. This could involve, for instance, working alongside different people with disability to ensure that all CDR information and education is accessible, user friendly and easy to understand*" (Submission by the Australian Communications Consumer Action Network).

28.7 Finally, another stakeholder [FinTech Australia] noted that when considering resourcing that is required for the CDR regime, it is important to ensure those resources are the "right" people, rather than merely the "right number" of people.

Governance Framework

28.8 In our view, there is a risk that there is an insufficiently clear framework for the division of responsibility for implementation and ongoing operation of the CDR regime. CDR Consumers (and where applicable, Data Holders and Accredited Data Recipients) may not have a sufficiently clear understanding of whether the OAIC or the ACCC is responsible for the effective implementation of particular aspects of the CDR regime. In addition, CDR Consumers, Data Holders and/or Accredited Data Recipients may be confused about the role of the Data Standards Body and/or the Department, as the Commonwealth agency responsible for administration of the CDR Act.

28.9 We understand that the Department, the OAIC and the ACCC are currently working to implement appropriate governance arrangements between them.

28.10 We support this approach, which will assist in ensuring effective communication channels between the various entities, and for ensuring that the regulators have a clear and consistent approach to regulation of the CDR regime, which will be essential in ensuring that its privacy protections are effectively implemented. We suggest that such arrangements should clearly set out the processes for, amongst other things, access to appropriate information as permitted by the CDR Act and as needed to effectively manage any complaints or reports of potential misconduct or technical failures, including for enforcement activities.

Compliance framework

28.11 As mentioned above, it will be critical to the success of the CDR regime that compliance with the legislative requirements by Data Holders and Accredited Data Recipients is effectively checked (and enforced where needed).

28.12 The CDR Act will mean that both the ACCC and the OAIC will have powers to audit compliance and to take appropriate enforcement action in relation to certain aspects of the CDR Act.

28.13 It will also be important that Data Holders and Accredited Data Recipients realise that their compliance will be monitored. Accordingly, we recommend that the OAIC and the ACCC consider the strategies that should be included in a compliance framework and whether these should be made publicly available (**Recommendation 10**). For example, strategies that could be considered include:

28.13.1 sampling approaches to auditing;

28.13.2 CDR Consumer survey approaches; and/or

28.13.3 "own motion" investigations, acting on CDR Consumer complaints, or investigating reports of potential misconduct (as appropriate for the particular regulator).

Effective complaints management

28.14 The CDR legislative framework is based on a policy of implementing a 'no wrong door' approach to complaints made by CDR Consumers, including in relation to complaints about privacy. Under this policy, CDR Consumers may submit complaints via the ACCC or the OAIC, with referrals, appropriate delegations and other mechanisms put in place to ensure that CDR Consumers are never required to redirect their complaint (i.e. any required redirection will be done by the OAIC and the ACCC, where necessary). As discussed above, we are instructed that the OAIC and the ACCC are currently considering the administrative and other governance arrangements for the management of the complaints workflow and

have indicated that a separate privacy impact statement about the arrangements will be released.

28.15 For the initial implementation of the CDR regime, it is intended that the ACCC will recognise an external dispute resolution scheme under the CDR Act for the resolution of disputes (for the banking Sector, this will be Australian Financial Complaints Authority (**AFCA**)).[61]

28.16 In our view, it will be critical that the processes for the management of the workflow are clearly established, to mitigate the risk that complaints will be 'lost' in the system or otherwise not managed in an expeditious and efficient manner.

28.17 Additionally, if there is a 'no wrong door' approach to complaints, there is a risk that CDR Consumers will not understand how their complaint or dispute will be managed, and by whom (meaning that it may make it difficult for a CDR Consumer to follow up on the progress of a complaint they have made).

28.18 We note that it is likely to be extremely difficult for a CDR Consumer to determine which entity or entities, if any, should bear responsibility if, for example, there are any failures of the various ICT systems to communicate effectively with each other or to transmit data correctly (i.e., it is not clear whether the responsibility will lie with the Data Holder or the Accredited Data Recipient or the Accreditation Registrar if something goes wrong). In this case, it will be essential that they be able to complain to an effective regulator, to determine this on a case by case basis.

28.19 We therefore recommend that, in addition to the provision of guidance for CDR Consumers (see **Recommendation 2**), the ACCC and the OAIC (and the recognised external dispute resolution scheme(s)) should have consistent information about the processes for the making of reports/complaints (e.g. similar or identical website information and/or processes) (see **Recommendation 10**).

28.20 We note that stakeholders who provided submissions broadly supported consistent processes to enable a CDR Consumer to make a complaint to any of these entities in relation to their privacy under the CDR regime.

Effective external dispute resolution scheme

28.21 A number of stakeholders also raised the need for CDR Consumers to be referred where appropriate to the relevant external dispute resolution scheme. This was because, for example, it is "*not appropriate that the OAIC or the ACCC are the only avenue of redress for consumers"* (Submission by the Australian Communications Consumer Action Network).

28.22 Stakeholders noted that any external dispute resolution scheme available to CDR Consumers should be accessible, independent, accountable, efficient and effective, and this is particularly important for future implementations in other Sectors (for example, the Telecommunications Industry Ombudsman supported the notion that external dispute resolution schemes will need to be carefully considered for other Sectors in future implementations of the CDR regime).

28.23 We note the view of the Australian Banking Association that AFCA, as an external dispute resolution scheme for the banking Sector, "*has not traditionally been tasked with dealing with complaints relating exclusively to privacy. Given the complexity of the CDR regime and the number of regulatory bodies involved, there is a potential risk of inconsistent outcomes arising*." It submitted that the adequacy of resourcing for this speciality area needs to be reviewed.

[61] We understand that, since the "point in time" established for the conduct of this PIA, under the *Competition and Consumer (External Dispute Resolution Scheme-Banking Sector) Instrument 2019*, AFCA has been recognised as the external dispute resolution scheme for the banking Sector, in accordance with section 56DA(1) in the CDR Act.

28.24 Finally, another stakeholder [the Australian Privacy Foundation] noted the importance of ensuring that external dispute resolution schemes recognise the loss that can be caused to individuals from breaches of their privacy. We agree that external dispute resolution schemes for the CDR regime should recognise and value the financial and other losses associated with breaches of privacy, and award appropriate compensation as a result if this is within the external dispute resolution scheme's powers (see **Recommendation 10**).

Clearer Data Standards

28.25 The current wording and structure of the Draft Data Standards as at the date of this PIA is such that there is uncertainty about:

28.25.1 exactly which artefacts generated to date are (or will be) Data Standards made under the Draft Rules; and

28.25.2 which of the requirements in those artefacts are (or will be) binding Data Standards under the Draft Rules. This is partly because some of the Draft Data Standards artefacts adopt language used in various international IT standards (which use terms such as 'may', and 'must' in ways that do not necessarily match with a legal understanding of those terms), and the artefacts do not necessarily use terminology that is consistent with the defined terms used in the CDR Act and Draft Rules.

28.26 We have recommended that the Data Standards (when finalised) be drafted with further clarity, to distinguish binding Data Standards and using terminology that is consistent with the legislative framework (see **Recommendation 5**).[62]

[62] As described in footnote 5 above, we are aware that a new version of the Draft Data Standards has subsequently been published (version 1.0.0), which appears to address some of these concerns, but we have not undertaken a detailed analysis of this version.

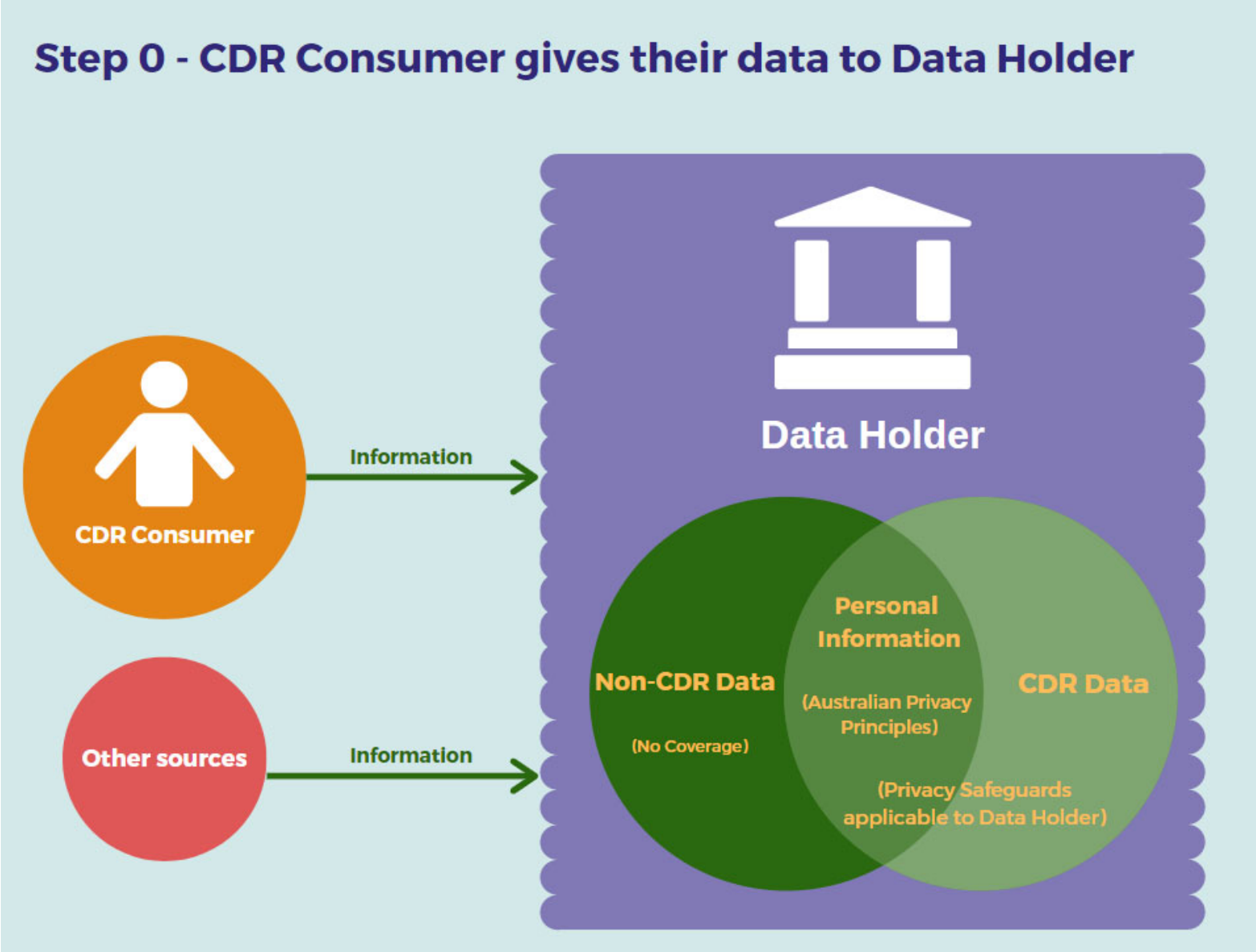
Attachment 1 Glossary

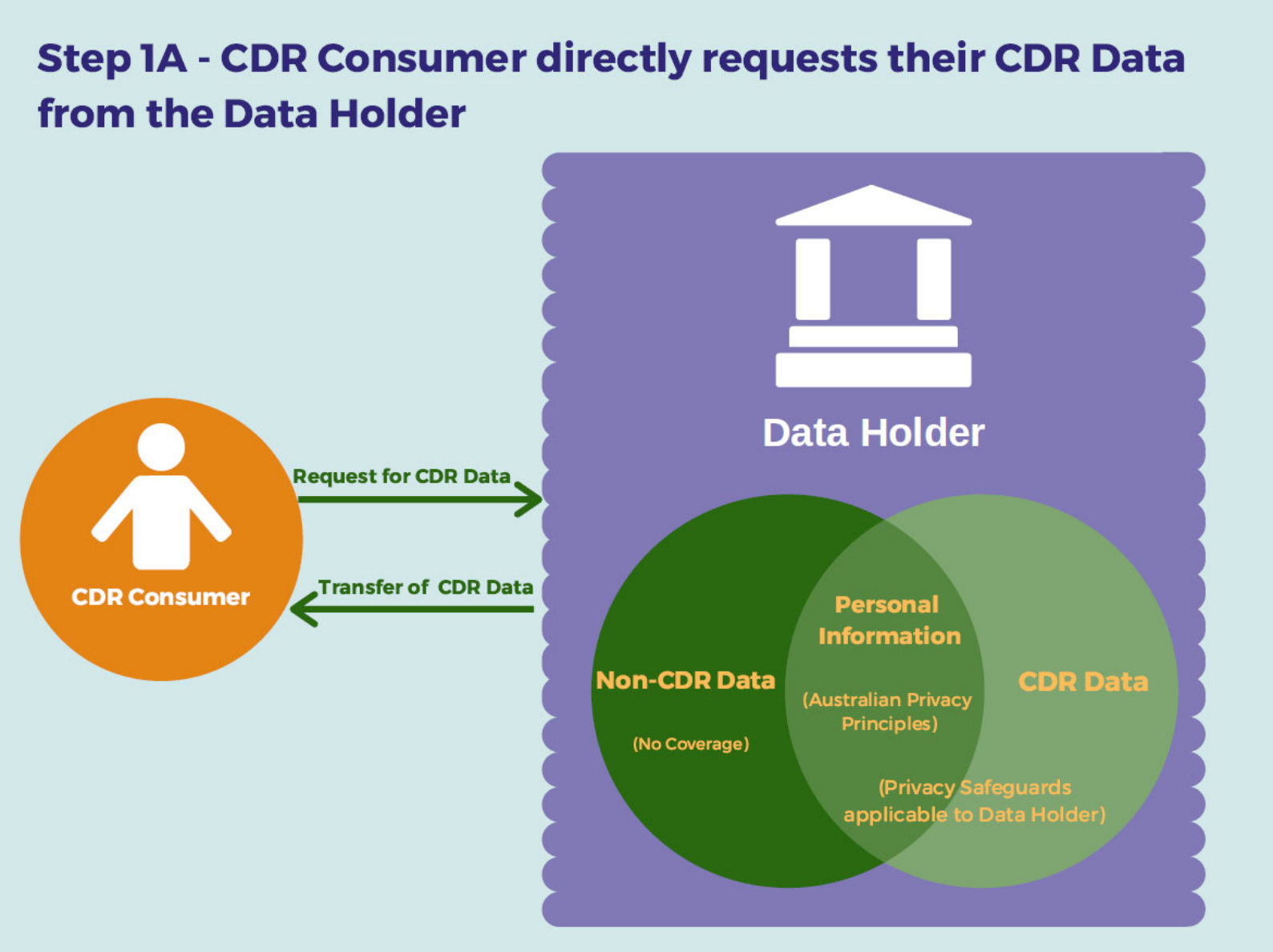
Term	Meaning
ACCC	means the Australian Competition and Consumer Commission.
Accreditation Register	means the register to be established in accordance with subsection 56CE(1) in the CDR Act.
Accredited Data Recipient	has the meaning given by section 56AK in the CDR Act.
AFCA	means the Australian Financial 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.

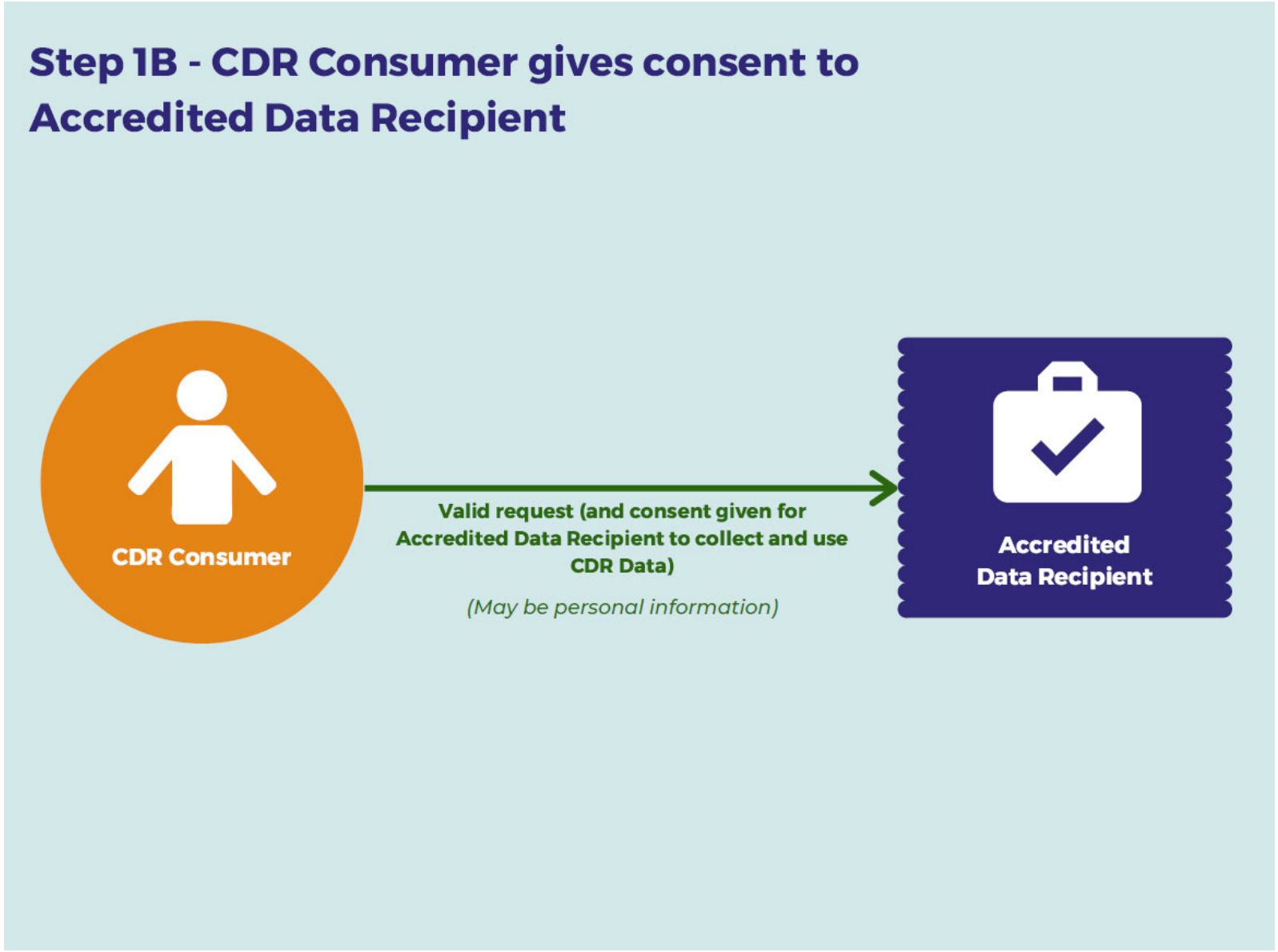
Guidelines (CX Guidelines)	
Data Holder	has the meaning given by subsection 56AJ in the CDR Act.
Data Recipient Accreditor	means the person appointed to the role of Data Recipient Accreditor in accordance with subsection 56CG in the CDR Act.
Data Standards Body	means the body holding an appointment under 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.
Draft Data Standards	means that draft of the data standards to be made under subsection 56FA in the CDR Act.
Draft Rules/Rules	means the *Competition and Consumer (Consumer Data Right) Rules 2019*.
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 draft PIA 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.

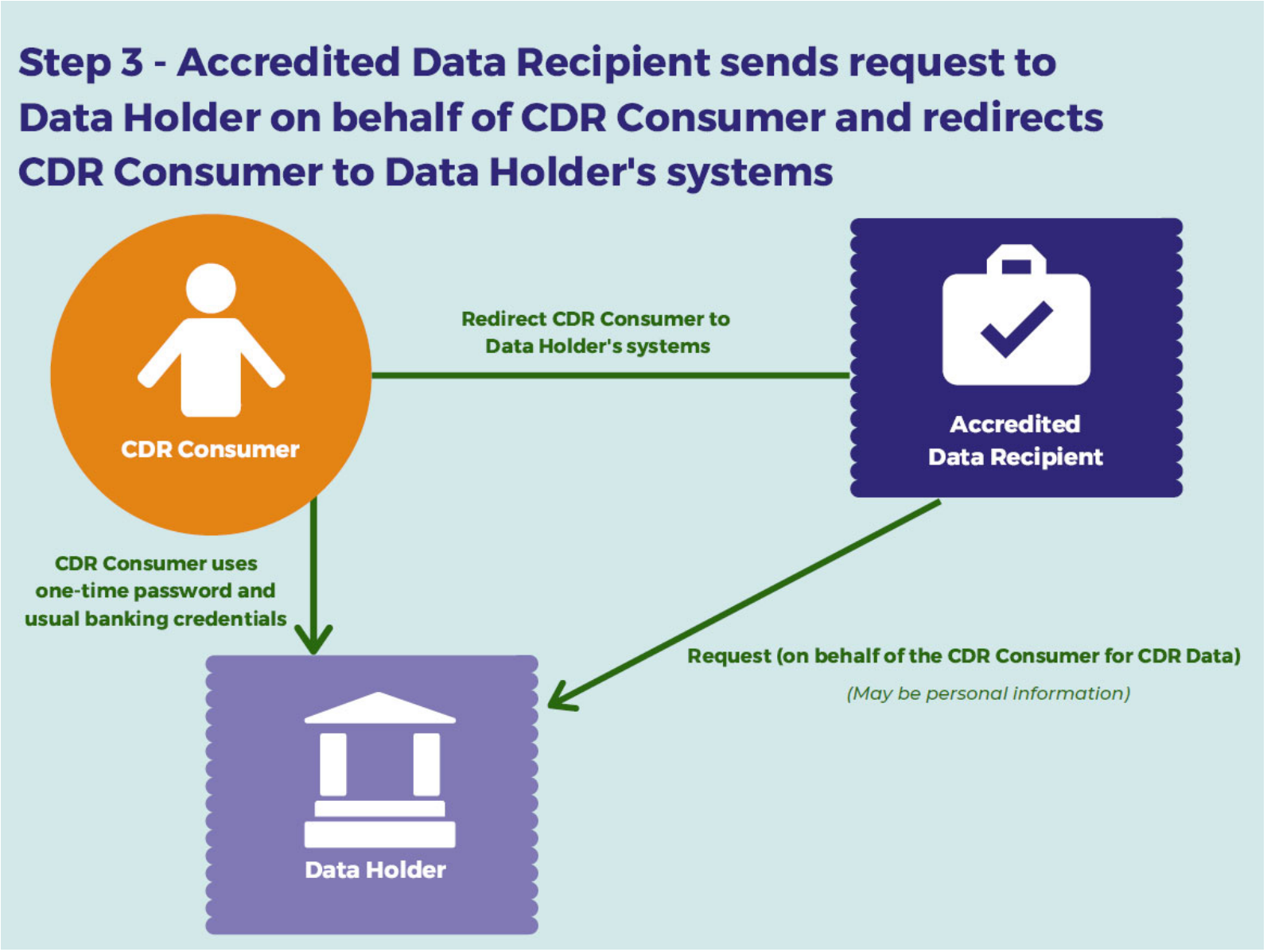
Attachment 2 Diagrams of Information Flows

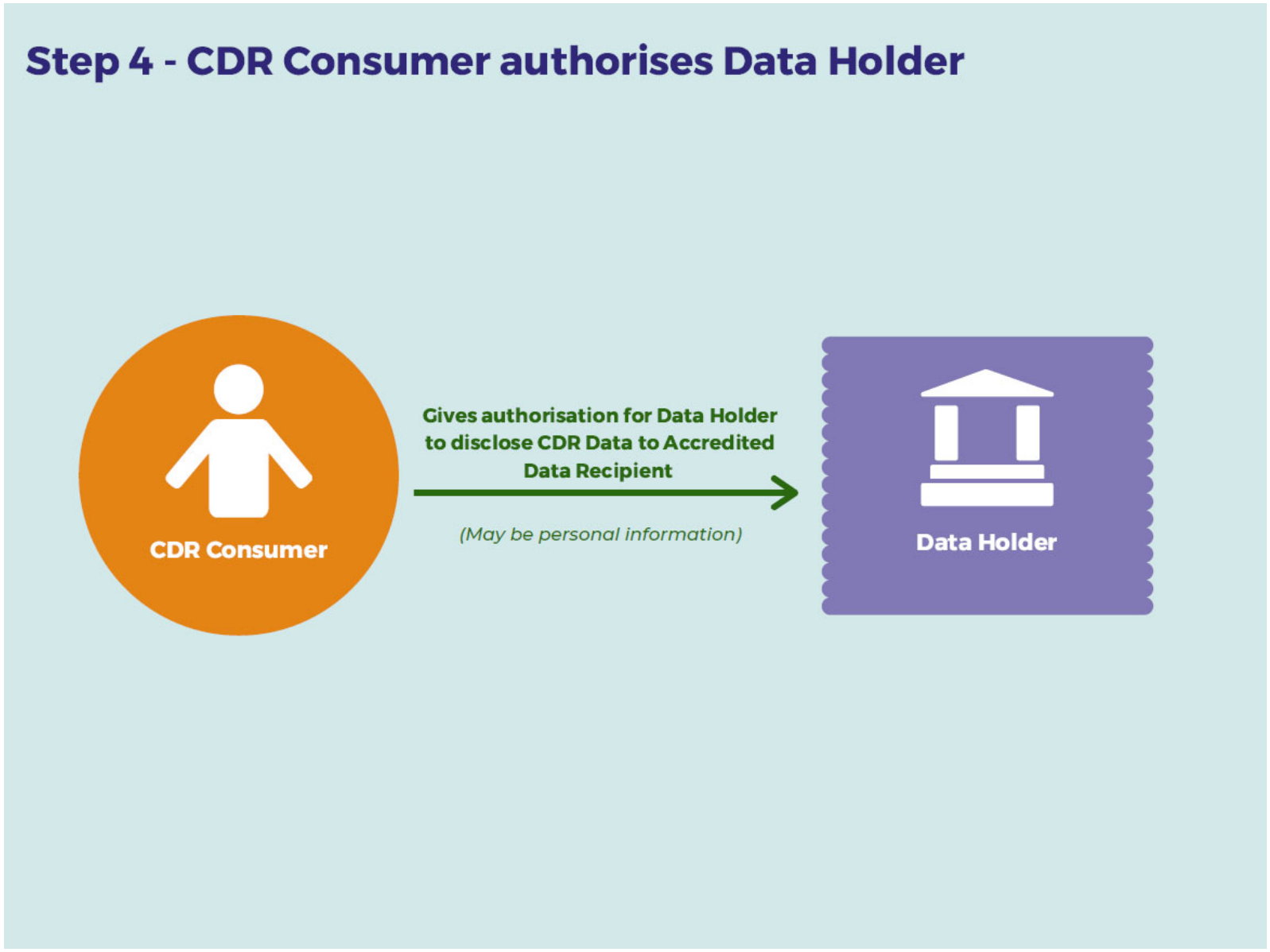






Step 2 - Accredited Data Recipient uses the ACCC CDR ICT system to obtain technical information to send request to Data Holder

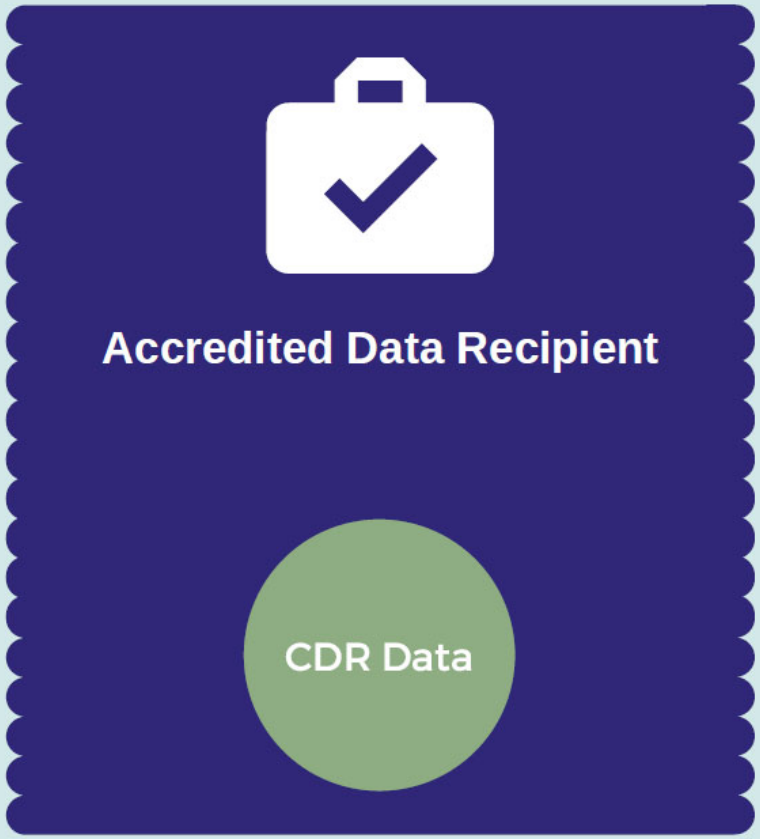

Step 3 - Accredited Data Recipient sends request to Data Holder on behalf of CDR Consumer and redirects CDR Consumer to Data Holder's systems
CDR Consumer
Redirect CDR Consumer to Data Holder's systems
Accredited Data Recipient
CDR Consumer uses one-time password and usual banking credentials
Request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

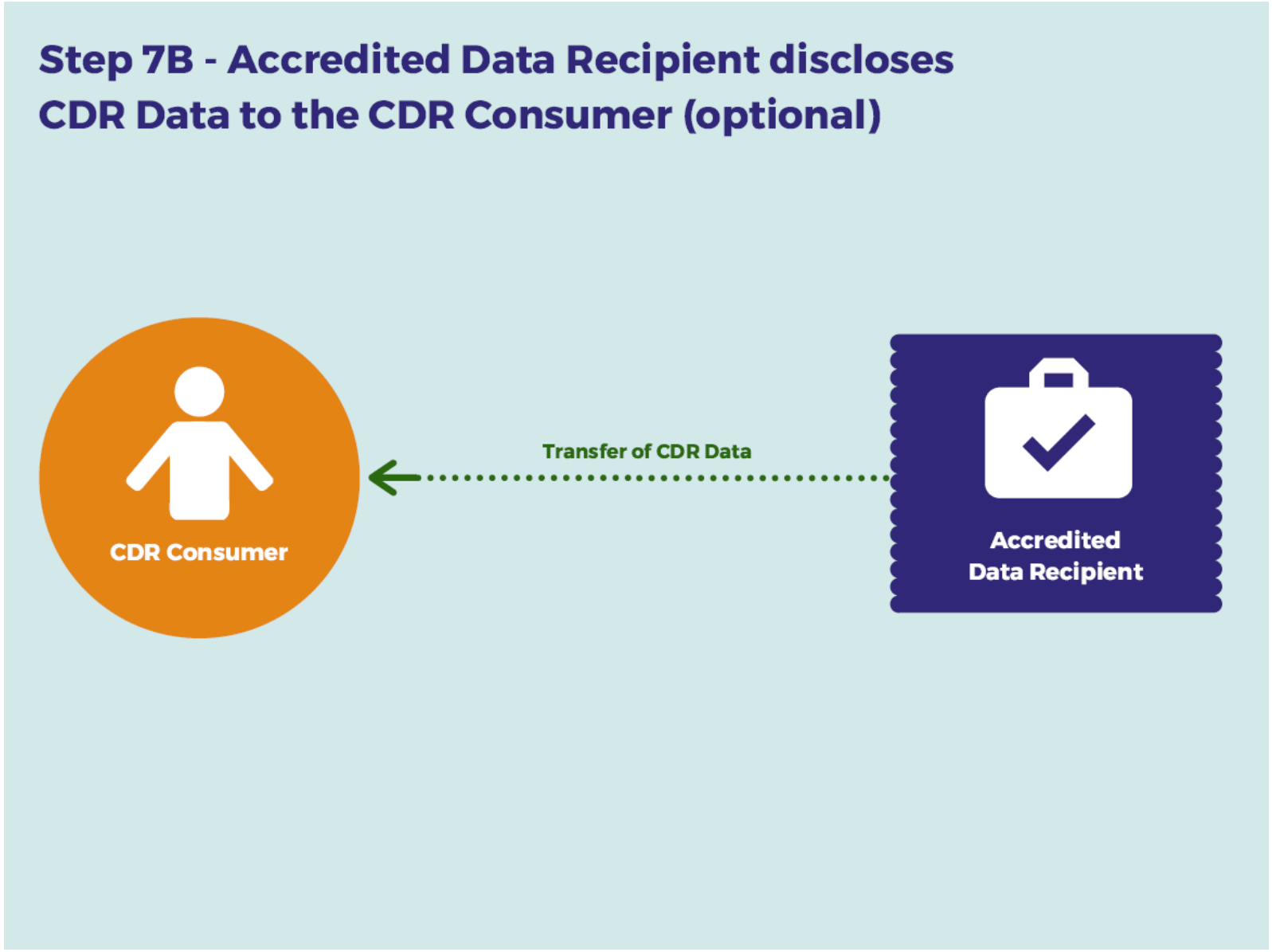


Step 5 - Data Holder checks credentials of Accredited Data Recipient using ACCC CDR ICT system (and Accreditation Register)

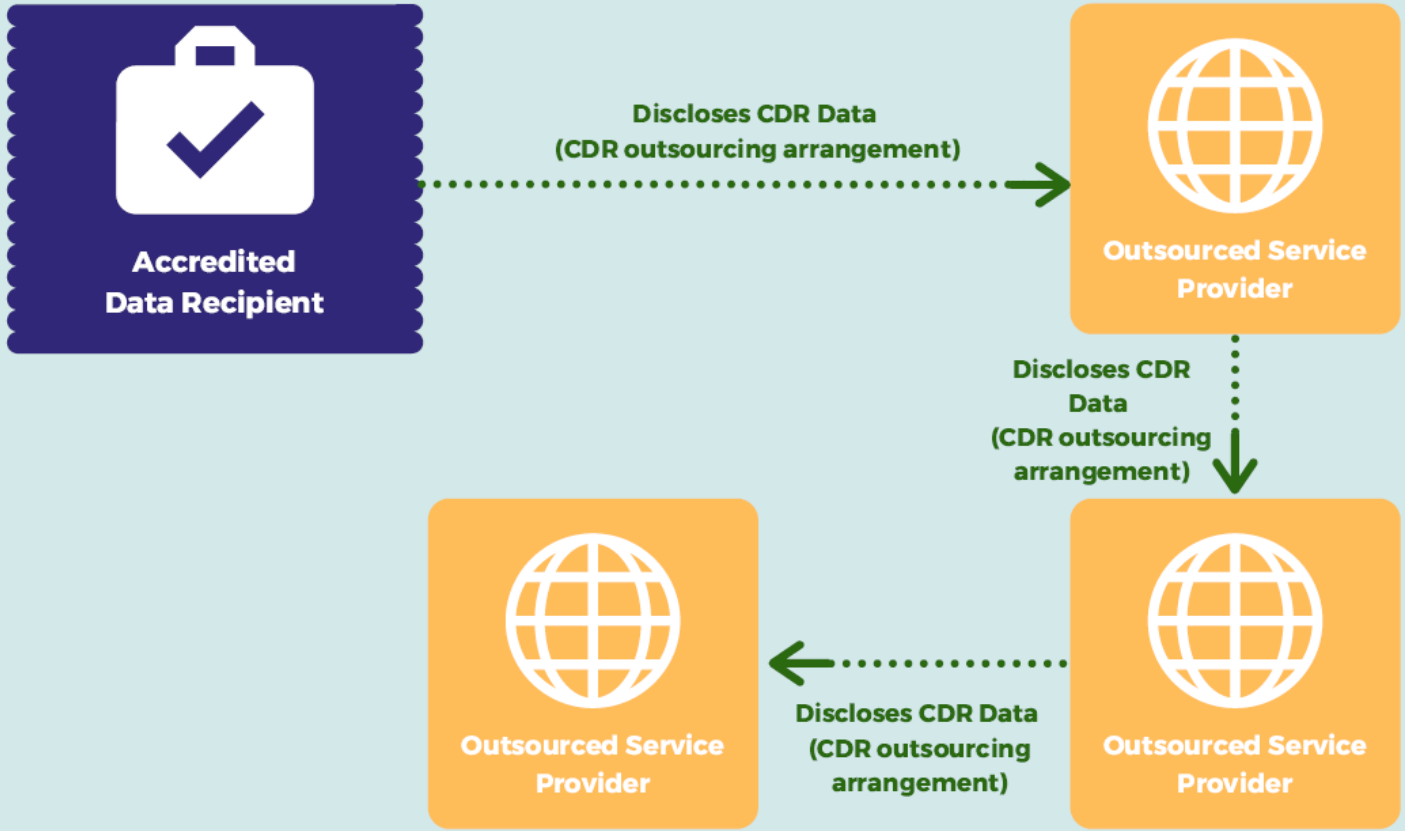
Step 6 - Data Holder sends CDR Data to the Accredited Data Recipient and Accredited Data Recipient collects the CDR Data

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

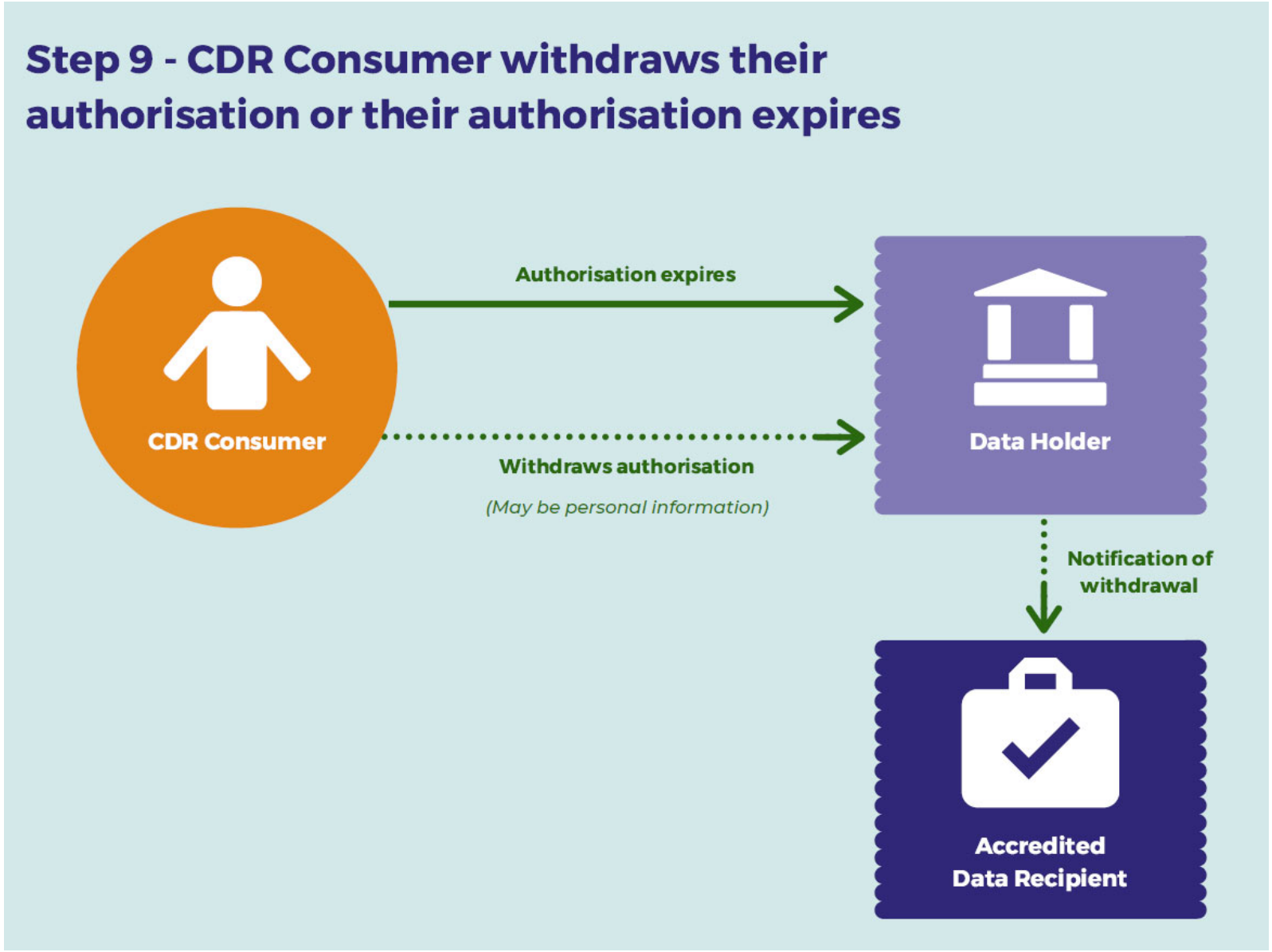


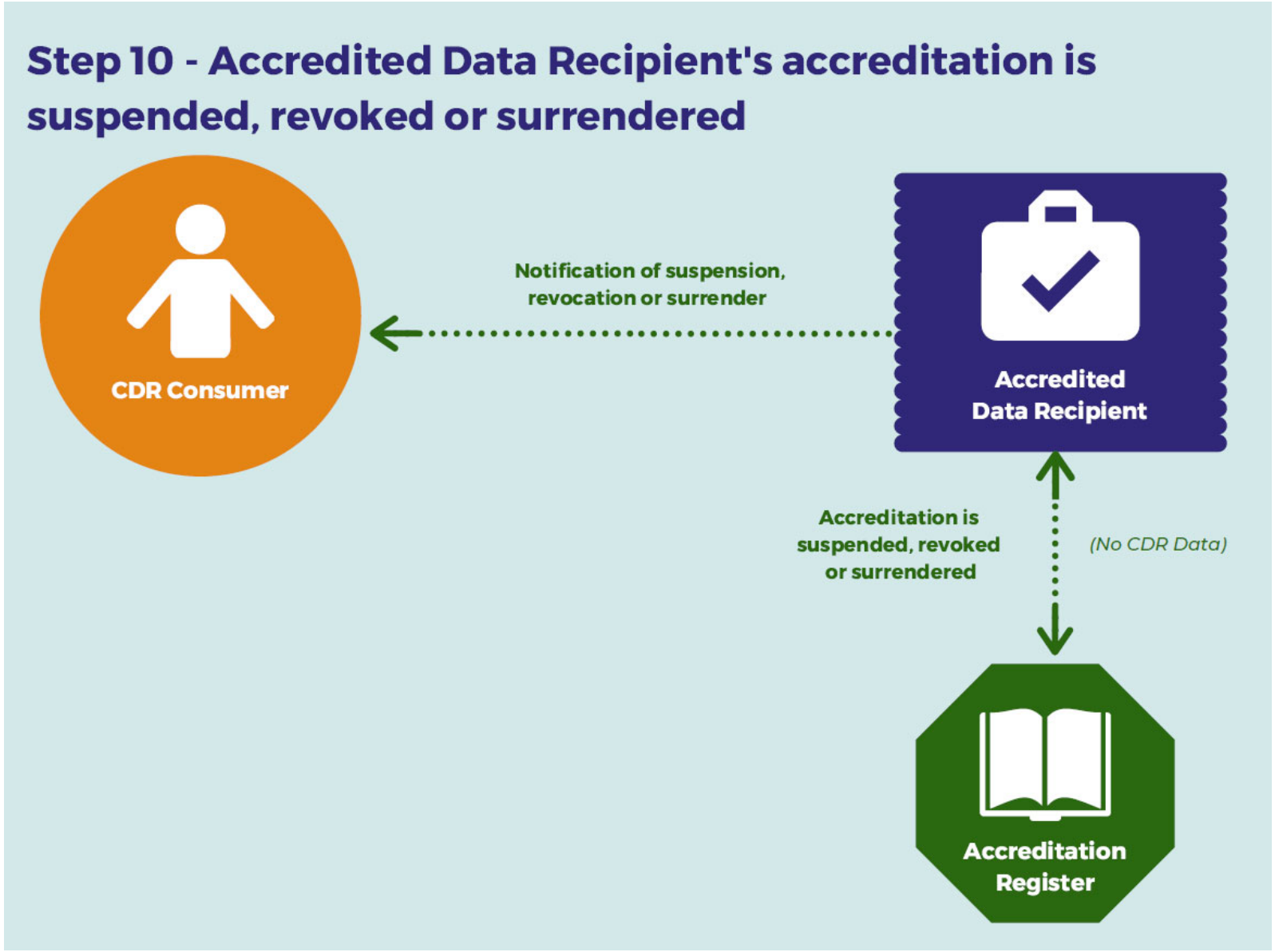


Step 7C - Accredited Data Recipient discloses CDR Data to outsourced service provider (optional)



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





Attachment 3 List of Materials Reviewed

1. *Treasury Laws Amendment (Consumer Data Right) Bill 2019* (as introduced into the House of Representatives on 13 February 2019).

2. *Competition and Consumer (Consumer Data) Rules 2019* (Exposure Draft – 29 March 2019).

3. *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019* (Exposure Draft).

4. Draft API standards (v0.9.5) (as published by Data61).

5. Draft Information Security profile (as published by Data61).

6. Draft of the Consumer Experience Guidelines (CX Guidelines) (as published by Data61).

7. Independent Information Security Report.

8. Phase Two CX Research reports (as published by Data61).

9. *Treasury Laws Amendment (Consumer Data Right) Act 2019.*

10. *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019.*

11. *Competition and Consumer (Consumer Data Right) Rules 2019* (Proposed rules – August 2019).

12. *Treasury Laws Amendment (2019 Measures No. 2) Act 2019*.

13. Privacy Impact Assessment – Consumer Data Right – March 2019, published by the Department of the Treasury (https://treasury.gov.au/publication/p2019-t361555).

14. Written submissions provided to us in response to a draft version of this PIA report by:

    14.1 Legal Aid Queensland;

    14.2 IOOF Holdings Ltd;

    14.3 Australian Retail Credit Association;

    14.4 Financial Rights Legal Centre;

    14.5 Australian Communications Consumer Action Network;

    14.6 Telecommunications Industry Ombudsman;

    14.7 Australian Privacy Foundation;

    14.8 Australian Finance Industry Association Limited;

    14.9 FinTech Australia;

    14.10 Redfern Legal Centre;

    14.11 Australian Banking Association;

14.12 Mortgage & Finance Association of Australia; and

14.13 Data Standards Body.

Note that we have also reviewed a great number of publicly available articles and papers, and guidance material and other information on numerous websites, including about the proposed implementation and operation of the CDR regime in Australia, and broadly equivalent regimes or schemes in other jurisdictions. However, we have not listed any of those materials in this **Attachment 3**.

Attachment 4 List of Stakeholders Consulted

Stakeholder consultation meetings were undertaken with the following entities (either individually or in group sessions):

1. Department of the Treasury;
2. Australian Competition and Consumer Commission;
3. Office of the Australian Information Commissioner;
4. Data Standards Body (Data61);
5. Financial Rights Legal Centre;
6. Australian Privacy Foundation;
7. Australian Banking Association;
8. FinTech Australia; and
9. Consumer Policy Research Centre.

In addition, written submissions in relation to a draft of this PIA report were received from the following entities:

1. Data Standards Chair, Andrew Stevens;
2. Financial Rights Legal Centre;
3. Australian Privacy Foundation;
4. Australian Banking Association;
5. FinTech Australia;
6. Legal Aid Queensland;
7. IOOF Holdings Ltd;
8. Australian Retail Credit Association;
9. Australian Communications Consumer Action Network;
10. Telecommunications Industry Ombudsman;
11. Australian Finance Industry Association Limited;
12. Redfern Legal Centre; and
13. Mortgage & Finance Association of Australia.