Australian Government

Consumer Data Right

CDR rules expansion amendments

Consultation Paper

September 2020

Table of Contents

Glossary 3

Executive summary 4

1. Introduction 5

    1.1. Background 5

    1.2. Overview of this consultation 6

    1.3. Indicative timeline for this consultation 7

2. Timeline for proposed rules to take effect and overview of key proposed rules 8

3. Increasing the number and types of businesses that can participate in the CDR 9

    3.1. Restricted level: limited data restriction 11

    3.2. Restricted level: data enclave restriction 13

    3.3. Restricted level: affiliate restriction 15

    3.4. Information security obligations 17

    3.5. Proposed information security requirements for accreditation 20

4. Expanding how accredited persons can work together 24

    4.1. Combined Accredited Person arrangements 24

    4.2. Transfer of CDR data between accredited persons 25

5. Greater flexibility for consumers to share their CDR data 28

    5.1. Disclosure to trusted advisors 29

    5.2. Disclosure of CDR insights 30

6. Extending the CDR to more consumers 32

    6.1. Proposed approach to enabling CDR data sharing by non-individuals 32

    6.2. Specific rules for business partnerships 34

    6.3. Secondary users 36

7. Facilitating improved consumer experiences 39

    7.1. Sharing CDR data on joint accounts 39

    7.2. Amending consents 42

    7.3. Separate consents approach 44

    7.4. A ‘point in time’ redundancy approach and the impact of withdrawing authorisation 45

7.5. Improving consumer experience in data holder dashboards 47
7.6. Use of the CDR logo 48
7.7. Permitting use of CDR data for research 48
8. Clarifying rule amendments 49
8.1. Application of product reference data rules to 'white labelled' products 49
8.2. Closed accounts 50
8.3. Reporting and record keeping requirements 50
8.4. Disclosure of voluntary product data 51
8.5. Registrar amendments 51
8.6. Commencement table amendments 51
9. Attachments 51

Glossary

ACCC	Australian Competition and Consumer Commission
Act	*Competition and Consumer Act 2010* (Cth)
ADR	Accredited data recipient
ADI	Authorised deposit-taking institution
Authorised Representative	For the purposes of this consultation document, means: • Chief Executive Officer; • Chief Financial Officer; • Chief Legal Counsel; or similar executive role with the authority to approve and accept the associated risks if implementation requirements are not met.
CDR	Consumer Data Right
Current rules	*The Competition and Consumer (Consumer Data Right) Rules 2020*
CX	Consumer experience
Open Banking Review	*Review into Open Banking: giving customers choice, convenience and confidence*, December 2017
Standard/s	The technical Consumer Data Standards made by the Data Standards Chair

Executive summary

The Consumer Data Right (**CDR**) is a significant economic reform. Rolling out on a sector-by-sector basis, it is creating an economy-wide framework to allow consumers to access data about themselves held by businesses, and direct that data to be shared with accredited third parties of their choice.

The Australian Competition and Consumer Commission (**ACCC**) made the foundational *Competition and Consumer (Consumer Data Right) Rules 2020* in February 2020.[1] These rules have supported the commencement of consumer data sharing for the major banks from 1 July 2020.

We are now consulting on a set of proposals to build on the foundational rules, and continue implementation of recommendations of the Open Banking Review that have been accepted by Government. These are intended to encourage the growth and functionality of the CDR, meet the objectives of promoting competition and innovation in the data economy, and empower consumers' choices about their data.

The proposals are designed to allow for the entry of a greater number and type of businesses in the CDR and build on changes to the rules to be made, subject to the Treasurer's consent, that allow the collection of CDR data by accredited persons. These proposals represent a significant expansion of the CDR regime and we recognise there will be a range of views on these policy issues. The ACCC will carefully consider stakeholder feedback against the criteria set out in the *Competition and Consumer Act 2010* (Cth) (**the Act**).[1]

The proposed rules we are consulting on:

- **Introduce new accreditation levels:** creating new pathways for service providers to become accredited data recipients. Proposals for new levels ('tiers') of accreditation are intended to lower barriers to entry and reduce compliance costs for service providers that do not require unrestricted access to CDR data. They also recognise that supply chains for data services regularly involve multiple service providers, and that CDR participants can appropriately manage risk and liability through commercial arrangements.
- **Provide greater choices for consumers about who they share their data with:** permitting accredited data recipients to disclose CDR data with a consumer's consent to third parties, including to their trusted professional advisors (such as accountants, tax agents and lawyers), and any third party on a limited 'insights' basis.
- **Increase consumer benefit:** allowing business and corporate consumers to access their CDR data, and adding flexibility and functionality to improve consumer experience in respect of the management of consumer consents to collect and use CDR data, joint bank accounts, and accounts that have additional card holders.

The proposals in this paper should be considered with the mark-up draft amendments to the current rules (**the proposed rules**) and the CDR Roadmap available on the ACCC website. The ACCC will also publish a draft Privacy Impact Assessment report and other technical documentation in support of the consultation soon.

We seek submissions to this consultation paper by **Thursday, 29 October 2020**. Subject to the Treasurer's consent, we intend to amend the rules in December 2020.

[1] See section 56BP of the Act.

1. Introduction

1.1. Background

The CDR is an important reform that gives Australians greater control over their data, empowering consumers to choose to share their data with trusted recipients for the purposes the consumer has authorised.

The *Competition and Consumer (Consumer Data Right) Rules 2020* have been developed to facilitate CDR as an economy-wide right. The Australian Competition and Consumer Commission (**ACCC**) made the foundational rules for CDR in February 2020 (**the current rules**).[2] This included rules to govern the application of CDR in the banking sector. Consumer data sharing obligations in the banking sector commenced on 1 July 2020.

In April 2020, the ACCC consulted on some amendments to clarify the intended operation of the current rules and to address issues that were identified during the build process for commencement of consumer data sharing on 1 July 2020. These amendments came into effect in June 2020.

The ACCC consulted on further amendments to the current rules in June 2020 to allow accredited persons to use other accredited parties (often referred to as 'intermediaries') to collect CDR data on their behalf and provide other services that facilitate the provision of goods and services to consumers ('collection arrangements'). This consultation was expedited to provide CDR participants with greater flexibility to enter into collection arrangements while longer-term measures are considered. Subject to the Treasurer's consent, the ACCC will soon amend the current rules to permit the use of accredited intermediaries to collect data through an expansion of the rules relating to outsourced service providers.

The proposed rules build on the current rules and the collection arrangement amendments. In particular, they include proposals for:

- new levels of accreditation
- permitting the transfer of CDR data between accredited data recipients
- allowing for certain disclosures of CDR data to non-accredited persons
- increasing flexibility in respect of joint accounts and the management of consumer consents
- extending the CDR framework to include more business consumers.

In proposing changes to the Rules, the ACCC has considered the following matters:

- the likely effect of the Rules on:
  - consumers, including the privacy or confidentiality of consumers' information
  - the efficiency of relevant markets
  - promoting competition
  - promoting data driven innovation
  - any intellectual property in the information to be covered by the instrument
  - the public interest

[2] The CDR rules are available at: *Competition and Consumer (Consumer Data Right) Rules 2020*.

- the likely regulatory impact of allowing the consumer data rules to impose requirements relating to the information to be covered by the Rules.[3]

1.2. Overview of this consultation

This consultation paper accompanies the draft amendments to the current Rules (**the proposed rules**) and the CDR Roadmap published on the ACCC's website. It outlines the context for the proposed rules and their intended operation, and raises questions where we are seeking specific feedback.

The proposed commencement dates for the proposed rules is a key area where we are seeking feedback from stakeholders, and in particular data holders and potential accredited data recipients. Further detail on implementation timeframes and the CDR Roadmap is provided in section 2 of this paper.

The ACCC has engaged Maddocks to undertake an assessment of the privacy impacts of the proposed rules where they affect an individual's personal information and privacy. Maddocks is preparing a draft Privacy Impact Assessment update report so this can be consulted on concurrently with the proposed rules. This will be made available on the ACCC website soon. Maddocks will finalise its report having regard to all written submissions on privacy issues received in this consultation.

How to respond

You are invited to provide written submissions to the ACCC. We particularly seek comment on the consultation questions posed in this paper and the proposed rules. However, you do not need to respond to each individual question and may decide to raise additional issues.

Please note the ACCC will provide any submissions that comment on the draft Privacy Impact Assessment, or otherwise engage with issues relevant to the Privacy Impact Assessment, to Maddocks for the purpose of finalising its report.

Submissions are due by close of business **Thursday 29 October 2020** and can be made by email to ACCC-CDR@accc.gov.au. We ask that interested parties use the email subject line 'Rules consultation' when making submissions.

We encourage stakeholders to stay informed about this consultation process and broader CDR developments by subscribing to updates via the ACCC website.

Publishing of submissions

To foster an informed and consultative process, all submissions will be considered as public submissions and will be posted on the ACCC's website. If interested parties wish to submit commercial-in-confidence material, they should submit both a public version and a commercial-in-confidence version of their submission. Any commercial-in-confidence material should be clearly identified, and the public version of the submission should identify where commercial-in-confidence material has been removed. Parties will be required to provide reasons in support of any claims of confidentiality.

Further information on the process parties should follow when submitting confidential information to the ACCC can be found in the ACCC/AER Information Policy, which sets out our general policy on the collection, use and disclosure of information. A copy of the policy is available on the ACCC website.

[3] See section 56BP of the Act.

1.3. Indicative timeline for this consultation

The following dates are indicative. Under the Act the Treasurer must consent to rule amendments before they are made by the ACCC.[4]

29 October 2020	Submissions to this consultation close
November 2020	Consideration of submissions and finalisation of proposed rules
Mid-December 2020	Earliest anticipated date for the proposed rules to be made

[4] Section 56BP of the Act.

2. Timeline for proposed rules to take effect and overview of key proposed rules

We have worked closely with the Data Standards Body to prepare the CDR Roadmap published with this consultation paper. This includes greater detail on the phasing for the introduction of the proposed rules, in addition to proposed changes to the CDR Standards to be made by the Data Standards Chair, proposed changes to the CDR Register and other matters raised by industry via GitHub.

The ACCC is conscious of the need to balance the introduction of new functionality in the CDR with appropriate implementation timeframes. We have developed the proposed commencement dates in the CDR Roadmap having regard to:

- the importance of developing the CDR beyond the foundational rules
- the potential benefits of expanding the CDR to encompass new and innovative business models
- limiting the regulatory impact on data holders where possible
- the impacts of COVID-19 on consumers and businesses
- the likely technological build impacts on CDR participants and for the CDR Register
- the corresponding Standards and CX Guidelines amendments that may be required, and
- the need to consider and incorporate feedback and views of interested parties.

Where we have not assessed proposed rules as having a potential build impacts for participants or the CDR Register, the rules are not included in the CDR Roadmap.

In addition, there are a number of proposed rules mentioned in the CDR Roadmap where we have not proposed specific commencement dates because we consider that there is a need to understand from stakeholders the complexity involved in the implementation of these proposals:

- In relation to levels of accreditation, the ACCC's preliminary assessment is that all proposals have potential build impacts. In light of consultation the ACCC will determine which proposals to proceed with or to prioritise and commencement dates following further impact analysis and assessment of stakeholder feedback.
- In relation to enabling CDR data sharing by non-individuals, business partnerships and secondary users of accounts, the ACCC considers that these are priority amendments to be implemented but recognises that the build for data holders may be relatively complex. We also recognise the approach in the current rules for a phased approach, with non-major ADIs having an appropriate additional period to the major banks to bring in new functionality.

Consultation questions

1. We welcome comments on the proposed timeline for the proposals referred to in the CDR Roadmap.

3. Increasing the number and types of businesses that can participate in the CDR

For the consumer benefits of the CDR to be fully realised, it is critical for there to be a broad range of accredited data recipients participating in the system. Broad participation is required to achieve the competition and innovation objectives of the regime, and for the CDR to support Australia's digital economy.

While the ACCC is currently considering a number of applicants for accreditation at the unrestricted level, the ACCC also wants to support participation from entities that may not be able to meet the requirements for accreditation at this level having regard to the nature of their business or the type of data they seek to access. The unrestricted level sets a high bar for accreditation in recognition that a person accredited to the unrestricted level is able to receive any CDR data in scope under the regime.

When making the current rules we noted our intention to introduce additional levels (or "tiers") of accreditation in a subsequent version of the rules. The Open Banking Report recommended that the CDR regulatory framework provide for risk-based levels of accreditation. The report envisaged that parties would be accredited to receive and hold data based on a risk assessment of the harm posed by the relevant data set or the party seeking to become accredited to consumers, and to the CDR system.[5]

The three proposals for a new level of 'restricted' accreditation, with certain kinds of restrictions, have been informed by submissions to the consultation process the ACCC conducted at the end of 2019[6] and feedback from our engagement with stakeholders to date. The three kinds of restricted accreditation in the proposed rules are the limited data restriction, the data enclave restriction and the affiliate restriction. The proposals aim to lower barriers to entry by reducing some of the upfront and ongoing costs of accreditation as compared to the unrestricted level, while maintaining appropriate information security and consumer protections.

We are seeking feedback on whether these models support use cases and whether there will be demand for these different ways of participating in the CDR regime, so we can determine which proposal/s to finalise and prioritise for implementation. We also welcome views on alternative risk-based proposals for accreditation levels and information about the types of use cases they would support.

Under the current rules, the accreditation criteria at the unrestricted level, in broad terms, are that a person must:

- take the steps outlined in Schedule 2 to protect CDR data (the information security criterion)
- have internal dispute resolution processes that meet the rules
- be a member of a recognised external dispute resolution scheme
- have an address for service, or, if a foreign entity, have a local agent that has an address for service
- be a fit and proper person as defined in the rules
- have adequate insurance or a comparable guarantee.

[5] Open Banking Review, page 25.

[6] ACCC consultation on facilitating participation of intermediaries in the CDR regime (available here).

The CDR accreditation system is a core element of the CDR and is intended to support consumer trust in the CDR regime. In developing the proposed rules, the ACCC has assessed these criteria and considers that each is relevant to an assessment of whether a person should be accredited, regardless of accreditation level. However, in order to lower barriers to entry and the ongoing cost of participation in the CDR system, the ACCC considers that it is appropriate to adopt a risk-based approach to information security, and has sought expert cyber security advice on how this could be implemented. For the proposed restricted level of accreditation, we consider that the aims of the accreditation process can be appropriately met through a tailored attestation and self-assessment process, complemented by a targeted audit and compliance program.[7]

Our accreditation proposals at the restricted level reflect this approach either by:

- applying a subset of the requirements in Schedule 2
- reducing information security requirements, where the applicant leverages the accreditation of an unrestricted person, and/or
- reducing the evidentiary requirement that applies at the accreditation stage and on an ongoing basis.

A summary of the information security criteria that we propose would apply to the restricted level of accreditation is at section 3.5. These criteria were informed by a risk assessment of the different models, which are set out in detail at sections 3.1 to 3.3. The summary sets out how requirements would apply if each model were granted a different kind of access, meaning that a person accredited to the restricted level would require separate accreditation for the enclave, affiliate or limited data restriction.

However, an alternative to this would be to provide for a general restricted level of accreditation, covering each model we chose to take forward. Such an approach may have administrative and commercial benefits, as it would allow the flexibility for a person accredited at the general restricted level to access data subject to any conditions imposed by the Data Recipient Accreditor. Such conditions may require the person accredited at the general restricted level to fulfil certain requirements, such as to have a sponsor before they can access data as an affiliate. We welcome feedback on this issue (see consultation question 2).

Besides information security, the proposed rules envisage that a person seeking accreditation at the restricted level will otherwise be required to meet the remaining accreditation criteria in rule 5.5, including the requirement to be a fit and proper person and requirements relating to dispute resolution. The insurance criterion is already risk-based and capable of flexible application to new levels of accreditation, because it requires adequate cover (see the supplementary accreditation guidelines on insurance, available here).

Key proposed rules

- Subdivision 5.2.1A Levels of accreditation
- Rule 5.5 Criteria for unrestricted, data enclave and limited data accreditation
- Rule 5.5A Criteria for affiliate accreditation
- Schedule 2 Clause 1A.1 Application of provisions of this Schedule to different accredited persons

[7] For the ACCC and OAIC joint compliance and enforcement policy (available here).

Consultation questions

2. The proposed rules include three discrete kinds of restricted accreditation (i.e. separate affiliate, data enclave or limited data restrictions). We welcome views on this approach and whether it would provide sufficient flexibility for participants. In responding to this question you may wish to consider whether, for example, restricted accreditation should instead be based on a level of accreditation that permits people to do a range of authorised activities.
3. We also welcome views on alternative risk-based restrictions that could apply to a lower level/s of accreditation, as envisaged by the Open Banking Report, including views on whether, and in what way, an approach based on volume (for example, volume of customers or customer records), could provide an appropriate basis for developing levels of accreditation.

3.1. Restricted level: limited data restriction

The limited data model is a form of restricted accreditation based on the relative risk of particular data in scope under the CDR. This form of accreditation is intended to apply across sectors such that a person will be able to collect data that has been assessed as lower risk compared to the complete range of data in scope under the unrestricted level of accreditation. As new sectors are brought into the CDR, a risk assessment will be conducted and consultation carried out with industry to determine what types of data could be included at this level.

Figure 1: Limited data restriction

*Accredited Data Recipient access to CDR data is limited to particular data clusters

Having regard to the datasets available in the CDR in the banking sector, the proposed rules contemplate that a person with the limited data restriction would be permitted to collect, from data holders, data that relates to:

- bank accounts
- basic customer data
- payees
- regular payments.

This translates to the following datasets (or 'authorisation scopes') in the Standards, set out in Table 1 below.

Table 1: Preliminary assessment of risks associated with data sets

Scope name	Description	Indicative risk level
Basic Bank Account Data	This includes basic information about a customer's accounts. It includes simple account information such as an account balance. It does not include account identifiers, product information or transaction data.	Low
Detailed Bank Account Data	This includes detailed information about a customer's accounts. It is an additional authorisation scope to Basic Bank Account Data and is meaningful if the Basic Bank Account Data scope is also authorised. It includes basic account information plus account identifiers and product information. It does not include transaction data.	Medium
Basic Customer Data	This includes personally identifiable information about the customer. For retail customers, this is information about the customer themselves. For business customers, this includes the name of the specific user but also information about the business. It includes name and occupation for individuals and name, business numbers, and industry code for businesses. It does not include date of birth for individuals.	Low
Bank Payee Data	This includes payee information stored by the customer. It includes payee information such as billers, international beneficiaries, and domestic payees.	Medium
Bank Regular Payments	This includes regular payments. It includes Direct Debits and Scheduled Payments.	Medium

This is a preliminary assessment of the indicative risk of the data sets and is based on the relative sensitivity of this data compared to other data in scope under the regime. Data relating to a customer's banking transactions, for example, would not be included in this model, due to its potential to reveal more sensitive information about a consumer.

The ACCC is cognisant that the risk of particular CDR data is highly contextual and that data can have a cumulative risk when combined with other data (whether publicly available data or not). However, recommendation 2.8 in the Open Banking Review was to develop risk-based levels of accreditation based on data 'type', and to do this, it is necessary to engage with relative risk of the data that is, and will be, in scope under the CDR. As part of this consultation, we welcome views about the appropriateness of our preliminary risk assessment.

Accreditation criteria for the restricted level (limited data restriction)

If the limited data model were implemented as a distinct kind of restricted accreditation, a person with this access would be required to meet the accreditation criteria in rule 5.5, namely:

- have internal dispute resolution processes that meet the current rules
- be a member of a recognised external dispute resolution scheme
- have an address for service, or, if a foreign entity, have a local agent that has an address for service
- be a fit and proper person to be accredited at that level

- have adequate insurance or comparable guarantee.

With respect to information security obligations, see section 3.5.

Key proposed rules

- Rule 5.1A Levels of accreditation
- Rule 5.1C Limited data accreditation
- Rule 5.2(2) Applying to be an accredited person
- Schedule 2 Clause 1A.1 Application of provisions of this Schedule to different accredited persons
- Schedule 3 Clause 7.2A Limited data level accreditation

Consultation questions

4. What are your views on the low to medium classification of risk for the data set out in Table 1?
5. Are the accreditation criteria that apply to a person accredited to the restricted accreditation level (limited data restriction) appropriate for that level?
6. Do you consider the restricted level (limited data restriction) would encourage participation in the CDR? What are the potential use cases that this level of accreditation would support, including use cases that would rely on the scope of data available under this level increasing as the CDR expands to cover new sectors beyond banking?

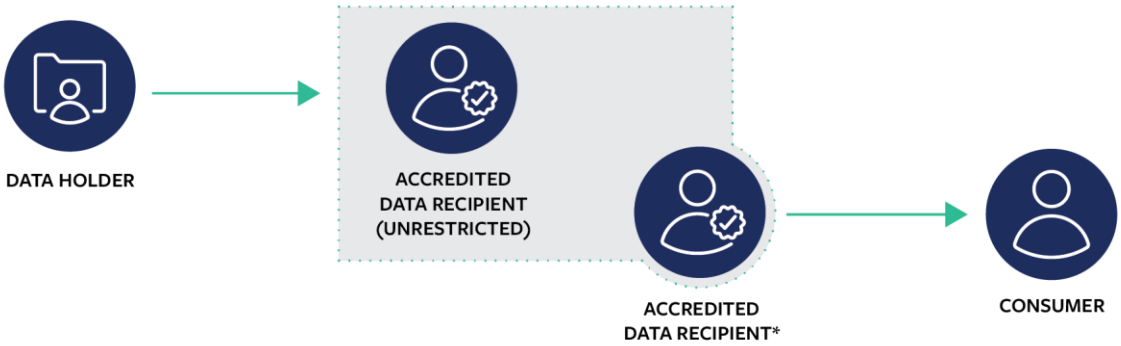
3.2. Restricted level: data enclave restriction

The restricted level (**data enclave restriction**) engages with the idea in the Open Banking Review that parties accredited at a restricted level 'could work with higher-risk data sets behind the data security firewalls of higher tier accredited parties'.[8] The proposed rules develop this concept by requiring the person accredited at the restricted level to have a relationship with an unrestricted accredited data recipient that has established a data 'enclave' (the **enclave provider**).

A person accredited at this restricted level (the **principal**) would be able to access any CDR data collected and held by the enclave provider on its behalf through a combined accredited person (**CAP**) arrangement (see section 4.1). In addition, the principal could host applications in that environment (i.e. the application that the principal provides to consumers). The principal would not be able to access data outside the enclave or download local copies of the data to another environment.

[8] Open Banking Review, page 25.

Figure 2: Data enclave restriction



*ADR may only access CDR data within the unrestricted ADR's data environment

Example of data enclave arrangement

Polis, an enclave provider, offers accredited persons different service offerings:

- the bronze service – where it collects and holds CDR data on behalf of principals
- the silver service – where it collects and holds CDR data on behalf of principals, and also offers principals a platform service with access to Polis's proprietary 'out-of-the-box' algorithms
- the gold service – where it collects and holds CDR data on behalf of principals, and also partners with them to perform data analytics and insight extraction tailored to the principals' needs.

Umbel, a small start-up, enters into a CAP arrangement with Polis and opts to use its bronze service. Umbel hosts its software product and undertakes its own data analysis within the enclave provided by Polis.

As a principal will leverage the information security capabilities of the enclave provider, a principal will need to meet a subset of the Schedule 2 requirements either in full or partially (see section 3.5).

Key proposed rules

- Rule 1.1B Combined accredited person (CAP) arrangements
- Rule 5.1A Levels of accreditation
- Rule 5.1B Data enclave accreditation
- Rule 5.1C Limited data accreditation
- Rule 5.2(2) Applying to be an accredited person
- Rule 5.5 Criteria for unrestricted, data enclave and limited data accreditation
- Rule 5.17 Grounds for revocation, suspension and surrender of accreditation as accredited person
- Schedule 2 Clause 1A.1 Application of provisions of this Schedule to different accredited persons

Consultation questions

7. Do you consider the data enclave restriction would increase participation in the CDR? Where possible, please have regard to potential use cases in the banking sector and

future CDR sectors.

8. Should the combined accredited person (CAP) arrangement between an enclave provider and a restricted level person include additional requirements, for example, in relation to incident management between the parties?
9. Should there be additional requirements under Part 1 of Schedule 2 for enclave providers in relation to the management of data enclaves?

3.3. Restricted level: affiliate restriction

Under this model, a person accredited to the unrestricted level (**sponsor**) could certify to the Data Recipient Accreditor that it has a commercial relationship with a third party (**affiliate**) and is satisfied that the affiliate meets the accreditation criteria at rule 5.5. Particular information would be required to be supplied by the sponsor for this purpose. This information would provide the basis for the Data Recipient Accreditor to be satisfied that the affiliate of the unrestricted person should be granted accreditation. A person could be an affiliate of multiple sponsors, allowing them to receive relevant data from each one.

Figure 3: Affiliate restriction

[1] Data flow in accordance with ADR-to-ADR transfer for combined accredited person arrangement

This model is intended to leverage the due diligence that many persons already undertake in relation to third party partners before sharing information with them, and engages with risk on the basis of the risk the affiliate presents to consumers and to the CDR regime, as envisaged by the Open Banking Review.[9]

An affiliate would only have access to CDR data collected by their sponsor. This could be either through a CAP arrangement – where the sponsor collects CDR data on the affiliate's behalf (see section 4.1) or ADR to ADR transfers – where the consumer has a direct relationship with the sponsor and gives a disclosure consent to the sponsor to disclose data to an affiliate (see section 4.2). An affiliate, as an accredited person in its own right, will be subject to all of the obligations under the CDR regulatory regime, including with respect to seeking consent, deletion and de-identification of CDR data, and the privacy safeguards.

A sponsor that has provided certification to the Data Recipient Accreditor about its affiliates will be subject to additional liability under the rules as a result of providing that assurance. The sponsor will need to take reasonable steps to ensure its affiliates continue to comply with the accreditation requirements and the ongoing obligations of an accredited person, and a civil penalty provision could apply for failing to take those steps. The failure to take reasonable steps, particularly where it results in or contributes to a breach of CDR obligations by an affiliate, may be grounds for suspension or revocation of

[9] Open Banking Review, page 25.

the accreditation of the sponsor. As accredited persons in their own right, affiliates could still be liable for misuse of CDR data or failing to meet other obligations under the regime.

Accreditation process for affiliates

A sponsor will be required to attest to the Data Recipient Accreditor that its affiliates meet the accreditation criteria and provide certain evidence in support. For example, the sponsor would be required to provide an assertion that the affiliate is a member of the relevant external dispute resolution scheme, plus their membership number. With respect to information security, the sponsor will be required to provide, with its application for an affiliate's accreditation, an attestation statement by the affiliate which confirms implementation of the requirements and controls in Schedule 2. As for the other types of restricted accreditation, the statement should be made by an Authorised Representative[10] of the affiliate. An affiliate will also be required to complete a self-assessment against Schedule 2. The self-assessment should provide details as to how the controls are implemented within the affiliate's CDR data environment.

For an affiliate to maintain its accreditation, a sponsor will need to annually attest that the affiliate continues to meet the accreditation criteria. This will include providing evidence of an annual self-assessment and attestation statement by each affiliate regarding continued compliance with Schedule 2.

Persons accredited to this level would be subject to a targeted audit program to be developed by the ACCC and OAIC as part of their general compliance activities.

Example of affiliate arrangement based on ADR to ADR transfers
Podium, a platform service that offers consumers a good or service as well as the ability to download apps from its add-on marketplace and share their data with them, is an unrestricted accredited person that acts as a sponsor in the CDR system. Podium undertakes due diligence of the third parties that host apps on its platform, and certifies to the Data Recipient Accreditor that those third parties meet the accreditation criteria in order to be accredited as affiliates of Podium. Podium relies on the ADR to ADR transfer rules to share data with its accredited affiliates, at a consumer's request, in situations where a consumer downloads the affiliates' apps from its marketplace.

Example of an affiliate arrangement based on CAP
Puggle, a start-up, wants to provide an account aggregation service directly to its customers, using CDR data. Puggle already partners with Wattle Bank, which is a person accredited at the unrestricted level, in relation to Puggle's other services. Wattle Bank chooses to sponsor Puggle as an affiliate, enabling Puggle to use CDR data for the new service. Consumers would have a direct relationship with Puggle to receive the account aggregation service. However, as an affiliate, Puggle relies on Wattle Bank to collect CDR data on its behalf under a CAP arrangement. Many consumers that use Puggle do not otherwise have a direct relationship with Wattle Bank. Wattle Bank provides certification to the Data Recipient Accreditor on an annual basis about Puggle's continued ability to meet the accreditation criteria for an affiliate.

Key proposed rules

- Rule 1.10B Combined accredited person (CAP) arrangements

[10] See the definition in the Glossary.

- Rule 5.1A Levels of accreditation
- Rule 5.1C Limited data accreditation
- Rule 5.1D Affiliate accreditation
- Rule 5.2(2) Applying to be an accredited person
- Rule 5.5A Criteria for affiliate accreditation
- Rule 5.17(1) Grounds for revocation, suspension and surrender of accreditation as accredited person
- Schedule 2 Clause 1A.1 Application of provisions of this Schedule to different accredited persons

Consultation questions

10. Do you consider the affiliate restriction level would increase participation in the CDR? Where possible, please have regard to potential use cases in the banking sector and future CDR sectors.
11. Should there be additional requirements under Part 1 of Schedule 2 for sponsors?
12. Where a sponsor and affiliate rely on a CAP arrangement, should the CAP arrangement include additional requirements, for example, in relation to incident management between the parties?
13. The draft rules envisage that all of Schedule 2 will apply to an affiliate of a sponsor. However, depending on the relationship between the sponsor and the affiliate, there may be options to reduce the risk associated with this model which in turn could result in less controls being relevant for some affiliates. We are interested in views on whether a distinction could, or should, be made for different levels of access to data between sponsors and affiliates (some examples below), and, if so, what approach to assurance of the information security criterion may be appropriate.

    Example level 1: affiliate is able to obtain access to any CDR data collected by the accredited sponsor and all data is held and managed on the affiliate member's systems.

    Example level 2: affiliate is able to access all data sets, but uses some of the sponsor's systems and applications to access or manage the data.

    Example level 3: affiliate obtains access to a limited amount of CDR data held by the sponsor, or entirely uses the accredited sponsor's systems and applications to access or manage the data.

3.4. Information security obligations

The proposed rules contemplate that attestation statements and self-assessments would be provided to the Data Recipient Accreditor on an ongoing basis for persons accredited to the restricted level, and for unrestricted accredited persons that act as an enclave or sponsor in the CDR regime. This would apply as a default condition of accreditation, which is at Schedule 1 to the proposed rules.

In respect of the accreditation application stage, our intention is that the approved form for accreditation would similarly require applicants for accreditation at the restricted level to provide an attestation and assessment about their compliance with Schedule 2. The requirements in relation to the information security criterion would be further

explained in the guidelines issued by the ACCC in its capacity as the Data Recipient Accreditor. The approved accreditation forms and guidelines would also set out the specific requirements applying to sponsors and enclave providers.

Restricted level

Accreditation application

For the data enclave or limited data accreditation, an applicant will be required to provide an attestation statement ('restricted level attestation') which confirms implementation of all security controls as outlined in section 3.5, which would apply instead the independent assurance report (or equivalent report) required at the unrestricted level. The statement would need to be signed by an Authorised Representative[11] of the accredited person.

In addition, an applicant for data enclave or limited data accreditation will need to complete and provide to the Data Recipient Accreditor a self-assessment ('restricted level assessment') against the security controls. We envisage that the self-assessment would provide details as to how the controls are implemented within the applicant's environment.

Ongoing obligations

On an ongoing and annual basis, a person accredited to the restricted level will be required to provide a self-assessment and attestation regarding its compliance with the information security requirements to the Data Recipient Accreditor.

For the affiliate restriction (see section 3.3), we intend for the restricted level attestation and self-assessment to be provided by the sponsor on behalf of its affiliates to the Data Recipient Accreditor.

The ACCC anticipates that a targeted compliance and audit program for persons accredited to the restricted level would be developed by the ACCC and OAIC as part of their general compliance activities.

Enclave providers

Noting the additional risks associated with maintaining and operating a data enclave, there are a number of key controls in Schedule 2 relevant to the secure operation and management of an enclave by an enclave provider (see section 3.5). These controls would already apply as part of the enclave provider's unrestricted accreditation.

To provide the services of a data enclave provider, we envisage that an unrestricted accredited person would be required to provide an attestation statement which confirms implementation of the security controls outlined in section 3.5 with specific regard to management of the enclave. The statement would be in addition to the person's requirements for unrestricted accreditation. A data enclave provider would then be required to maintain their annual requirements for accreditation, and provide an annual attestation regarding their continued compliance with the specified controls pertaining to the enclave.

When completing assurance reports in line with their requirements for unrestricted accreditation, data enclave owners would be encouraged to expand the scope of those reports to include processes specific to the management of data enclave members.

[11] See the definition in the Glossary.

Sponsors

Similarly, we envisage that specific controls in Schedule 2 will need to be implemented specifically by an unrestricted accredited person that seeks to act as a sponsor in the CDR system. These controls, with the exception of third party management, would already apply as part of the unrestricted person's accreditation (see 3.5), however, sponsors would need to implement the controls specifically in respect of their affiliates.

All accredited sponsors will be required to provide an attestation statement ('sponsor attestation' which confirms implementation of the security controls as outlined at 3.5. The statement will be provided in addition to the assurance provided in order to be accredited to the unrestricted level, as it would include attestation against the additional responsibilities, referred to above, including the person's ability to monitor, assess and manage the relationship with its affiliates. The statement would need to be signed by an Authorised Representative[12].

Accredited sponsors would also be required to provide a self-assessment ('sponsor assessment') against the security controls referred to above to the accrediting body. The self-assessment would provide details as to how the controls are implemented within the accredited sponsor's business.

On an annual basis, a sponsor will be required to provide an attestation and assessment ('sponsor attestation' and 'sponsor assessment') regarding continued compliance with the sponsor-specific controls in Schedule 2.

Reporting period

The proposed rules also include an amendment to the definition of the 'reporting period' in Schedule 1 of the rules. This will allow the Data Recipient Accreditor to determine that the reporting period for an accredited person to be the financial or calendar year and will allow appropriate flexibility for the Data Recipient Accreditor to manage the ongoing reporting obligations under Schedule 1.

[12] See the definition in the Glossary.

3.5. Proposed information security requirements for accreditation

	Unrestricted level of accreditation			Restricted level of accreditation		
Evidentiary requirement (application):	**Independent assurance report**			**Attestation statement and self-assessment**		
Evidentiary requirement (ongoing):	**Independent assurance report (biannual)** **Attestation statement (biannual)**			**Attestation statement and self-assessment (annual)**		
Schedule 2 requirements	**Unrestricted**	**Unrestricted + enclave provider**	**Unrestricted + sponsor**	**Data enclave restriction**	**Affiliate restriction** Note: See consultation question 13.	**Limited data restriction**
Part 1						
1.3 – Step 1—Define and implement security governance in relation to CDR data	Applies in full	*Meets in capacity as an unrestricted accredited person*		Applies in full	Applies in full	Applies in full
1.4 - Step 2—Define the boundaries of the CDR data environment	Applies in full			Applies in full	Applies in full	Applies in full
1.5 - Step 3—Have and maintain an information security capability	Applies in full			Applies in full	Applies in full	Applies in full
1.6 - Step 4—Implement a formal controls assessment program	Applies in full			Applies in full	Applies in full	Applies in full
1.7 - Step 5—Manage and report security incidents	Applies in full			1.7(2) 1.7(3)(b) 1.7(3)(c)	Applies in full	Applies in full

	Unrestricted level of accreditation			Restricted level of accreditation		
Evidentiary requirement (application):	**Independent assurance report**			**Attestation statement and self-assessment**		
Evidentiary requirement (ongoing):	**Independent assurance report (biannual)** **Attestation statement (biannual)**			**Attestation statement and self-assessment (annual)**		
Schedule 2 requirements	**Unrestricted**	**Unrestricted + enclave provider**	**Unrestricted + sponsor**	**Data enclave restriction**	**Affiliate restriction** Note: See consultation question 13.	**Limited data restriction**
				1.7.4		
Part 2						
2.2(1) An accredited data recipient must have processes in place to limit the risk of inappropriate or unauthorised access to its CDR data environment.	Applies in full	Applies in full Note: a person would need to implement these controls specifically for the enclave (e.g. implement processes to limit the risk of inappropriate or unauthorised access to the enclave).	2.2(1)(i) Note: Applies in respect of each affiliate.	Applies in full	Applies in full	Applies in full
2.2(2) An accredited data recipient of CDR data must take steps to secure their network and systems within the CDR data environment.	Applies in full	2.2(2)(d) Note: Implement specifically for the enclave.	2.2(2)(d) Note: Applies in respect of each affiliate.	Applies in full	Applies in full	Applies in full
2.2(3) An accredited data recipient must securely manage information assets within the	Applies in full	Applies in full Note: Implement specifically for the	N/A	N/A	Applies in full	Applies in full

	Unrestricted level of accreditation			Restricted level of accreditation		
Evidentiary requirement (application):	**Independent assurance report**			**Attestation statement and self-assessment**		
Evidentiary requirement (ongoing):	**Independent assurance report (biannual)** **Attestation statement (biannual)**			**Attestation statement and self-assessment (annual)**		
Schedule 2 requirements	**Unrestricted**	**Unrestricted + enclave provider**	**Unrestricted + sponsor**	**Data enclave restriction**	**Affiliate restriction** Note: See consultation question 13.	**Limited data restriction**
CDR data environment over their lifecycle.		enclave.				
2.2(4) An accredited data recipient must implement a formal vulnerability management program to identify, track and remediate vulnerabilities within the CDR data environment in a timely manner.	Applies in full	Applies in full Note: Implement specifically for the enclave	N/A	Applies in full Note: implementation restricted to the devices the restricted members use to access the data enclave or host their network from which they access the data enclave.	Applies in full	Applies in full
2.2(5) An accredited data recipient must take steps to limit prevent, detect and remove malware in regards to their CDR data environment.	Applies in full	Applies in full Note: Implement specifically for the enclave	N/A	Applies in full Note: anti-malware and anti-virus, application whitelisting and web and email content filtering, specifically only for the devices the restricted members use to access the data enclave.	Applies in full	Applies in full

	Unrestricted level of accreditation			Restricted level of accreditation		
Evidentiary requirement (application):	**Independent assurance report**			**Attestation statement and self-assessment**		
Evidentiary requirement (ongoing):	**Independent assurance report (biannual)** **Attestation statement (biannual)**			**Attestation statement and self-assessment (annual)**		
Schedule 2 requirements	**Unrestricted**	**Unrestricted + enclave provider**	**Unrestricted + sponsor**	**Data enclave restriction**	**Affiliate restriction** Note: See consultation question 13.	**Limited data restriction**
2.2(6) An accredited data recipient must implement a formal information security training and awareness program for all personnel interacting with CDR data.	Applies in full	N/A	N/A	Applies in full	Applies in full	Applies in full
2.2(7) Third party management	N/A	N/A	Applies in full Note: Applies in respect of each affiliate.	N/A	N/A	N/A

4. Expanding how accredited persons can work together

To support a flexible and dynamic CDR ecosystem, the proposed rules will also expand the types of arrangements that accredited parties may put in place to share and deal with CDR data. The objective of these proposed rules is to provide to range of options for accredited parties to work together and to support the development of a varied and innovative service offerings to consumers.

4.1. Combined Accredited Person arrangements

In June 2020, we consulted on combined accredited person (**CAP**) rules to facilitate the collection of CDR data by an accredited person ('intermediary'). As a result of that consultation, subject to the Treasurer's consent, the ACCC will soon make collection arrangement rules that expand the existing CDR outsourcing rules and permit an accredited outsourced service provider to collect CDR data on a person's behalf.

The proposed rules retain the concept of Combined Accredited Person arrangements but these rules are intended to apply in a different way to the expanded outsourcing rules. In the context of the present consultation, the CAP rules are about enabling a restricted accredited person to work with an unrestricted accredited person in two situations:

- to support data enclave restricted accreditation (where it would be mandatory to use a CAP arrangement), or
- to support affiliate restricted accreditation (where it would be optional to use a CAP arrangement).

At the restricted level (data enclave restriction), a person accredited to this level (the principal) must enter into a CAP arrangement with an unrestricted accredited enclave provider, for the unrestricted enclave provider to collect data and hold it in its enclave on behalf of the principal. The CAP arrangement may also include the use of that data by the provider on behalf of the principal (see section 3.2).

Similarly, at the restricted level (affiliate restriction), an affiliate may enter into a CAP arrangement so that their unrestricted sponsor collects CDR data on their behalf from a data holder. This is in addition to sponsors and affiliates being able to offer discrete goods or services to consumers, and use ADR to ADR transfers to facilitate data sharing between them (see 4.2).

Where a CAP arrangement is in place, rule 7.4 (notifying the collection of CDR data) and 7.9 (notifying the disclosure of CDR data) apply only in relation to the provider, and rule 7.10(1)(a) requires the provider to be identified.

Under the enclave or affiliate restricted models of accreditation (as supported by a CAP arrangement), both principal and provider will be acting in their capacity as accredited persons. As accredited entities, both the principal and the provider will have obligations under the CDR rules including in relation to their collection, use and disclosure of data. Section 84(2) of the Act may also apply such that conduct engaged in by the provider on behalf of the principal may be deemed to be conduct engaged in by the principal.

Key proposed rules

- Rule 1.10B Combined accredited person (CAP) arrangements
- Rule 5.1B Data enclave accreditation

- Rule 5.1D Affiliate accreditation

Consultation questions

14. We consider that in the case of a CAP arrangement, it is appropriate for the principal (having the relationship with the consumer) to be responsible for ensuring that customer-facing aspects of the CDR regime are delivered (for example, dashboards and any customer-facing communications, including in relation to dispute resolution). We welcome views on this position.

4.2. Transfer of CDR data between accredited persons

Permitting transfer of CDR data between accredited persons will facilitate an efficient data supply chain, leading to data-driven innovation. Innovation in the CDR is likely to result in new products and services for consumers that are convenient and tailored to their circumstances.

The proposed rules will permit accredited persons to collect and disclose CDR data between themselves in order to offer goods and services to consumers. The transfer of CDR data will likely involve commercial arrangements between accredited persons. An ADR that transfers CDR data under the proposed rules would not be precluded from charging a fee for this service.

The proposed rules require a two-step process in order for the disclosure to occur:

1. The CDR consumer has a valid consent to collect, and a valid consent to use, in place with the accredited person (**ADR 1**)
2. The consumer has a valid consent to disclose in place with the accredited data recipient (**ADR 2**).

The transfer of the data is not restricted to two accredited persons, and it may be that CDR data is transferred to other accredited persons or to a non-accredited person, as contemplated at section 5 of this consultation document. Similarly, the proposed rules would not limit the transfer of CDR data to persons accredited at the 'unrestricted' level, but the rules would not permit a person with the limited data level of accreditation to rely on these rules to obtain CDR data from another accredited person that it could not itself collect.

These proposed rules are distinct from those proposed at section 4.1 above, as those rules authorise accredited persons to partner together to deliver a particular good or service to a consumer. However, the proposed rules in this section permit accredited persons to transfer CDR data between themselves in order to offer consumers *distinct* goods or services requested by consumers. For example, one accredited person could offer a product comparison service and recommend a product of another accredited person. With a consumer's consent, the first accredited person could transfer the consumer's CDR data to another accredited person in order for the consumer to acquire the recommended product.

The transfer of CDR data between accredited persons could be initiated in two ways:

1. ADR 1 may recommend the good or service of ADR 2 to the consumer
2. the consumer may independently seek the good or service directly from ADR 2.

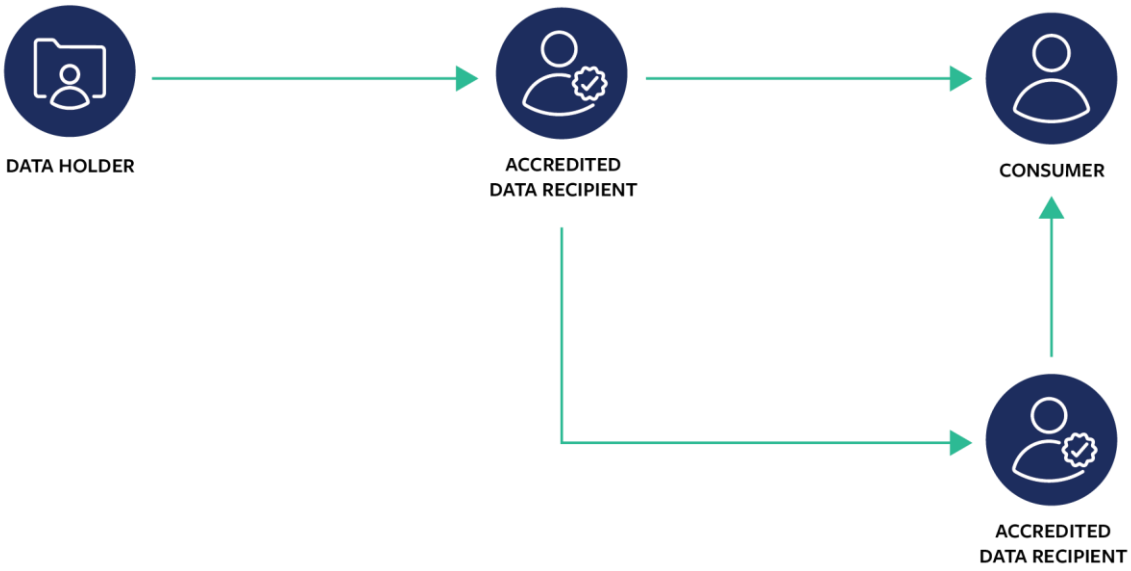
In order for ADR 1 to recommend the good or service of ADR 2, it must have a direct marketing consent in place and reasonably believe the CDR consumer may benefit from

the good or service offered by ADR 2. Alternatively, ADR 1 may recommend the good or service of ADR 2 if that is the nature of the service it is offering (such as a product comparison service).[13]

Where CDR data is transferred between accredited persons and each accredited person is providing a good or service to the consumer, each must independently provide consumer dashboards, CDR receipts and the appropriate notifications.[14] Transfers between accredited persons may also be a mechanism to support voluntary 'centralised dashboards' until such time that consent or authorisation data is designated (if ever).

We are proposing that while there may be CX Standards and/or Guidelines that apply to the consent processes, there would be no technical data standards that govern how the CDR data must be transferred in the first instance. Instead, this would be left to commercial arrangements. Over time, technical data standards may be developed and introduced to support interoperability, however, this is not currently contemplated.

Figure 4: Transfer of CDR data between accredited persons



Key proposed rules

- Rule 1.10A Types of consent
- Rule 4.3 Request for accredited person to seek to collect CDR data
- Rule 4.4 Consumer data request by accredited person to data holder
- Rule 4.7A Consumer data request by accredited person to accredited data recipient
- Rule 4.7B Accredited data recipient may ask eligible CDR consumer for AP disclosure consent

Key proposed rules relating to dealing with CDR data

[13] See Office of the Australian Information Commissioner, 'Chapter 7: Privacy Safeguard 7 — Use or disclosure of CDR data for direct marketing by accredited data recipients or designated gateways', in particular examples one and two (available here).

[14] See for example, rule 4.20.

- Rule 7.5(1)
- Rule 7.5(3)
- Rule 7.5(3)

Consultation questions

15. Should consumers be able to consent to the disclosure of their CDR data at the same time they give a consent to collect and a consent to use their CDR data?
    a. Is the proposed threshold for being able to offer an alternative good or service in rule 7.5(3)(a)(iv) appropriate?
    b. The transfer of CDR data between accredited persons will be commonly facilitated through commercial arrangements. Should those commercial arrangements be made transparent to the consumer and, if so, to what extent?

5. Greater flexibility for consumers to share their CDR data

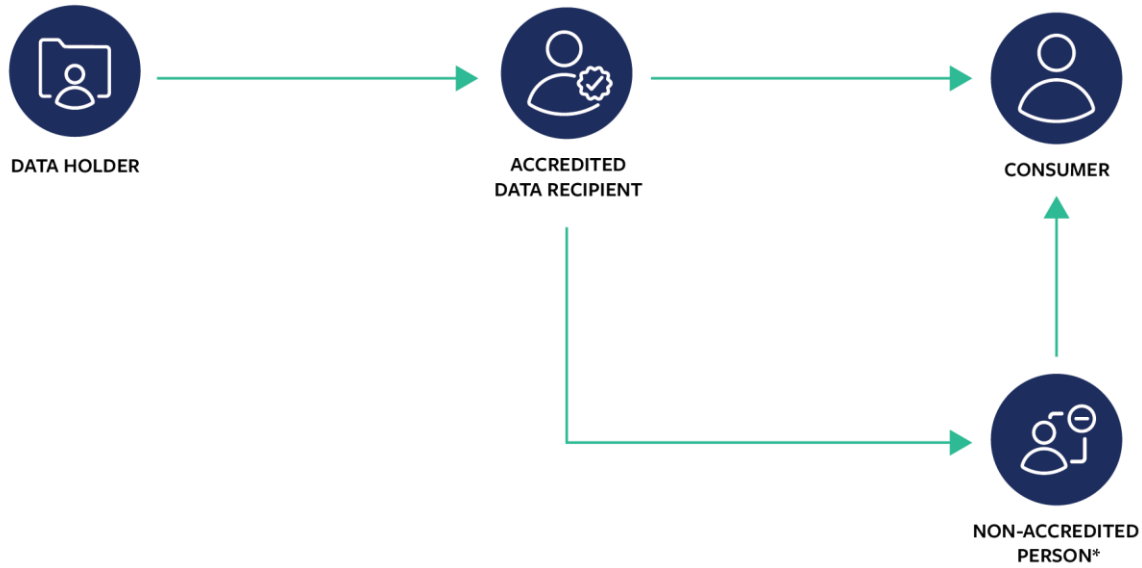
Consumers routinely entrust their sensitive data to others for a range of reasons. In respect of banking data, consumers share their data so they can receive professional services — for example, when seeking services from their accountant or tax agent. Consumers may also share their banking data to demonstrate their financial status — for example, as part of an application for credit. The CDR offers an opportunity for consumers to share their data in an efficient, secure and cost effective way.

Under the current rules, consumers are able to consent to an ADR collecting and using their CDR data. The ADR may then disclose CDR data to the consumer themselves as part of providing a good or service or to an outsourced service provider that supports the delivery of the good or service to the consumer. However, the rules do not currently permit the disclosure of CDR data by the ADR to other parties that the consumer may wish to share their CDR data with.

The following sections discuss proposed rules that would allow ADRs, with consent from a consumer, to:

- disclose CDR data to a trusted advisor who falls within a specified professional class, and
- disclose limited 'insights' derived from CDR data to any nominated person.

Figure 5: Disclosures to non-accredited perons



* The non-accredited person is limited to receiving limited 'insights' or is the consumer's trusted advisor

Expanding the CDR regime to allow for the disclosure of CDR data to non-accredited persons is consistent with the principles of consumer choice and control which underpin the CDR regime. However, we recognise that stakeholders will hold a range of views on the inherent risks to consumers of allowing disclosures of CDR data to non-accredited persons. While recognising these risks, we consider it is important to consult on measures that will encourage participation in the CDR and benefits for consumers, including through expanding the range of service offerings that CDR participants can provide.

The proposed rules authorise an ADR to disclose CDR data to non-accredited persons at the consumer's request, however, the rules do not require ADRs to do so. Therefore, disclosures to non-accredited persons will only occur where an ADR wishes to offer this functionality to consumers. The ADR would not be precluded from charging a fee for this service.

We anticipate that disclosures of this kind are likely to occur in the context of an established commercial relationship between the ADR and the non-accredited person. For example, an accountant may recommend services of a particular ADR, or the ADR may identify accountants the consumer may use and transfer their CDR data to. This context provides incentives for ensuring good consumer experience and trust and to mitigate the risk of reputational damage arising from unauthorised disclosure of data.

However, we recognise that allowing the disclosure of CDR data to non-accredited persons is a significant shift in the CDR regime, which currently only permits accredited persons to receive CDR data (with the exception of outsourced service providers). While non-accredited parties are often subject to regulatory requirements, including under professional regulatory regimes and protections set out in the *Privacy Act 1988*, they would not be subject to the requirements of the CDR framework. As such, there would be no obligation on non-accredited parties to delete data in accordance with any election made by the consumer as this election only applies to CDR data held by an accredited person. We therefore consider that these kinds of disclosures should be limited.

If an ADR offers this functionality, the proposed rules require the ADR to ask for the consumer's consent to disclose their CDR data to a non-accredited person separately from the initial consent to collect and use their CDR data. Distinguishing the consumer's consent for the ADR to collect and use their CDR data from consent to disclose that data reflects the fact that the purpose and scope of these consents differs.

The ADR will be required to update the consumer dashboard to record the nature of each disclosure consent, and for each disclosure, details of to whom the CDR data was disclosed and when. Similarly, the ADR would be required to keep records of the consents provided and each of the disclosures made in accordance with the disclosure consent.

When asking for the consumer's consent to disclose to the non-accredited person, the ADR will need to comply with any standards made by the Data Standards Chair and have regard to CX guidelines made by the Data Standards Body. Any standards or guidelines may incorporate, for example, warnings that the non-accredited person may not be subject to the *Privacy Act 1988* (Cth).

5.1. Disclosure to trusted advisors

The proposed rules will permit ADRs to disclose CDR data to particular classes of non-accredited persons with a consumer's informed consent. The intent of these rules is to allow consumers the choice and flexibility to consent to an ADR disclosing their CDR data to their professional advisor so they can receive professional services in a manner that is convenient and secure, and avoid situations where the consumer may otherwise need to handle their data or share their credentials to provide access to their trusted professional.

The proposed rules list a number of classes of trusted advisors that CDR data could be disclosed to and allow the ACCC to include additional classes as appropriate. We consider the following factors are relevant to the consideration of additional classes of trusted advisors:

- the likely benefit to consumers of disclosures of CDR data to the relevant class being authorised under the Rules

- whether the class is subject to existing professional or regulatory oversight, including whether the class is subject to obligations consistent with safeguarding consumer data (e.g. fiduciary or other duties to act in the best interests of their clients).

The classes currently proposed to be included as trusted advisors include: accountants, lawyers, tax agents, BAS agents, financial advisors, financial counsellors, and mortgage brokers. Consumers routinely share their banking data with members of these professionals and we consider there will be consumer benefit in allowing this to occur via the CDR.

The proposed rules set out the classes at a high level. We seek views on whether the classes need to be further defined in the rules. We also note that some of these classes will hold either an Australian financial services licence or an Australian Credit licence. We welcome views on whether these licensees should be included as a class in their own right.

Subject to the consumer's consent, the format and scope of the CDR data that an ADR could disclose to a trusted advisor is not limited. This raises a potential concern that an ADR could become a conduit for CDR data that enables other entities to receive CDR data without being accredited and attracting obligations under the CDR regime. The proposed rules seek to mitigate this risk by only permitting disclosures by an ADR who are themselves supplying a good or service to the consumer. However, we acknowledge that there are likely to be situations where a consumer would want to share CDR data with a trusted advisor and not receive a good or service from the ADR other than the secure collection, management, and disclosure of their data. We seek stakeholder feedback on how the rules could facilitate disclosures to trusted advisors in such circumstances without unintended consequences.

5.2. Disclosure of CDR insights

The proposed rules will permit ADRs to disclose an 'insight' derived from CDR data to any person with a consumer's consent. The intent of this rule is to recognise the broad range of services an ADR can provide both to consumers and third parties which, if provided with an 'insight', can be provided in a secure and safe way. This may include, for example, income and expense verification, verification of payments, or outcomes of responsible lending assessments.

The proposed rules do not seek to prescribe the specific kinds of products that are able to be offered. Instead, the proposed rules take a principled approach to defining an 'insight' as being derived CDR data that when disclosed is coupled with an identifier of the consumer, but taken without this identifier, could not reasonably be used to identify the individual consistent with the standard of de-identification set by the rules.

As drafted, 'insights' are *derived* CDR data. Therefore, they should not disclose any of 'raw' CDR data as originally disclosed by the data holder to the ADR. However, we recognise that this may preclude some use cases. We welcome stakeholder views on how insights are defined.

We acknowledge that, depending on the nature of the information product, insights derived from CDR data may still be highly sensitive to an individual. We therefore consider it is important for the ADR to provide transparency over the disclosure to the consumer. We seek stakeholder feedback on processes for affording the right level of transparency. The proposed rules would require an ADR to record when an insight was disclosed and to whom, and enable a consumer to request records of each insight disclosed by the ADR but, mindful of the overall cognitive load of the CDR consent process for consumers, the proposed rules do not require additional information to be incorporated into consent

processes.

Key proposed rules

Disclosures to trusted advisors

- Rule 1.10A(1) Types of consent
- Rule 1.10C Trusted advisors
- Rule 9.3(2) Records to be kept and maintained

Disclosures of insights

- Rule 1.7(1) Definition *CDR insight*
- Rule 1.10A(1) Types of consent
- Rule 1.14(3) Consumer dashboard-accredited person
- Rule 7.5(1) Meaning of *permitted use or disclosure* and *relates to direct marketing*
- Rule 9.3(2) Records to be kept and maintained

Consultation questions

16. To which professional classes do you consider consumers should be able to consent to ADRs disclosing their CDR Data? How should these classes be described in the rules? Please have regard to the likely benefits to consumers and the profession's regulatory regime in your response.
17. Should disclosures of CDR data to trusted advisors by ADRs be limited to situations where the ADR is providing a good or service directly to the consumer? If not, should measures be in place to prevent ADRs from operating as mere conduits for CDR data to other (non-accredited) data service providers?
18. Should disclosures of CDR data insights be limited to derived CDR data (i.e. excluding 'raw' CDR data as disclosed by the data holder)?
19. What transparency requirements should apply to disclosures of CDR data insights? For example, should ADRs be required to provide the option for consumers to view insights via their dashboard, or should consumers be able to elect to view an insight before they consent for it to be disclosed to a non-accredited person?

6. Extending the CDR to more consumers

The Open Banking Review recommended that the obligation to share data at a customer's direction should apply for all consumers holding a relevant account in Australia.

For the commencement of the CDR in the banking sector, individuals (including sole traders) aged 18 or over are currently eligible to authorise data sharing. They can do this from accounts they hold singly, or from accounts held jointly with one other individual. [15] The proposed rules will allow more business consumers, such as limited companies and business partnerships, to benefit from access to the CDR.

Extending data sharing to these consumers will increase the value created by the CDR, promoting uptake by businesses and by accredited data recipients providing innovative, business-focused products and services.

Relatedly, the proposed rules enable data sharing by individuals who are not account holders themselves, but who are authorised to transact on accounts held by other individuals. This could provide certain individuals who are not account holders, such as secondary card holders, with access to CDR data they have generated. It would also give account holders greater flexibility to delegate sharing of their CDR data to certain authorised persons.

6.1. Proposed approach to enabling CDR data sharing by non-individuals

The ACCC has sought to take a principles-based and non-prescriptive approach in designing these rules, with the aims of providing flexibility for data holders in dealing with a diverse range of business consumers, accommodating existing industry processes and systems wherever possible, and introducing an approach that can apply economy-wide. To achieve this, the proposed rules require data holders to allow non-individual consumers, such as bodies corporate, to nominate individuals (such as employees) to share CDR data on their behalf.[16]

The ACCC is not proposing that every individual who is authorised to transact on behalf of a non-individual consumer should automatically be authorised to share CDR data. We understand that businesses grant different levels of authority to transact to a wide range of individuals, including those with a relatively low degree of authority, who may not have discretion to share data externally. We therefore do not consider it appropriate to grant blanket authority to these individuals to share CDR data, which may be commercially sensitive and confidential.

Instead, the ACCC is proposing an 'opt-in' model, where a data holder must allow non-individual consumers to nominate individuals as 'nominated representatives' who can share CDR data, and manage data sharing, on their behalf. This is reflected in the proposal to oblige data holders to provide a service to their non-individual consumers to make and revoke such nominations.

[15] See Section 7.1 below for our proposal to extend CDR data sharing to joint accounts held by more than two individuals

[16] These proposed rules do not affect the existing mechanism by which an individual acting as a business, such has a sole trader, may share CDR data.

Application of the proposed rules

Under the proposed rules, a non-individual consumer would need to nominate at least one individual as a nominated representative in order for the business consumer to share CDR data.

We envisage that a nominated representative would then be able to:

- request an accredited person to provide goods or services to the non-individual CDR consumer; and
- consent to the accredited person seeking to access the CDR consumer's data.

Consistent with the consent flow for an individual CDR consumer, and in accordance with the data standards, the nominated representative would need to be authenticated by the data holder against the credentials held on the data holder's system.

We envisage that, in order to be successfully authenticated, an individual would therefore need both:

- valid credentials in relation to the non-individual consumer's account (e.g. because they are an employee authorised to transact on behalf of the non-individual); and
- current status as a nominated representative.

The nominated representative would then be able to authorise disclosure of the non-individual consumer's CDR data. If no representatives are nominated, a data holder would not be required or authorised to disclose CDR data.

The proposed rules do not set out any communications or options a data holder must provide to an individual seeking to share data on behalf of a non-individual consumer in circumstances where that individual is not a nominated representative. To the extent that communications (such as a prompt to seek to become a nominated representative) would be appropriate, we expect they could be set out in the Consumer Experience Standards following development by the DSB.

Dashboards and management of authorisations

The proposed rules also require data holders to provide a consumer dashboard to the non-individual consumer, which all of its nominated representatives would be able to access and use to manage data sharing. We consider that providing all nominated representatives with access to a single dashboard would allow non-individual consumers to share CDR data in a flexible way.

It would also ensure that authorisations given on behalf of the consumer will not be dependent on, or limited by, the involvement of any particular individual. For example, if a business chooses to revoke the nomination of a nominated representative, or if the nominated representative leaves the organisation, there would be no disruption to authorisations that had been initiated by that individual. Instead, any remaining or new nominated representative would be free to manage those authorisations on an ongoing basis.

Implementation issues

The ACCC views the extension of the CDR to business consumers as particularly important in driving the value of the CDR and its uptake by consumers and ADRs.

In terms of implementation, the ACCC expects that for ADIs that operate multiple business digital banking channels (through internet banking and/or mobile apps), the accounts in scope under the rules will initially be accounts that are made available through the ADI's primary business banking channel. In these situations, the ACCC considers that it would be appropriate for an ADI to meet its obligations under the rules by leveraging its primary business banking channel.

It is also expected that all business consumers should have the option to participate in the CDR. In practice, this would mean that a business consumer wishing to utilise the CDR, but whose products are not at that time available through the ADI's primary business banking channel, should be given the option to access the primary business banking channel by the ADI. This would allow the business customer to authorise the sharing of CDR data in relation to any product it has with the bank that is in scope under the rules. This approach will help ensure all consumers, including small, medium and institutional-sized business consumers, will have the option to participate in CDR.

If the ACCC makes these rules, we would expect to confirm the above approach (if adopted) in the accompanying Explanatory Statement, consistent with our approach to clarifying which accounts were in scope in the Explanatory Statement to the *Competition and Consumer (Consumer Data Right) Amendment Rules (No.1) 2020*.

6.2. Specific rules for business partnerships

The current policy intention is that all business partnerships should be able to share CDR data. Partnerships typically consume business-focused products and services, and should generally be treated like other business consumers, including non-individuals such as bodies corporate. However, we are conscious that there are a number of differences between non-individual consumers and partnerships. These are relevant to our consideration of how they should be accommodated by the CDR.

Business partnerships are not legal entities. This means that partners may, singly or jointly, procure products or services on behalf of the partnership. In the simplest cases, where these partners are individuals and the account is held by one or two partners, such partnerships may already be able to share data under the rules either as single individuals or via the Joint Account rules (see below for additional discussion on this point).

However, we do not consider this is a long-term, sustainable solution for the CDR. While some partnerships may be entirely constituted by individuals, partners can also be non-individuals such as bodies corporate. Further, partnerships may have employees to whom they wish to delegate the ability to share CDR data.

We therefore consider that:

- it would be inappropriate to seek to extend the rules on Joint Accounts to cover business partnerships; and
- it would be overly complex to create bespoke rules to cater for every possible permutation of partner types (e.g. partnerships made up of either individuals or non-individuals, or mixed partnerships with both types of partner).

Accordingly, the proposed rules treat business partnerships in line with the approach the ACCC is proposing for non-individual consumers. Under this approach, data holders would be required to provide business partnerships with the ability to nominate representatives to share CDR data on behalf of the partnership, and manage CDR data sharing via a single consumer dashboard, as described above.

Personal information relating to partners who are individuals

Where partners are individuals, CDR data sharing may result in the disclosure of personal information about individuals who are partners. In the banking sector, for example, customer data may include personally identifiable information where individual partners are account holders. However, we consider that a key consideration is that these individuals are acting in a commercial context, and will already have granted other partners considerable discretion to legally bind them in a number of ways.

Accordingly, we are considering the appropriate balance between the need to ensure such information is adequately protected, and the benefits to innovation and competition that are likely to arise from the enablement of CDR data sharing by business partnerships in a manner that does not impose undue regulatory burden.

Implementation issues

In terms of implementation, we expect to provide similar clarification about the banking channel/s through which we expect CDR data sharing to be enabled for business partnerships in the same way as discussed above in relation to CDR data sharing by non-individual consumers.

Subject to this, the proposed rules would apply to all business partnership accounts. However, we understand that some data holders may already be planning to enable data sharing under the existing joint account rules for all accounts held jointly by two individual account holders, including those used for business partnerships.

The ACCC's focus for the implementation of joint accounts, due to commence on 1 November 2020 for initial data holders, is on joint accounts held by two individuals for non-business purposes. We are therefore comfortable for joint accounts used for business partnerships, including those with two individual account holders, to be fully enabled when the 'business partnership rules' come into force. However, we do not want to preclude initial data holders who are working to enable these customers earlier, in accordance with the commencement table set out in the CDR rules, and we would welcome this as something that extends the reach of the CDR.

Key proposed rules

- Rule 1.7 Definitions
- Rule 1.13 Consumer data request service
- Rule 1.15 Consumer dashboard – data holder
- Schedule 3, Clause 2.1 Meaning of *eligible* – banking sector
- Schedule 3, Clause 3.2 Meaning of *required consumer data* and *voluntary consumer data* – banking sector

Consultation questions

20. We are seeking feedback on the proposal for enabling business consumers (both non-individuals and business partnerships) to share CDR data.
21. In particular, we welcome comment on the proposal to require a data holder to provide a single dashboard to business consumers which can be accessed by any nominated representative to manage CDR data sharing arrangements.
22. Are there other implementation issues the ACCC should be aware of in relation to the proposed rules for CDR data sharing by non-individuals?

23. We welcome comment on the proposed approach to require data holders to treat business partnerships in line with the approach for dealing with business consumers? Do you foresee any technical or other implementation challenges with taking this approach for business partnerships that the ACCC should take into account?
24. Should additional protections be introduced for personal information relating to business partners who are individuals?
25. Are there other aspects of the rules that may require consequential changes as a result of the enablement of business consumers? For example, are the internal dispute resolution requirements appropriate for business consumers?

6.3. Secondary users

The current rules permit eligible[17] account holders in the banking sector to share their CDR data with accredited persons. However, these rules currently do not permit anyone other than the account holder to share data relating to the account.

The proposed rules broaden the scope of the current rules and permit anyone who:

- has 'account privileges' in relation to the account holder's account, as defined in each designated sector's schedule, and
- is approved by the account holder through a 'secondary user instruction' to share CDR data relating to the account with accredited persons.

The proposed rules are intended to be flexible and recognise there are likely to be different types of secondary users between different sectors. For example, in the superannuation and insurance sectors, we understand it is common for account holders to create 'authorised users' so family members and other third parties may have access to the account(s).

For the banking sector, we consider someone with 'account privileges' should be someone who is:

- an individual who is 18 years of age or older, and
- able to make transactions on an account which is a phase 1, phase 2 or phase 3 product.[18]

Additionally, the person with account privileges must be 'eligible' to ensure authentication is possible. That is, they must have access to an account with the data holder that is open and accessible online.

Example of types of individuals who will be captured under proposed rules

Hanna has a credit card account with Globe Bank. She adds Annika as a secondary card holder, and they agree to do all their household spending on the credit card due to the additional benefits offered by Globe Bank. Hanna is legally responsible for the payments on the account although the transaction data generated on the account relates to Annika as much as Hanna, and Annika uses her own online credentials to do the monthly reconciliation. Under the proposed rules, Hanna may provide Globe Bank with a 'secondary user instruction', which will enable Annika to make consumer data requests. As the account holder, Hanna will have oversight of Annika's data sharing on the credit card account.

[17] See clause 2.1 of Schedule 3.

[18] See clause 1.4 of Schedule 3.

Consistent with the current rules, any secondary user who shares CDR data will receive a consumer dashboard with the data holder and relevant accredited persons.

The proposed rules also operate in a similar format to the joint account rules, in that where a secondary user shares CDR data, the account holder will have a consumer dashboard that:

- provides an overview of the authorisations to disclose given by secondary users
- allows them to withdraw any 'secondary user instruction' at any time.

We consider withdrawing a 'secondary user instruction' should be akin to removing a joint account disclosure option. That is, all sharing of CDR data on the relevant account by the secondary user should cease, but any authorisations in place should not be automatically withdrawn.

This is because a secondary user may have given an authorisation that relates to both (a) an account for which they are account holder; and (b) the account on which they are a secondary user. We do not consider it would be a good consumer outcome for withdrawal of the secondary user instruction on (b) to disrupt sharing from (a).

Our proposed approach ensures any other accounts associated with an authorisation continue to be shared so that the secondary user may continue to receive the requested good or service, as follows:

Example of proposed outcome where the account holder withdraws a 'secondary user instruction'

Annika is sharing her CDR data with Umbel. She is sharing:

- her personal savings account with Globe Bank
- the credit card account with Globe Bank that Hanna has enabled through the 'secondary user instruction'.

If Hanna withdraws her 'secondary user instruction', Globe Bank should cease sharing CDR data on the credit card account, but should continue to share CDR data on the personal savings account.

We are not proposing that the account holder should have granular control and be able to withdraw sharing initiated by secondary users with certain accredited persons, while allowing sharing to continue with other accredited persons. Unlike joint accounts, where both account holders have equal privileges reflecting that they each have the status of an account holder, we consider that secondary users are likely to be subordinate users, so granular controls may not be appropriate. Instead, secondary users will have 'all or nothing' CDR sharing abilities.

Example of 'all or nothing' CDR sharing abilities

Annika is sharing CDR data on the credit card account with Globe Bank that Hanna has enabled through the 'secondary user instruction' with the following accredited persons:

- Umbel
- Pard.

Hanna can withdraw her 'secondary user instruction', and cease Annika's sharing with both Umbel and Pard. However, Hanna does not have granular control and may not cease Annika's sharing with Pard, but continue to allow sharing with Umbel.

In our view, any current privileges that relate to secondary users should not be automatically extended in a CDR context. For example, if a secondary user has significant account privileges on an account now, this should not automatically translate to having a CDR 'secondary user instruction'. Instead, the account holder will still have to create a new CDR-specific 'secondary user instruction' in order for the secondary user to share CDR data. This is consistent with our approach to joint accounts.

Key proposed rules

- Rule 1.7(1) Definitions (*account privileges, secondary user, secondary user instruction*)
- Rule 1.13(1) Consumer data request service
- Rule 1.15(5) Consumer dashboard - data holder
- Schedule 3 Clause 2.1(1) Meaning of *eligible* - banking sector
- Schedule 3 Clause 2.1A Meaning of *account privileges* - banking sector
- Schedule 3 Clause 4.8(1) Consumer data requests that relate to joint accounts

Consultation questions

26. We welcome feedback on the proposals for enabling authorised users to share CDR data.
27. Should persons beyond those with the ability to make transactions on an account be considered a person with 'account privileges' in the banking sector?
28. How should secondary users rules operate in a joint account context?
29. As well as having the ability to withdraw a 'secondary user instruction', should account holders be able to have granular control and withdraw sharing with specific accredited persons that have been initiated by a secondary user?

7. Facilitating improved consumer experiences

To support consumer comprehension and trust in the CDR regime, the proposed rules seek to enhance consumer and accredited person control. These new rules also seek to reduce negative friction in consumer processes and compliance costs for accredited persons and encourage innovative use cases for the benefit of consumers.

7.1. Sharing CDR data on joint accounts

The current rules contain obligations for data holders in relation to banking products that fall within the meaning of joint accounts. Initial data holders are required to commence sharing CDR data on joint accounts from 1 November 2020, with sharing for other authorised deposit-taking institutions to commence 12 months later.

Consumer experience findings published by the Data Standards Body found that the authorisation flow provides a 'natural context' for consumers to set their preferences for sharing CDR data from joint accounts (referred to as 'preferences').[19]

The current rules do not permit consumers to set their preferences as part of the authorisation process. The proposed rules will require data holders to allow consumers to set their preferences as part of the authorisation process where consumers have not previously set up such preferences (for example, the first time the consumer initiates data sharing). This process will require compliance with CX Data Standards, if any.[20]

Currently, data holders may choose to offer the joint account management service exclusively through offline channels.[21] The proposed amendments require data holders to, at a minimum, offer the joint account management service online. Data holders may choose to also offer the joint account management service through offline channels. This amendment recognises the need to have an online process in order to support the ability to set preferences as part of the authorisation process. Under the proposed rules, joint account management services must also comply with any Data Standards in place.[22]

The proposed rules also provide for the expansion of existing protections for vulnerable consumers. Under the current rules, data holders may refuse to disclose CDR data on a joint account, or update a consumer dashboard, in circumstances where the data holder considers it necessary in order to prevent physical or financial harm or abuse.[23] The proposed rules are intended to offer vulnerable consumers protection from potential harm that may arise from sharing their CDR data. The proposed additions will enable vulnerable consumers to share CDR data on a joint account as if the account was held in their name alone, where the data holder is satisfied that to do so is necessary in order to prevent physical or financial harm or abuse.

The proposed rules also detail requirements for the joint account management service provided by data holders and notification requirements, which align with current ACCC guidance.[24] In light of feedback from CDR participants, the operation of joint account provisions is also intended to be simpler and clearer.

---

19 Data Standards Body, 'Consumer Experience Research Phase 3: Round 1 and 2', p.4 (available here).

20 Any CX Data standards will be subject to a separate consultation process before being made.

21 Clause 4.2(2)(a) of Schedule 3 of the CDR rules.

22 Any CX Data standards will be subject to a separate consultation process before being made.

23 See clause 4.7 of Schedule 3 of the CDR rules.

24 CDR Zendesk, Rules Guidance, 'Joint Account Guidance' (available here).

At this stage, the proposed rules do not require data holders to offer both 'pre-approval' (commonly referred to as 'one to authorise') and 'co-approval' (commonly referred to as 'two to authorise') disclosure options. Consistent with the approach under the current rules, the new rules propose that 'pre-approval' will be mandatory for data holders to offer, while 'co-approval' will be voluntary. We understand there are technical implementation considerations that need to be resolved before data holders should be required to offer both 'co-approval' and 'pre-approval' disclosure options to consumers.

The current rules stipulate that if joint account holders select a:

- 'pre-approval' disclosure option, both joint account holders, joint account holder A and B, may individually withdraw an approval
- 'co-approval' disclosure option, in order to withdraw an approval, both joint account holders must agree to remove it.[25]

The proposed rules depart from this approach, and would allow joint account holder B to independently withdraw the approval, regardless of the disclosure option selected. The proposed rules will increase joint account holder B's control over their CDR data, and recognise that regardless of who provides the authorisation, both joint account holders should be able to stop CDR sharing on a joint account.[26]

We understand there are a small number of joint accounts where there are three or more account holders. The proposed rules also expand joint accounts from accounts held in the name of two individuals[27] to include joint accounts held in the name of two *or more* individuals. The proposed approach to joint accounts held in the name of more than two individuals is substantially the same.

The proposed rules for amending consent and authorisation also have implications for the joint account rules. The proposed rules are to the effect that regardless of which disclosure option is selected, if joint account holder A amends an authorisation, the data holder must notify joint account holder B of the nature of the amendment. The proposed rules do not provide for joint account holder B to 'approve' any amendments to the authorisation. We consider this approach to balance the following considerations:

- the risk of 'approval' fatigue if joint account holder B is required to approve all authorisation amendments
- the potential delays in the ability to disclose data where joint account holder B is required to approve all authorisation amendments
- the oversight already provided by the notification to joint account holder B of an authorisation amendment
- the protections already offered to joint account holder B through the ability to remove an 'approval' or remove their disclosure option
- the additional technical build that would be required for data holders if joint account holder B is required to 'approve' authorisation amendments in a 'co-approval' context.

Joint account holder B will have transparency and high-level control over what CDR data can be shared by the data holder to an accredited person. It is not proposed, however, that joint account holder B will have oversight or control over further disclosure of CDR data by the accredited person. For example, if joint account holder A provides a consent

---

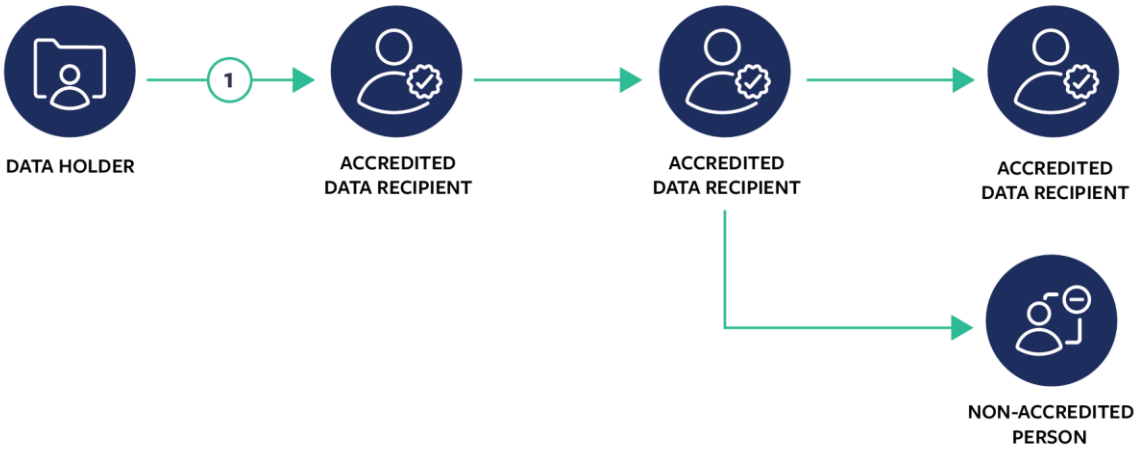
[25] Clause 4.2(2)(b) of Schedule 3 of the CDR rules.

[26] Joint account holder A could remove a joint account from sharing by amending their consent with the accredited person or if the data holder offers such functionality, removing the account from the sharing arrangement.

[27] See clause 1.2 of Schedule 3 of the CDR rules.

for an accredited person to disclose their CDR data to other persons, as contemplated in sections 5 and 4.2 of this consultation document, joint account holder B will have no transparency or notification of that disclosure. This is because data holders do not have oversight of the consents or disclosures that occur after the initial disclosure. To illustrate this point, if the data flow is as represented in Figure 6 below, joint account holder B will only be presented with the information relevant to the flow of data at step 1. It will not have oversight of any subsequent disclosures.

Figure 6: Data flow and oversight by joint account holder B



The ACCC considers the technical implementation costs for data holders and accredited persons to implement additional oversight for joint account holder B outweigh the potential benefits, particularly given accredited persons offering 'multi-party centralised dashboards' may competitively fill this gap.

Key proposed rules

- Schedule 3 Part 4 Joint accounts

Consultation questions

30. We are seeking feedback on our proposals relating to sharing CDR data on joint accounts, including:
    a. the proposed approach to require data holders to allow consumers to set their preferences (a disclosure option) as part of the authorisation process
    b. the proposed approach of allowing 'joint account holder B' to withdraw an approval at any time
    c. the expansion of the rules to include joint accounts held by more than two individuals
    d. the proposal that joint account holder B does not have to 'approve' amendments to authorisations
    e. the proposed approach that the rules do not require (but do not prohibit) the history of disclosure option selections being displayed to consumers as part of the joint account management service or data holder consumer dashboard.
31. Do the benefits of requiring data holders to display on-disclosures to 'joint account holder B' outweigh the costs?

7.2. Amending consents

Under the current rules, in order to amend a consent, consumers must create a new concurrent consent or remove an existing consent and replace it with a new one. The proposed rules seek to expand functionality, allowing consumers to have more control over their consents. This approach is consistent with the decision to increase functionality in the rules over time.

Amending consents could involve multiple attributes, including:

- adding or removing uses
- adding or removing data types
- adding or removing accounts
- amending durations
- adding or removing data holders.

The proposed rules do not take a prescriptive approach and simply authorise amendments to consent. This means accredited persons are able to determine the best approach for their particular good or service. For example, some accredited persons may offer the ability to amend multiple attributes in one consent process, while others may not.

The proposed rules also permit pre-selected options during the consent amendment process where the consumer has previously selected a particular option in the past. This includes:

- data types
- time periods
- accredited persons (in the case of disclosure consents)
- data deletion elections.

Given the separate consents approach proposed in section 7.3, as well as the ability to offer pre-selected options, we envisage the amendment process will be streamlined, allowing the consumer to focus on the changing attribute.

Where consumers amend their consent, the proposed rules require the accredited person to notify the data holder, in order for the data holder to invite the consumer to correspondingly amend their authorisation. This ensures the consumer dashboards are synchronised and technical mechanisms prevent the disclosure of CDR data no longer subject to a valid consent. In our view, the information the data holder must present to the consumer during initial authorisation[28] is also appropriate for amending an authorisation. However, we are interested in feedback on this preliminary position.

The proposed rules allow consumers to amend their consent through two mechanisms. Firstly, it is proposed that a consumer should be able to amend their consent at any time through the accredited person's consumer dashboard. Some use cases may be such that accredited persons are only be able to offer the ability to amend some aspects of a consent. However, our current preference is that accredited persons should be required to offer consumers the ability to amend the consent in the consumer dashboard to the extent possible, in order to encourage consumer control. For some use cases that may mean only offering consumers the ability to amend a consent to associate a new account or a new

[28] See rule 4.23.

data holder with the arrangement. The ACCC is interested in feedback on this preliminary position.

Example of why an accredited person may not be able to offer consumers the ability to amend data sets

Umbel is an accredited person who offers a service to consumers in compliance with the data minimisation principle. Umbel requires the collection and use of the following data types in order to provide its service:

- Account balance and details
- Transaction details
- Direct debits and scheduled payments.

Umbel cannot offer consumers the ability to remove data types in its consumer dashboard, because if consumers removed data types, it could no longer provide the requested service. Umbel also has a limited service offering, so cannot offer consumers the ability to amend a consent to add additional data types.

Secondly, it is proposed that accredited persons should be authorised to invite consumers to amend a current consent where the amendment would:

- better enable the accredited person to provide the requested goods or services to a consumer; or
- enable the accredited person to provide modified goods or services that have been agreed to by the consumer.

These limitations are proposed to ensure accredited persons are not 'spamming' consumers in order to seek additional data or uses.

Accredited persons may choose to offer multiple consent management options, such as amending consents, or withdrawing and replacing consents and concurrent consents as part of their service offering. Alternatively, an accredited person may choose to offer consumers the ability only to amend their original consents.

If the proposed rules are introduced, the technical implementation will be as per the current data standards. That is, while a consumer may be *legally* amending their consents, *technically* the process will be to call the revocation endpoints of the relevant data holder(s), and create a new consent with the "cdr_arrangement_id".[29] This means that the technical process for amending consents and authorisations will be to remove the existing consent and authorisation and replace it with a new one. The process to allow consumers to add or remove an account through processes managed by accredited persons will necessarily require re-direction to the data holder's processes. This can occur through calling existing oAuth endpoints. The Data Standards Chair may amend the data standards or create new data standards to enable technical amendments to consent in future.

If the proposed rules, or similar, are introduced the Data Standards Chair is likely to also amend the CX Standards and update the CX Guidelines accordingly.[30]

[29] Consumer data standards, Identifiers and Subject Types, CDR Arrangement ID (available here).

[30] Any CX Data Standards will be subject to a separate consultation process before being made.

Key proposed rules

- Subdivision 4.3.2A Amending consents
- Rule 4.18C Notification if consent to collect CDR data is amended
- Rule 4.22A Inviting CDR consumer to amend a current authorisation
- Rule 4.23 Asking CDR consumer to give authorisation to disclose CDR data or inviting CDR consumer to amend a current authorisation

Consultation questions

32. Should accredited persons be required to offer consumers the ability to amend consents in the consumer dashboard, or should this be optional?
33. We are seeking feedback on the proposed rules about the way accredited persons are able to invite consumers to amend their consents. Should a consumer be able to amend consent for direct marketing or research in the same way as amending consent for use of data in the provision of goods and services?
34. Should the authorisation process for amending authorisations also be simplified?

7.3. Separate consents approach

The ACCC implemented a combined concept of a 'use and collection consent' in the current rules based on earlier consumer experience findings. The ACCC is proposing to move away from this approach with the development of rules that allow for separate consents for collection of CDR data and consents to use CDR data.

Re-framing the rules so these consents are separate concepts creates more flexibility for accredited persons, and enables more granular consent options.

Example of the flexibility of separate consents

A consumer may have the following consents with an accredited person:

- Consent to collect for 24 hours;
- Consent to use for 3 months;
- Consent to direct marketing for 3 months;
- Consent to disclose to a trusted advisor on a single-occasion.

Given they are different consents, the consumer could independently withdraw or amend each consent.

Having separate consents supports the point in time redundancy approach and impact of withdrawing authorisation discussed at section 7.4 of this consultation document.

Key proposed rules

- Rule 1.10A Types of consents
- Subdivision 4.3.2 Giving consents
- Subdivision 4.3.2A Amending consents
- Subdivision 4.3.2B Withdrawing consents
- Subdivision 4.3.2C Duration of consent

Consultation questions

35. We are seeking feedback on the proposed approach of separating the consent to collect from the consent to use CDR data (rather than combining consent to collect and use).
36. Should accredited persons be able to offer disclosure consents only after an original consent to collect and use is in place (with the effect that combining a use and collection consent with a disclosure consent would be prohibited)? See also the consultation questions in section 7.2 above.

7.4. A 'point in time' redundancy approach and the impact of withdrawing authorisation

Under the current rules, there may be different outcomes depending on the action taken by a consumer to withdraw an authorisation. For example:

- if a consumer is sharing CDR data with an accredited person from one data holder, withdrawing the authorisation results in the consumer's consent to collect and use expiring and the accredited person is subsequently required to comply with redundancy requirements under privacy safeguard 12.
- if a consumer is sharing CDR data with an accredited person from multiple data holders, withdrawing an authorisation with a particular data holder results in the consent to collect and use expiring to the extent it was associated with that particular data holder only. This means the accredited person is required to comply with redundancy requirements under privacy safeguard 12 in relation to CDR data collected from that particular data holder only.
- if a joint account approval is removed by joint account holder B, the data holder must stop disclosing CDR data on the joint account. However, no communication is made to the accredited person, so redundancy obligations under privacy safeguard 12 are not relevant, and the accredited person may continue to use the CDR data already collected on the joint account.

These different outcomes may create confusion for consumers and do not support consistent messaging about how deletion and de-identification works under the CDR regime. The ACCC also understands that the consequence of having to delete or de-identify CDR data from a particular data holder only may result in significant costs for accredited persons to separate that data from a larger dataset. This may include costs associated with tagging CDR data from the point of collection. For these reasons, we are proposing to move towards a 'point in time' redundancy approach in the proposed rules.

Accredited persons may still choose to offer consumers the ability to have data become redundant at different times, if preferred. If accredited persons do intend to implement

the 'point in time' redundancy approach, it may have subsequent impacts on consumers' ability to amend a current consent. See our example of different approaches below.

For completeness, we also note these proposed rules will not displace the ability for accredited persons to retain CDR data where they are required to by, or under, an Australian law or a court/tribunal order, or where the data relates to a current or anticipated legal or dispute resolution proceeding to which the CDR entity is a party.[31]

Example of different approaches

Redundancy occurring at different times	**Point in time approach**
Umbel offers consumers the ability to amend their consents at the same time, including to remove data types that are 'optional' fields. After the amendment process, Umbel tells consumers: *You have successfully amended your consents to collect and use. We will no longer collect your **account balance and details**, and will delete all of this data we hold overnight…*	Pard offers consumers the ability to amend their consents to collect, in order to remove data types that are 'optional' fields. After the amendment process, Pard tells consumers: *You have successfully amended your consent to collect CDR data. We will no longer collect your **account balance and details**, but we will use the data we've already collected. Don't worry – when you withdraw your use consent or when it expires on 1 October, we will delete it, along with all your other data…*

As CDR expands across sectors, it will become increasingly common for consumers to have multiple authorisations in place for a single good or service (e.g. a consumer may have an authorisation with more than one data holder). In order to support the point in time redundancy approach, the impact of withdrawing an authorisation must result in the withdrawal of a consent to collect with the accredited person only. We consider amending the rules in this way will have numerous benefits, including ensuring consumers are not ceasing a consent to use without an informed understanding of the consequences from the accredited person.

The trade-off of such an approach is that consumers will not be able to cease all consents with an accredited person via their data holder. Although, in the (likely common) scenario that multiple data holders are involved in the provision of a single good or service, a consumer would be required to withdraw authorisations with each data holder individually to cease all consents with an accredited person in any event. We also consider the maximum duration of 12 months for a consent to limit potential harms that may arise from consumers attempting to cease all consents with accredited persons via their data holder.

The proposed rules require that once accredited persons are notified of the withdrawal of authorisation, they must notify the consumer to inform them that they may also withdraw the use consent, if desired. This notification must occur in writing and outside of the consumer dashboard, however it may also occur through the consumer dashboard. In our view, this ensures consumers are notified of the consequences even where they no longer use the good or service of the accredited person, as the notification does not rely on interaction with the consumer dashboard.

[31] See section 56EO of the Act.

Key proposed rules

- Rule 4.11(1) Asking CDR consumer to give consent
- Rule 4.14(1A) Duration of consent
- Rule 4.18A Notification if collection consent expires
- Rule 4.18B Notification if collection consent or use consent expires

Consultation questions

37. We are seeking feedback on the 'point in time' redundancy approach.
38. We are seeking feedback on the proposed approach where a consumer withdrawing their authorisation for a data holder to disclose their CDR data results in removal of the ADR's consent to collect only.
39. We are seeking feedback on the collection consent expiry notification and permissible delivery methods.

7.5. Improving consumer experience in data holder dashboards

Under the current rules, data holders are required to present consumers with the name of the accredited person during the authorisation process and in the consumer dashboard.[32]

The proposed rules ensure data holders are required to also display additional information to consumers that is held in the Register for the purpose of inclusion in the authorisation process or inclusion on the consumer dashboard.

Additionally, the proposed rules ensure data holders are required to display additional information received through the data standards for the purpose of inclusion in the data holder's consumer dashboard. These data standards are not yet developed, but are likely to be optional metadata for accredited persons to include in the authorisation request. Any standards developed will be subject to a separate consultation process, and interested parties may provide detailed feedback on the technological solution at this stage.

Example of a use case the proposed rules are intended to support

Botanical is the parent company of Umbel. Umbel offers consumers a tax-tracking app 'TaxCap'. TaxCap requires concurrent consents to support its use case.

Under the current rules, 'Botanical', as the accredited entity, is required to be presented to consumers by data holders during the authorisation process and on the consumer dashboard.

The proposed rules require data holders to also display to consumers information provided by Umbel in the Register for the purpose of inclusion in a data holder's consumer dashboard and authorisation process. For example, Umbel could require:

- TaxCap by Umbel

to also be presented during the authorisation process and on the consumer dashboard.

The proposed rules support data holders displaying to a consumer information as entered by Umbel in the metadata of certain data standards (for example, authorisation request metadata). This future functionality is intended to allow Umbel to have some 'free text' fields. For example, Umbel may use the free text to ensure the data holder displays their concurrent consent information in a meaningful way such as:

[32] See rules 1.15 and 4.23.

- TaxCap by Umbel – initial consent 1 July 2020
- TaxCap by Umbel – joint account 1 November 2020

Key proposed rules

- Rule 1.15(1)
- Rule 4.23(2)
- Rule 7.9

Consultation questions

40. We welcome any comment on the proposed rules to improve consumer experience in data holder dashboards.

7.6. Use of the CDR logo

The CDR logo is intended to be a symbol of trust in the CDR regime and can only be used by those CDR participants who are licensed to use the logo. The proposed rules will require an accredited person to take all reasonable steps to ensure it is licensed to use any CDR logo approved by the ACCC for the purpose of the consumer data rules and as required by the standards.

Where an accredited person fails to comply with the data standards with respect to use of the CDR logo this may constitute a ground for suspension or revocation of accreditation.

7.7. Permitting use of CDR data for research

The current rules limit ADRs from using CDR data for purposes beyond what is reasonably needed in order to provide the requested goods or services.[33] This precludes consumers from consenting to ADRs using their CDR data for research purposes where it does not relate to the goods or services requested.

Where an ADR seeks to collect and use CDR data for the purpose of providing a good or service, the proposed rules will allow ADRs to also seek the consumer's express consent to use that same data for the purposes of research. The consumer may choose to agree to this option or not. When seeking the consumer's consent, an ADR will need to provide a link to a description of the research and any benefits to be provided to the consumer as set out in its CDR policy. The benefit to the consumer could be, for example, the ADR paying a fee to the CDR consumer or providing a discount on services provided to the CDR consumer. If the consumer consents to this research use, this would allow the ADR to use the data collected for providing a good or service for other activities such as product development or business development.

As is currently the case, the ADR would only be able to disclose or sell CDR data if it was de-identified in accordance with the CDR data de-identification process.[34]

[33] Rule 7.5(1); 7.6(1).

[34] See rule 1.17.

8. Clarifying rule amendments

8.1. Application of product reference data rules to 'white labelled' products

White labelled products are products created and operated by one entity (a 'white labeller') and branded and retailed to consumers by another entity (a 'brand owner'). They are prominent in credit card and home loan products in the banking sector.

The white labeller, often an ADI, is typically responsible for the creation and operation of the product, and compliance with regulatory obligations. The brand owner, sometimes an ADI, is typically responsible for branding and retailing the product, by marketing the product to consumers under its brand. We consider it is important for white label products to be included in the CDR regime.

The proposed rule amendments will affect the product data request rules only and are designed to provide clarity and certainty about: (a) how the product data request rules apply where both the white labeller and the brand owner are data holders (e.g. where both are ADIs); and (b) the information that must be provided in relation to white label products such as credit cards, where there is no requirement to provide a product disclosure statement. This formalises guidance previously issued by the ACCC on its expected approach to disclosure of product data for white label products.[35]

The proposed amendments clarify that for white label products where more than one data holder is involved, the data holder responsible for responding to product data requests is the data holder who enters into a contractual relationship with the consumer.[36] We understand that the consumer generally enters into a contractual relationship with the white labeller.

This is intended to avoid unnecessary duplication across multiple data holders by allowing flexibility for (a) the other data holder (i.e. the data holder who does not enter into a contractual relationship with the customer) to also respond to product data requests if they choose to, or (b) for the data holders to reach agreement on who will meet the obligation in practice, while retaining clarity about which data holder retains the regulatory obligation.

Finally, the proposed rules address uncertainty around the product data that the data holder must disclose for certain white label products.[37]

We understand that products such as credit cards may not be subject to the regulatory requirement to provide a product disclosure statement. Further, product data for a white label product may not be contained on the white labeller's website. Stakeholders have requested clarity about what data (if any) must be included in such circumstances. Proposed amendments to the product data disclosure rules seek to clarify the sources of product data in these cases by introducing a new definition, 'disclosure document', to ensure that products that are not subject to the requirement to provide a product disclosure document are explicitly covered by the rules.[38]

We note that the proposed amendments do not affect the rules relating to consumer data requests. We are continuing to develop our position with respect to consumer data

[35] See *Approach to disclosure of product data: white label products* on the ACCC website.

[36] Proposed sub-rule 2.3(1), and sub-rules 2.4(4) and 2.4(5).

[37] Proposed sub-rule 2.4(3) and 2.4(6).

[38] Proposed sub-rule 2.4(3)(b)(ii)(B).

requests for white label products and would welcome stakeholder engagement about this matter.

Key proposed rules

- Rule 2.3 Product data requests
- Rule 2.4(2A)-(6) Disclosing product data in response to product data request

Consultation questions

41. We are seeking feedback on whether the proposed amendments place the obligation on the party best placed to meet the obligation.
42. Are there any technical or other implementation issues of which the ACCC should be aware?

8.2. Closed accounts

The current rules state that required consumer data, which a data holder must provide upon request, does not include transaction data in relation to an account that was closed more than 24 months before the request. However, the rules do not apply the same exclusion to account data or product specific data that relates to closed accounts.

The proposed rules align the data sharing requirements for closed accounts across transaction data, account data and product specific data. The effect of these amendments is that a data holder only required to share these categories of data if the request is made within 24 months of the account being closed.

8.3. Reporting and record keeping requirements

Proposed rules relating to reporting, record keeping and audit rules:

- provide further clarity on the ACCC's expectations regarding CDR participants' record keeping and reporting obligations,
- improve the quality and format of the information required to be reported to the ACCC and the OAIC, and
- enhance CDR consumer access to records being held by data holders and ADRs which relate to them.[39]

The proposed rules have been developed in response to CDR participant feedback about the current operation of the record keeping and reporting obligations.

Consequential amendments are also proposed with respect to the management of consumer consents and the application of product reference data rules to 'white labelled products'.

Our understanding is that these amendments will not impose a significant burden or implementation cost to data holders and ADRs and, as proposed in the CDR Roadmap, could commence upon the making of the proposed rules (currently expected in December 2020). We welcome feedback in relation to:

[39] Division 9.3.

- any implementation challenges or consequences that are foreseen as they relate to these proposed rules, and
- if the proposed commencement date in the CDR Roadmap is not appropriate, alternative timeframes for commencement of these rules.

8.4. Disclosure of voluntary product data

The proposed amendment will align the text of the rules around disclosure of product reference data with the simplified outline and flowchart in Part 2.[40] This is to specify that a data holder that discloses any requested voluntary product data must do so through its product data request service and in accordance with the data standards. A civil penalty provision could apply for failing to comply.

8.5. Registrar amendments

The proposed amendments will provide the Registrar with powers to protect the security, integrity and stability of the Register and associated database.

The Registrar will be able to take steps to prevent the Register and associated database being used to make consumer data requests to a data holder, for a period up to 10 days, if the Registrar reasonably believes this is necessary to protect the security, integrity and stability of the Register.

The Registrar will also be able to direct an accredited person to not make consumer data requests or data holders not to respond to consumer data requests for a period up to 10 days if the Registrar reasonably believes it is necessary to protect the security, integrity and stability of the Register or associated database.

8.6. Commencement table amendments

The ACCC intends to update the commencement table, setting out the mandatory data sharing obligations for data holders (also known as the 'phasing table'), to reflect the revised phasing table published on the CDR website and relevant exemptions granted by the ACCC. Consequential amendments will remove references to 'voluntary participating ADIs' as this 'swim lane' is not relevant to the revised phasing table, and reflects the proposal to remove this concept from the rules consulted on in February 2020. Data holders that are ready to share certain phases of CDR data early will be permitted to do so, subject to completion of any testing (via the Conformance Test Suite) and other on-boarding requirements. Further information will be provided about this process via future CDR newsletters.

9. Attachments

The following attachments to this consultation are available on the ACCC website:

- the mark-up draft amendments to the current rules
- the CDR Roadmap.

A draft Privacy Impact Assessment report and other technical documentation will also be published on the ACCC website soon.

[40] Proposed sub-rule 2.4(2A).