Australian Government

Office of the Australian Information Commissioner

OAIC Submission to the CDR Rules Expansion Amendments Consultation

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

29 October 2020

OAIC

Contents

Overview

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the Australian Competition and Consumer Commission's (ACCC's) draft *CDR Rules Expansion Amendments* and associated consultation paper. We understand the proposed package of amendments to the *Competition and Consumer (Consumer Data Right) Rules 2020* ('existing Rules') is intended to continue the implementation of recommendations of the Open Banking Review, where these have been accepted by Government.[1]

The proposed amendments cover a wide range of policy issues, including accreditation requirements, disclosures of CDR data and insights to non-accredited third parties, arrangements to facilitate the transfer of CDR data between accredited data recipients (ADRs), joint accounts, consents and the ability to conduct research with CDR data. By way of overall comment, the OAIC is broadly supportive of the majority of positions set out in the consultation paper and draft rules. Many are privacy-enhancing and will increase choice, transparency and control for individual consumers in relation to the use of their CDR data.

However, the OAIC also notes that if enacted as drafted, the proposed Rules would mark a significant expansion of the CDR system, particularly in relation to the type and number of actors who may participate. Further, certain proposals represent a recalibration of existing CDR privacy settings, transforming the existing 'closed' CDR system into something more 'open'. We understand these changes are proposed with a view to encouraging the growth and functionality of the CDR, promoting competition and innovation in the data economy, and empowering consumers in relation to their data and acknowledge the importance of these underlying policy goals.

At the same time, we would emphasise the importance of ensuring that any privacy and security risks are appropriately mitigated, and the overall integrity of the CDR system is maintained. Robust privacy protections will be crucial to building and maintaining consumer trust and ensuring that there is consumer 'buy-in' to the CDR system. In this regard, the OAIC recommends a cautious approach be taken in relation to some of the proposals. In particular, the OAIC does not support the proposed model for the disclosure of CDR insights in its current form. The disclosure of an insight[2] generated from CDR data would be as insightful, if not more, than 'raw' CDR data itself. In our view, the current model would pose significant privacy risks for consumers, and particularly vulnerable consumers, and is therefore in need of further safeguards to ensure these risks can be appropriately mitigated. We would therefore recommend that the scope of this model be limited, in line with the recommendations outlined in this submission.

In addition, as the proposed changes to the accreditation requirements are likely to lead to increased participation by a broader range of actors in the CDR system, the nature of the CDR compliance and enforcement activities required to support the system will change. There will therefore be a need for the OAIC and ACCC to work closely together as co-regulators to ensure that any new privacy, security or general compliance risks are identified and appropriately mitigated. In this regard, we strongly

[1] See the *Review into Open Banking: giving customers choice, convenience and confidence*, December 2017.

[2] An 'insight' is information derived from a consumer's CDR data. This may include, for example, income and expense verification, verification of payments, or outcomes of responsible lending assessments: see page 30 of the paper.

support the ACCC's commitment to work with the OAIC to develop a robust and targeted audit and assessments program.[3]

Additionally, the OAIC also notes that the proposed package of amendments to the Rules may result in additional complexity both for the regulated community and consumers, particularly in relation to the navigation of the consent flow. The OAIC suggests the ACCC consider the cumulative effect of the changes when formulating the final package of amendments, and continue to work closely with the Data Standards Body to ensure that guidance for regulated entities (such as the CX standards and guidelines) is clear and supports a seamless consumer experience. This will help to reduce the risk of any consumer confusion, improve the ability of CDR entities to comply with their CDR obligations, and therefore enhance choice, transparency and control for individual consumers.

The OAIC provides comments and recommendations on the specific issues raised in the consultation paper and draft Rules below. The structure of our submission follows the format of the consultation paper, and a consolidated list of all recommendations is available in **Attachment A**. We also note the release of the Maddocks consultation document,[4] which contains a preliminary analysis of the privacy risks that may be raised by this version of the Rules, and will be used to inform the next update to the Privacy Impact Assessment (PIA) for the CDR. We strongly support the ACCC's decision to update the PIA and to consult on this document together with the consultation paper and draft rules. We recommend that the ACCC have regard to the final Maddocks recommendations as it works towards finalising this version of the Rules.

We are available to discuss our submission with the ACCC. The OAIC will update the CDR Privacy Safeguard Guidelines in due course, to assist regulated entities to understand and comply with their CDR privacy obligations.

About the OAIC and our role in the CDR system

The OAIC is Australia's independent regulator for privacy and freedom of information. The OAIC co-regulates the CDR scheme together with the ACCC. The OAIC enforces the privacy safeguards (and related Rules) and advises the ACCC and Data Standards Body (CSIRO's Data61) on the privacy implications of the CDR Rules and data standards. The OAIC is also responsible for undertaking strategic enforcement in relation to the protection of privacy and confidentiality, as well as investigating individual and small business consumer complaints regarding the handling of their CDR data.

Our goal in regulating the privacy aspects of the CDR system is to ensure that the system has a robust data protection and privacy framework, and effective accountability mechanisms to ensure consumers are protected.

[3] See, for example, pages 17 and 19 of the ACCC's *CDR rules expansion amendments Consultation Paper* ('consultation paper' or 'paper').

[4] Dated 29 September 2020.

Comments on specific issues raised in the consultation paper

Restricted accreditation

The proposed draft Rules would introduce additional levels of accreditation, in line with the recommendation from the Open Banking report that the CDR system should permit 'risk-based' levels of accreditation.[5] There is currently one 'unrestricted' level of accreditation in the CDR system, which enables an accredited data recipient (ADR) to receive all CDR data. The OAIC understands that the proposed amendments to the Rules are aimed at enabling participation from a wider range of entities, including those that may not currently be able to meet the requirements of unrestricted accreditation.

The ACCC proposes three models of 'restricted' accreditation to encourage greater participation:

- the limited data restriction
- the data enclave restriction, and
- the affiliate restriction.

For each of these restricted models, the accreditation criteria that apply at the unrestricted level would apply in the same manner, except in relation to the information security 'evidentiary' requirements. In this regard, the ACCC is proposing to impose 'lighter' evidentiary requirements, meaning that applicants for restricted accreditation would not be required to provide assurance reports.[6] Instead, they would provide an attestation statement confirming implementation of all relevant information security controls.[7] The draft Rules then set out specific arrangements for each of the restricted accreditation models (which are explored further below).

By way of general comment, the OAIC appreciates the importance of the underlying policy objective of increasing participation in CDR. However, the OAIC would be concerned if restricted levels of accreditation were to create or increase privacy risks that are unable to be appropriately mitigated. The OAIC therefore emphasises the importance of ensuring that any changes to accreditation requirements are carefully tailored to mitigate the risks posed by the specific data handling activities of the relevant entities, and in a way that ensures the privacy and security risks are managed consistently across the scheme and the overall integrity of the CDR system is maintained.

The OAIC also notes that the proposed accreditation changes in the CDR system will likely mean that a greater number of entities start to flow into the system, which will impact on compliance and regulatory activities. Further, many of these may be smaller entities (those with an annual turnover of

[5] The Open Banking 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 or the party seeking to become accredited to consumers, and the CDR system: Treasury, 'Review into Open Banking in Australia', Final Report, December 2017, page 25.

[6] See section 3.4 of the paper.

[7] The statement must be signed by an authorised representative (e.g. CEO or chief legal counsel). Once accredited at the restricted level, entities would be required to submit to the ACCC a self-assessment against the information security controls on an annual basis: clause 2.1 of Schedule 1 to the CDR Rules.

less than $3 million).[8] As many of these entities may not have been covered by the *Privacy Act 1988* (Privacy Act) prior to accreditation, this may result in varied levels of privacy regulatory maturity in the CDR system moving forward.

To ensure this increased participation does not result in greater privacy risks, the OAIC considers that the ACCC and OAIC as co-regulators will need to ensure that their regulatory stance is appropriately robust and strategic, so that any potential risks are identified and managed proactively. In this regard, the OAIC strongly supports the ACCC's intention to work with the OAIC to develop a targeted audit and assessment program for persons accredited at the restricted level.[9]

Given the different information security evidentiary requirements, and the particularities of the affiliate restriction model, the OAIC recommends that the ACCC and OAIC's integrated compliance program focus initially on:

- restricted ADRs' compliance with Privacy Safeguard 12, and
- the affiliate restriction model (for example, in relation to a sponsor's compliance with their obligation to take reasonable steps to ensure their affiliate is complying with their accreditation obligations).[10]

The OAIC notes that entities accredited at both the restricted and unrestricted levels would be subject to the Privacy Act,[11] and would also remain subject to all of the other CDR obligations that apply to accredited entities, including the privacy safeguards. The OAIC strongly supports these arrangements, both of which are important baseline protections that will assist in retaining consumer trust in the system.

Recommendation 1(a)

That the ACCC and OAIC review the existing co-regulatory approach to compliance and enforcement in light of the anticipated increase in CDR participation posed by restricted accreditation, to ensure the approach is appropriately integrated, robust and targeted to identify and mitigate potential risks.

Limited data restriction

Section 3.1 of the paper provides that the limited data model of restricted accreditation would allow an entity to collect certain data sets that have been assessed as 'lower risk' when compared to the

[8] A business is a small business at the time in a financial year if its annual turnover for the previous financial year is $3 million or less: section 6D of the Privacy Act. Most small businesses are not covered by the Privacy Act, but some are in certain circumstances.

[9] As noted on page 18 of the paper.

[10] While this obligation to take reasonable steps attaches to the (unrestricted ADR) sponsor, it is key to ensuring the restricted ADR (affiliate) is complying and would therefore be sensibly explored as part of the ACCC and OAIC's targeted compliance and audit program for restricted ADRs.

[11] All accredited persons are subject to the Privacy Act and APPs for personal information that is not CDR data: s 6E(1D) of the Privacy Act.

complete range of data in scope for an unrestricted ADR. In the banking sector, it is proposed that an entity accredited to this restricted level would be permitted to collect data that has been assessed to be low to medium risk, namely data relating to bank accounts, basic customer data, payees and regular payments.[12]

Assessing sensitivity and risk

The OAIC understands from the draft PIA that the risk level of a given data set was considered from a security perspective (i.e. the risks of the data type being the subject of a cyber security threat).[13] However, we consider that the concepts of data 'sensitivity' and 'risk' are complex and multi-faceted, encompassing more than just security considerations.

In response to consultation question 4, the OAIC would therefore recommend that the sensitivity or risk of particular data be evaluated with reference to a broader range of factors. For example, under the Privacy Act's Notifiable Data Breaches scheme, when assessing whether a breach poses a risk of 'serious harm', risks that a breach could pose for physical and mental wellbeing (as well as damage to reputation) must also be considered in addition to the risk of financial harm.[14]

Recommendation 1(b)

That the ACCC evaluate the sensitivity or relative risk of particular data with reference to a broader range of factors, when determining what data sets should be accessible via the limited data model of restricted accreditation.

Whether ADRs subject to the limited data restriction should be able to collect 'low risk' data across sectors

The OAIC understands from the paper that the model is intended to apply across sectors. The paper also notes that 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)'.[15] The OAIC strongly agrees with this view. As CDR is rolled out across the economy and data sets can be combined, richer and more granular insights may be derived about individual consumers, meaning the overall privacy risks for consumers may increase.

While we would take into account any further evidence that comes to light as a result of the consultation process, considering the above, the OAIC recommends that any limited data model of restricted accreditation be applied on a sector-specific basis only initially. Any cross-sector expansion should be evaluated at a later stage as part of the risk assessment that would be carried out to

[12] Importantly, they would not be able to collect transaction data, due to its potential to reveal more sensitive information about a consumer: see page 12 of the paper.

[13] Maddocks, 'Update 2 to Privacy Impact Assessment' for the CDR regime, stakeholder consultation document, analysis as at 29 September 2020, page 78.

[14] See e.g. 'Consequences of a data breach' in the OAIC's Data Breach Guide. See also pages 12-13 of the OAIC's submission to the Energy Rules Framework consultation for a list of factors which may be relevant when assessing the sensitivity level of a given data set.

[15] Page 12 of the paper.

determine what types of data could be included in this model, as new sectors are brought into the CDR system.[16]

Recommendation 1(c)

That the limited data model of restricted accreditation initially be applied on a sector-specific basis only.

Data enclave restriction

Section 3.2 of the paper outlines the data enclave model, which would allow an entity accredited at this level (the 'principal') to access CDR data collected on their behalf by an unrestricted ADR (the 'enclave provider'). The principal would only be able to access CDR data through a 'data enclave' provided by the (unrestricted) data enclave provider.[17] The OAIC understands from the paper that the data enclave is intended to be a secure area within the enclave provider's data security firewalls. The draft Rules require the principal and enclave provider to have a combined accredited person (CAP) arrangement in place to govern their relationship.

By way of general comment, the OAIC broadly supports the data enclave model as described in the paper. However, in our view it is not clear from the draft Rules what form the data enclave must take, and what responsibilities the principal and enclave provider would have in relation to the enclave under the CAP arrangement.[18] For example, the draft Rules do not make clear that an enclave provider must provide the data enclave for the principal.[19] The OAIC therefore recommends the ACCC clarify these matters in the Rules to provide regulatory certainty, and ensure the Rules are able to support the intended operation of the data enclave model.

Recommendation 1(d)

That the draft Rules be amended to clarify the form the data enclave must take, and what responsibilities the principal and enclave provider would have in the CAP arrangement (for example, in Rules 5.1B and Schedule 2).

Suggested amendments to support greater clarity of obligations

Draft Rule 5.1B(2)(ii) provides that the principal may not 'hold' CDR data otherwise than through an enclave provider. The OAIC understands from section 3.2 of the paper that the policy intention is that

[16] As noted on page 11 of the paper.

[17] Further, they would not be able to download local copies of the CDR data to another environment.

[18] See especially: draft Rules 1.10B and 5.1B; clause 1A.1 of Part 1 of Schedule 2 to the CDR Rules; and Part 2, Schedule 2 to the CDR Rules.

[19] In this regard, the OAIC notes that the definition of 'enclave provider' in draft Rule 5.1B(3) appears circular.

the principal will handle CDR data within the data enclave. However, the term 'hold' does not capture the full range of data handling activities that may be engaged in by a principal (e.g. collecting, using and disclosing). It is further unclear from the draft Rule that any data handling activities must occur 'within' the data enclave. The OAIC therefore recommends that draft Rule 5.1B(2)(ii) be amended to require that the principal may not 'handle' CDR data otherwise than through an enclave provider, and must only handle data within the data enclave.

In response to consultation question 8 about additional requirements for the CAP arrangement, please see the OAIC's comments in 'CAP arrangements' below.

Recommendation 1(e)

That draft Rule 5.1B(2)(ii) be amended to require that a principal may only 'handle' CDR data through an enclave provider, and within a data enclave.

Additional security requirements for enclave providers

In response to consultation question 9, the OAIC considers there should be additional information security requirements for enclave providers. The paper notes that enclave providers would be 'encouraged' to expand the scope of their information security assurance reports to include processes specific to the management of data enclaves.[20] The OAIC considers that enclave providers should instead be required to do so. This would be a useful additional protection given principals, as entities accredited to a restricted level, would not be required to submit assurance reports.[21]

The OAIC further considers that there may need to be additional information security requirements for principals. Specifically, it is unclear from the paper why a principal would not be required to comply with certain provisions in Schedule 2 to the CDR Rules.[22] The OAIC recommends the ACCC further consider these exceptions, having regard to the data handling activities of a principal in the proposed data enclave model.

Recommendation 1(f)

That the draft Rules be amended to require enclave providers to expand the scope of their information security assurance reports, to include processes specific to the management of data enclaves (for example, in clause 2.1 of Schedule 1).

[20] See page 18 of the paper.

[21] Clause 2.1 of Schedule 1 to the CDR Rules.

[22] Clause 1A.1 of Part 1 of Schedule 2 to the CDR Rules provides that principals do not need to comply with clauses 1.7(1), 1.7(3)(a) and 2.2(3) of Schedule 2 to the CDR Rules.

Recommendation 1(g)

That the ACCC further consider what information security provisions in Schedule 2 to the Rules should apply to a principal, having regard to the data handling activities of a principal in the proposed data enclave model.

Affiliate restriction

Section 3.3 of the paper explains that under the affiliate model of restricted accreditation, a person accredited to the unrestricted level (sponsor) would certify[23] that it has a commercial relationship with a third party (the affiliate) and is satisfied that the affiliate meets the accreditation criteria in the Rules.[24]

The OAIC notes the affiliate model departs from the other models of restricted accreditation, in that the entity accredited to the restricted level (the affiliate) has no direct relationship with the ACCC.[25] We understand from page 15 of the paper that the affiliate model is intended to leverage the due diligence that many persons would already undertake in relation to commercial relationships with third parties. The OAIC appreciates this policy rationale, however we would be concerned if the affiliate model was to result in or increase privacy risks. In this regard, see our comments under 'Restricted accreditation' above.

Rule 5.1D(6) requires a sponsor to take reasonable steps to ensure that the affiliate complies with its obligations as an ADR.[26] The OAIC supports this requirement, and considers it to be an important accountability measure that is complemented by the requirement for a sponsor to implement a third party management framework in relation to its affiliates.[27] The OAIC also supports the principles-based approach to formulating the third party management framework in Schedule 2 of the Rules, as this will allow sponsors flexibility to adjust their approach in response to the specifics of their commercial arrangement with an affiliate.

Suggested additional requirements

In addition to the protections outlined above, the OAIC would recommend that the ACCC specify certain minimum steps which must be taken by affiliates in the Rules, in order to provide greater regulatory certainty. For example, in relation to reporting requirements, the Rules could require an affiliate to provide their sponsor with reports prepared under Rule 9.4, in addition to providing the report to the ACCC and OAIC.

---

[23] To the Data Recipient Accreditor – the ACCC.

[24] The sponsor would be required to provide the ACCC with particular documentation for these purposes.

[25] Further, once accredited to the restricted level, the ACCC intends for the sponsor to provide the relevant attestation and self-assessment statements on the affiliate's behalf: see page 18 of the paper.

[26] Rule 5.1D(6) is a civil penalty provision.

[27] The third party management framework requires the sponsor to, amongst other things, undertake annual review and assurance activities and impose reporting requirements on the affiliate: clause 2.2(7) of Part 2, Schedule 2 to the CDR Rules.

In response to consultation question 12 about additional requirements for the CAP arrangement, please see the OAIC's comments in 'CAP arrangements' below.

Recommendation 1(h)

That the draft Rules be amended to specify the minimum steps which must be taken (and the arrangements that must be put in place) by sponsors in relation to their affiliates, for the purposes of Rule 5.1D(6) and clause 2.2(7) of Schedule 2 to the Rules.

Whether information security requirements should vary depending on the relationship between sponsor and affiliate

Consultation question 13 seeks views on whether different information security requirements should apply to an affiliate depending on the relationship between the sponsor and affiliate. The OAIC understands from the draft Rules that each of the information security requirements in Schedule 2 are proposed to apply to an affiliate.[28] We strongly support this, and consider this to be appropriate given that an affiliate is providing goods and services to a consumer in their own right as an ADR.

The OAIC would caution against changing this requirement depending on factors such as the level of data access an affiliate has, and recommends that all the information security requirements in Schedule 2 apply to affiliates regardless of the specific arrangement between the affiliate and their sponsor.

Recommendation 1(i)

That all of the information security requirements in Schedule 2 to the Rules should apply to affiliates, regardless of the specific arrangement in place between an affiliate and their sponsor.

Expanding how ADRs can work together

CAP arrangements

The OAIC understands that the proposed Combined Accreditation Person (CAP) arrangements seek to allow a principal (accredited at the unrestricted level) to partner with a provider (accredited at a restricted level) in order to provide a good or service to a consumer. These changes are intended to support a flexible and dynamic CDR system, giving accredited parties a variety of options for how they can work together and offer services to consumers. CAP arrangements may have a range of uses, but importantly for the purposes of this paper, they are intended to facilitate the operation of the data enclave or affiliated restricted accreditation models.

[28] Clause 1A.1 of Schedule 2 to the CDR Rules.

Under a CAP arrangement, as accredited entities both the provider and the principal will have to independently discharge their obligations under the Rules. However, there are some obligations which would only need to be discharged by one of the ADRs (the provider) as set out in the draft Rules at Rule 1.10B.

Need for further clarity on what CAP arrangements should cover

By way of general comment, the OAIC notes that the draft Rules adopt a 'light touch' approach to defining the CAP arrangement. Rule 1.10B defines the CAP arrangement as 'an arrangement in which the provider will perform functions specified in the provision on behalf of the principal for the purposes of [the] Rules'. While we appreciate the need for flexibility, the OAIC considers there is a risk that regulated entities may not have certainty about the content of the CAP arrangement and the responsibilities of each party – which may lead to increased privacy (and general compliance) risks.[29]

The OAIC understands that the particularities of a CAP arrangement are intended to be determined by other specific provisions in the Rules.[30] However, and in response to consultation questions 8 and 12, the OAIC considers there are some requirements that should be common across all CAP arrangements, and recommends these minimum requirements be set out in draft Rule 1.10B. For example, a requirement for the parties to a CAP arrangement to notify each other of the expiry of a consumer's consent or authorisation (as explained in the section below).

Recommendation 2(a)

That draft Rule 1.10B be amended to prescribe minimum requirements that should form part of all CAP arrangements.

Need to communicate withdrawal of consent

The OAIC also notes that privacy and compliance risks may arise in circumstances where a consumer withdraws consent (or consent otherwise expires), but only one party to a CAP arrangement is aware of that withdrawal/expiry. In such a case the other party might continue to use and disclose the consumer's CDR data without a valid consent. Similar privacy and compliance risks may arise where a consumer withdraws authorisation (or authorisation otherwise expires), but only one party to a CAP arrangement is made aware of that withdrawal/expiry. To mitigate these risks, the OAIC recommends that the ACCC amend the Rules to include an express obligation on parties to a CAP arrangement to notify the other of the withdrawal or expiry of a consumer's consent/authorisation.

Recommendation 2(b)

[29] See also Recommendation 1(d) of this submission, in relation to the need for further clarity in the draft Rules regarding the responsibilities of principals and enclave providers under a CAP arrangement.

[30] For example, draft Rules 5.1B and 5.1D contain references to what the CAP arrangement must and could include in the context of the data enclave and affiliate restricted accreditation models.

That the draft Rules be amended to expressly require a party to a CAP arrangement to notify the other party of the withdrawal or expiry of a consumer's consent/authorisation. This could be done in draft Rule 1.10B, as per Recommendation 2(a).

Whether one or both parties to a CAP arrangement should be required to discharge certain obligations under the Rules

As outlined above, as ADRs both the principal and provider in a CAP arrangement must discharge all their obligations under the Rules, with a few exceptions. Consultation question 14 seeks feedback on the ACCC's view that it is appropriate for the provider,[31] as the entity with the consumer-facing relationship, to be the entity responsible for ensuring the customer-facing aspects of the CDR are delivered (for example, dashboards and other consumer-facing notifications/communications). To give effect to this, draft Rule 1.10B states that only the provider needs to notify the consumer of the matters set out in Rules 7.4/7.9, and only the provider needs to be identified as the ADR to whom the CDR data was disclosed under Rule 7.10(1)(a).

The OAIC supports these arrangements, as they will enhance consumer comprehension and reduce the risk of notification fatigue that may occur if both entities discharged such consumer-facing obligations. However, we note that there are other obligations that in our view should only be discharged by the provider – for example, notifications relating to CDR receipts and consents in draft Rules 4.18–4.20. We would therefore recommend that Rule 1.10B be amended to specify the obligations in Rules 4.18-4.20 only need to be discharged by the provider as well.[32]

Further, draft Rule 1.14 requires an ADR to provide a consumer dashboard to a consumer, where they make a consumer data request on their behalf. We would therefore recommend clarifying that the obligations under Rule 1.14 should be discharged only by the provider in a CAP arrangement. From a user perspective, this will ensure that the consumer only receives one dashboard. It will also provide regulatory certainty for entities when determining their obligations under the CAP arrangement.

In addition to considering amendments to Rules 1.10B and 1.14, as outlined above, we recommend the ACCC considers whether there may be other obligations that should only be discharged by the consumer-facing provider (rather than both the provider and the principal).

Recommendation 2(c)
That draft Rule 1.10B be amended to specify that the obligations in Rules 4.18–4.20 need only be discharged by the provider.

Recommendation 2(d)

[31] Consultation question 14 refers to the 'principal', however given the OAIC's understanding from the draft Rules that the 'provider' is the ADR with the consumer-facing relationship, we have interpreted the question as referring to the 'provider'.

[32] Rules 4.18, 4.18A, 4.18B, 4.18C, 4.19 and 4.20.

That draft Rule 1.14 be amended to specify that the obligations relating to the consumer dashboard need only be discharged by the provider.

Recommendation 2(e)

That the ACCC consider whether there may be other obligations that should be discharged by only one of the ADRs (rather than both).

Transfer of CDR data between ADRs

In addition to proposing new Rules for CAP arrangements, the draft Rules will also allow ADRs to collect and disclose CDR data between themselves (with the consumer's consent).[33] These Rules can be distinguished from the CAP arrangements discussed above (which facilitate the provision of a single good or service), as they are designed to facilitate transfers of CDR data between ADRs to provide distinct services and goods as requested by the consumers. By way of an example, ADR 1 could offer a product comparison service and recommend a product or service of ADR2. If ADR1 has received the valid consents, they may be able to transfer the consumer's CDR data directly to ADR2, so the consumer can receive a more seamless service.

Disclosure consents

The OAIC understands that prior to transfers between ADRs occurring, the consumer must provide a valid consent to collect and use to the first ADR (ADR1), [34]and a valid consent to disclose to the second accredited data recipient (ADR2).[35] Consultation question 15 asks for views on whether consumers should be able to consent to the disclosure of their CDR data (to ADR2) at the same time that they provide a consent to collect and use their CDR data (to ADR1).[36]

In response, the OAIC does not consider that ADRs should be restricted from seeking all consents at the same time. We understand there will be benefits in allowing entities some flexibility as to when they seek particular consents. However, we also recognise there may be some confusion for consumers, in relation to the different types of consents that may be given.

In light of this, the OAIC would recommend that the processes for seeking consents in the Rules continue to be supported by robust consumer experience standards and guidelines, such that they are privacy-enhancing and consumers can easily understand the differences between consent to collect and use, and consent to disclose. Further the OAIC understands this would need to align with the requirement in draft Rule 4.10, that an ADR must ensure their processes for seeking and amending consent is in accordance with consumer experience standards (and to have regard to the consumer

[33] The paper suggests that ADR to ADR transfers will be facilitated through commercial arrangements.

[34] Under draft Rule 4.7A.

[35] Under draft Rule 4.7B

[36] Consultation question 36 also addresses this issue.

experience guidelines). The OAIC will continue to monitor this issue closely as implementation unfolds and re-evaluate at a later stage if necessary.

Recommendation 2(f)
That the processes for seeking consent in the Rules continue to be supported by robust consumer experience standards and guidelines, such that consumers can easily understand the differences between consents to collect and use, and consent to disclose.

Threshold for recommending the good or service of another ADR

The paper outlines on page 25 that transfer of CDR data may occur in two ways: either through the recommendation of the good or service by ADR1 or based on a request from the consumer directly. Further, ADR 1 may only recommend the good or service of ADR2 if a direct marketing consent is in place and ADR1 reasonably believes that the CDR consumer may benefit from the good or service (Rule 7.5(3)(a)(iv)).

Consultation question 15a seeks views on whether the threshold for recommending a good or service in draft Rule 7.5(3)(a)(iv) is appropriate. In response, the OAIC notes that the threshold provided is a broad one. There are likely to be many goods or services that an ADR 'reasonably believes' a CDR consumer may benefit from, notwithstanding that these goods or services may have no or a limited connection to the good or service currently being supplied by the ADR to the consumer. This raises the risk that a consumer may be 'spammed' with unwanted recommendations. Further, in the banking context, there is a risk that products could be recommended for a consumer that are inappropriate for their financial situation. Both of these practices could undermine consumer control and therefore trust in the CDR system. We also note that this represents a shift from the more cautious approach taken in the system to direct marketing to date.

In light of these factors, the OAIC recommends the ACCC amend draft Rule 7.5(3)(a)(iv) to include additional consumer protections, for example:

- requiring that promoted goods or services have a nexus with the existing good or service being provided or requested, and
- a prohibition on promoting or recommending goods or services, if the ADR considers they are likely to be inappropriate for the consumer.[37]

We note that other direct marketing protections would continue to apply, for example the consumer's ability to withdraw their direct marketing consents.[38]

[37] By way of example, this would mean an ADR is prohibited from recommending goods or services which they have determined, due to their own analysis, would not be appropriate for the consumer due to their current financial situation.

[38] The OAIC understands from draft Rules 1.14 and 4.11(1)(c) that ADRs would need to allow consumers the ability to withdraw each 'category' of consent set out in Rule 1.10A(2), including use consents and disclosure consents relating to direct marketing.

Recommendation 2(g)
That draft Rule 7.5(3)(a)(iv) be amended to include additional privacy protections for consumers, such as requiring promoted goods or services to have a nexus with the existing good or service, and a prohibition on promoting or recommending goods or services where the ADR considers they are likely to be inappropriate for the consumer.

Transparency of commercial arrangements

Section 4.2 of the paper provides that the transfer of CDR data between ADRs is likely to be facilitated through commercial arrangements. Consultation question 15b asks for views on whether these commercial arrangements between ADRs should be made more transparent. In response, the OAIC would recommend that information about commercial arrangements, and how CDR data is transferred, be described in the entity's CDR policy as a requirement under Rule 7.2. This enhances transparency for consumers – for example, by making them aware that ADR1 will receive payments if a consumer accepts their recommendation to access a good or service provided by ADR2.

Recommendation 2(h)

That Rule 7.2 be amended to require ADRs to include information about relevant commercial arrangements (those that facilitate ADR to ADR transfers) in their CDR policy.

Disclosures to non-accredited third parties

Disclosure to trusted advisors

The draft Rules allow the disclosure of CDR data by an ADR to a 'trusted advisor' with the consumer's consent. This will allow consumers to share their CDR data with their professional advisor so they can receive professional services. The OAIC is broadly supportive of the draft Rules in relation to disclosures to non-accredited third party 'trusted advisors'. In particular, we welcome the proposal to narrowly prescribe the types of trusted advisors in the draft Rules, as well as the underlying principles that trusted advisors will only be prescribed where the service they offer will provide a direct benefit to the relevant consumer, and where they are subject to existing professional or regulatory oversight.

While the OAIC generally supports these arrangements, we consider that CDR data provided to trusted advisors outside the CDR system should still be subject to a baseline level of protection, being the protections in the Privacy Act. This would ensure that consumers who wish to provide their CDR data to a trusted advisor would still have their data protected, in particular under the data breach notification scheme, and have access to redress mechanisms, monitoring and oversight by the OAIC.

One way to achieve this would be for the draft Rules to prohibit an ADR from disclosing CDR data to trusted advisors that are not subject to the Privacy Act. Where a trusted advisor wishes to be able to receive CDR data, but is not otherwise covered by the Privacy Act, they may consider 'opting in' to the

Privacy Act.[39] Alternatively, a regulation could be made to apply the Privacy Act to trusted advisors that are small business operators, in relation to the handling of CDR data disclosed to them in their trusted advisor capacity.[40]

Further, as the privacy framework that would apply to such disclosures would differ to the CDR framework, consumers should be clearly notified that the CDR privacy protections will not apply at the time of consent. Consideration should be given to how the Rules may provide for further specificity about how this information could be presented to the consumer, so that they are clearly informed of the potential consequences of a disclosure outside the system.

In relation to the draft rule which authorises the ACCC to approve further classes of trusted advisors,[41] the OAIC considers it would be appropriate for this Rule to set out the relevant factors that must be taken into consideration when prescribing additional types of trusted advisors in the future. This could cover the policy factors outlined in the paper (i.e. evidence of consumer benefit, whether the advisor is subject to professional obligations, etc).

In terms of the format and method for disclosure of CDR data to a trusted advisor, it appears that the proposed rules do not intend to limit how the CDR data can be transferred (for example, through a standard). While OAIC appreciates that it may not be practical to limit the format and method, we consider it is important that CDR data be transferred to trusted advisors via an appropriately secure method. The OAIC recommends that the ACCC consider whether the Rules should provide guidance about secure options, for example minimum security requirements, for transfer of CDR data to trusted advisors.

Recommendation 3(a)

That the draft Rules be amended to ensure CDR data may only be provided to a trusted advisor outside the CDR system where that trusted advisor is subject to the Privacy Act.

Recommendation 3(b)

That draft Rule 1.10C(2)(h) be amended to set out the relevant factors that should be taken into consideration when prescribing additional types of trusted advisors in the future.

[39] Section 6EA of the Privacy Act allows small businesses/not-for-profits, who would otherwise not be covered by the Privacy Act, to choose to be treated as an organisation for the Privacy Act and therefore subject to the Australian Privacy Principles.

[40] See ss 6E(1), (2) and (4) of the Privacy Act for more information. This will ensure that trusted advisors who are not otherwise covered by the Privacy Act because they are a small business, will need to comply with the Australian Privacy Principles in relation to their handling of CDR data. A business is a small business if its annual turnover is $3 million or less: section 6D of the Privacy Act. Most small businesses are not covered by the Privacy Act, but some are in certain circumstances.

[41] Draft Rule 1.10(c)(h).

Recommendation 3(c)

That the draft Rules be amended to ensure consumers are clearly informed that the CDR privacy protections will not apply to disclosures to trusted advisors.

Recommendation 3(d)

That the ACCC consider whether the Rules should provide for a secure method of data transfer between ADRs and trusted advisors.

Disclosure of CDR insights

The proposed Rules introduce the concept of a CDR insight,[42] and would permit ADRs to disclose an 'insight' derived from CDR data to any person outside the CDR system, provided they have the consumer's consent. An 'insight' is information derived from a consumer's CDR data. The insight would be provided together with an identifier for the relevant consumer, making it consumer data (however, in the absence of this identifier, this data would otherwise be considered de-identified data).[43]

The proposal aims to facilitate the provision of a broader range of services by an ADR to consumers and third parties, such as assisting entities to undertake inquiries and verification steps (including income and expense verification, verification of payments, or outcomes of responsible lending assessments).[44] It is also intended to make it easier for consumers to provide their CDR information to third parties of their choice.

Interaction with the credit reporting provisions in Part IIIA of the Privacy Act

We note that the CDR insight rule amendments have a similar policy objective and regulate the same (or similar) types of information as the credit reporting provisions under Part IIIA of the Privacy Act. Both these schemes aim to provide entities with sufficient information to assist them to verify banking-related information and assess risk about an individual, in relation to the provision of credit and/or access to goods or services.

Part IIIA seeks to achieve a balance between access to information for entities (that have a legitimate need to verify a consumer's financial position) and ensuring that appropriate consumer protections are in place in relation to the handling of credit information, recognising the significant impact that decisions relating to an individual's creditworthiness can have on their lives.[45] It does this by:

[42] See, for example, Rule 1.10A.

[43] See the definition of CDR insight at draft Rule 1.7.

[44] See page 30 of the paper.

[45] Explanatory Memorandum to the Privacy Amendment (Enhancing Privacy Protection) Bill 2012, pages 2-3.

- prescribing the types of information that can flow between credit providers and credit reporting bodies for use in assessing an individual's creditworthiness (and compiling their credit reports)[46]
- limiting the types of bodies which can access this information,[47] and
- limiting which types of credit information certain credit providers (and others) can access. For example, real estate agents and landlords are currently prohibited from accessing an individual's credit report,[48] and telecommunications and utility providers are prohibited from accessing repayment history information under Part IIIA.[49]

The interaction between the CDR and Part IIIA is addressed in section 56EC(3) of the *Competition and Consumer Act 2010* (Competition and Consumer Act), which states that '[s]ubject to the regulations, this Division does not limit Part IIIA (about credit reporting) of the Privacy Act 1988'.[50] This means that the Rules cannot permit credit providers and credit reporting bodies to collect, use or disclose CDR data for credit reporting purposes (except in ways where they are already permitted to use that same information under Part IIIA).

While s 56EC(3) makes clear that the operation of Part IIIA is not to be directly affected by the CDR, the proposed model for permitting disclosures of CDR insights appears to be inconsistent with the policy objectives of Part IIIA, by creating avenues to share similar types of information beyond what is currently prescribed and limited under that framework. For example, the draft Rules would allow entities prohibited from obtaining credit information or an individual's credit report (such as landlords and real estate agents), to obtain access to a CDR insight (derived from the same types of information used to compile credit reports) for their own commercial, non-credit related purposes. More broadly, it would allow insights from more granular information that cannot be collected, shared or used under Part IIIA (such as insights derived from transaction information)[51] to be shared outside the Part IIIA framework.

On a related note, the proposed rule may also create uncertainty and confusion for entities about the interaction between Part IIIA and the CDR scheme. For example, an ADR deriving insights from CDR data (which may relate to an individual's creditworthiness), may inadvertently breach the credit reporting laws by disclosing this information if they fall into the definition of credit reporting body under Part IIIA (and are unaware of this fact, believing they are operating under the CDR system).

If the ACCC determines that it is appropriate to make these proposed rules, in our view the interaction with Part IIIA should be more fully considered. However, given the matters outlined above, and further given the significant impacts this proposal could have on an individual's right to privacy (see comments on that issue below), it may be more appropriate for this policy change to be considered by Parliament.

---

[46] See, for example, ss 20E-20F and 21G-21H of the Privacy Act.

[47] See, for example, ss 20E-20F and 21G-21H of the Privacy Act.

[48] See this OAIC webpage for further information.

[49] See s 21D(3)(c) of the Privacy Act.

[50] The intention not to limit Part IIIA is also reflected in Privacy Act, as the 'authorised or required by law' exceptions in Part IIIA (in ss 20E, 21G and 22E, respectively), exclude the consumer data rules as an Australian law that would permit the use or disclosure of credit this information.

[51] See s 6N of the Privacy Act. Credit information cannot include detailed transaction information.

Recommendation 3(e)

That the ACCC and relevant agencies consider the impact of the draft CDR insights Rules on the policy objectives of the Part IIIA framework, and determine whether the CDR Rules framework is the appropriate vehicle to introduce such a policy change.

Appropriate limitations to protect vulnerable consumers

As recognised in the PIA on the draft Rules, the types of CDR insights discussed the paper,[52] such as the ability to afford essential goods and services (like rental accommodation, or the ability to repay credit), are likely to be more privacy invasive than the sharing of raw CDR data alone. Sharing a CDR insight would also likely provide similar (or more invasive) insights when compared with an individual's credit report. The concept of a CDR insight is similar to a credit report, as both use personal and financial information to generate a 'score' (or insight) that comments on the level of risk posed by a consumer to a provider.

In the absence of more specific limitations, we would be concerned that entities could require consumers to provide access to CDR insights generated about them as a pre-condition to being offered a product or service. While consumers would need to consent to this, we would be concerned about an individual's capacity to provide free and fully informed consent for such a disclosure, particularly where the good or service is essential.

The OAIC would therefore recommend:

- amending the Rules to prohibit the disclosure of CDR insights for certain prohibited purposes. Prohibited purposes could include assessing an individual's application for an essential good or service (such as housing, healthcare, or utilities), or any employment-related purposes.
- prescribing the types of entities that can (or cannot) collect and use CDR insights derived from CDR data.
- that CDR insights not be disclosed to entities that are not covered by the Privacy Act, and
- that the ACCC consider whether additional consent and notification requirements may be required in relation to the disclosure of CDR insights.

The proposed trusted advisor arrangements may provide a useful model in relation to the above matters.

Recommendation 3(f)

That the draft Rules relating to CDR insights be amended to describe purposes for which insights data cannot be disclosed.

[52] See section 5.2 of the paper.

Recommendation 3(g)

That the draft Rules relating to CDR insights be amended to prescribe the entities that can (or cannot) receive and handle CDR insights.

Recommendation 3(h)

That the draft Rules prohibit the disclosure of CDR insights to entities that are not covered by the Privacy Act.

Recommendation 3(i)

That the ACCC consider whether additional consumer consent and notification requirements are required in relation to CDR insight disclosures.

Additional matters in relation to the disclosure of CDR insights

We also note that draft Rule 7.5(aa)(ii), which permits the ADR to use CDR data for the purposes of 'the creation of an insight', is very broad, and may be inconsistent with existing Rule 4.12 which prohibits the aggregation of CDR data for the purposes of identifying, compiling insights into, or building a profile in relation to a person other than the consumer themselves. For an abundance of clarity, we recommend that7.5(aa)(ii) be amended to provide that the relevant insight must be in relation to the consumer only.

In relation to the definition of CDR insight in Rule 1.7(1)(c), we note the wording may require clarification, as Rule 1.17 sets out a process to be followed, rather than offering a definition of de-identified data. The OAIC recommends amending this sub-paragraph to read 'without that identifier, could be considered to be 'de-identified' as though it had undergone the processes set out in Rule 1.17', or similar.

Finally, as outlined in the paper,[53] the ACCC is seeking views on how an 'insight' derived from CDR data may be provided to a nominated person in a secure and safe way. Given the sensitive nature of a CDR insight, the OAIC would strongly support the ACCC developing Rules that will ensure transfer of a CDR insight occurs via a secure mechanism, and having regard to stakeholder feedback on the best way to do this.

Recommendation 3(j)

[53] See section 5.2 of the paper.

That draft Rule 7.5(aa)(ii) be amended to provide that the relevant insight must be in relation to the consumer only.

Recommendation 3(k)

That draft Rule 1.7(1)(c) be amended so that it is consistent with the wording of the de-identification rule in 1.17.

Recommendation 3(l)

That the draft Rules be amended to require disclosures of CDR insights to occur only via a secure mechanism.

Extending the CDR to non-individual consumers

Under the existing Rules, only individual consumers can authorise data sharing in the CDR system. Section 6 of the paper sets out proposed rules which would allow non-individual consumers (such as business partnerships and limited companies) to participate in the CDR.[54] The proposed Rules will require data holders to allow non-individual consumers to appoint 'nominated persons', who can share and manage CDR data on their behalf. From an information access perspective, the OAIC is supportive of the extension of the CDR to non-individual consumers in this way.

The OAIC also supports the requirement that the nominated person would need to be authenticated using the credentials held on the data holder's system. As the CDR expands to include non-individual consumers, the high degree of security afforded by the existing consumer authentication processes should not be diluted.

Consultation question 21 seeks views on proposed Rules 1.13 (c) and (d), which require data holders to provide a single dashboard to manage authorisations to disclose CDR data. In response, the OAIC supports having a single dashboard which can be used by all nominated representatives. We understand that this will allow for the continuity of authorisations given on behalf of the consumer, regardless of the involvement of a particular nominated representative (who may leave the business, for example).[55]

Consultation question 25 seeks views on whether the internal dispute resolution (IDR) requirements are appropriate for business consumers. The OAIC is of the view that existing IDR arrangements are

[54] This is also consistent with the Open Banking Review recommendation 3.7 that all consumers holding a relevant account should be able to authorise data sharing.

[55] We understand that future nominated representatives would still be required to undergo the initial authentication processes prior to managing authorisations to share CDR data.

appropriate for business consumers in relation to CDR (noting they were designed with both individual and business complaints in mind).

Business partnerships

Section 6.2 of the paper sets out the policy intention to treat business partnerships consistently with the approach the ACCC is proposing for non-individual consumers, as discussed above. The OAIC notes that business partnerships differ from other non-individual consumers (such as corporations), as they are not considered distinct legal entities; rather they may be comprised of one or more individual (or non-individual) consumers.

As partnerships may be comprised of individuals, CDR data sharing may therefore involve the disclosure of personal information relating to the individuals in the partnership (i.e. where individual partners are account holders). Consultation question 24 seeks views on whether additional protections should be introduced where business partners are individuals, as personally identifiable information may be shared in customer data relating to the partnership with other third parties.

By way of general comment, we note that any CDR data relating to the partnership would be subject to the usual Privacy Safeguards and the stringent privacy protections within the CDR scheme. Stakeholders may have more specific views on whether additional privacy protections are required, however we note that the proposed system (which would require appointment of a nominated person to engage in data sharing on behalf of a partnership entity) would appear to provide for appropriate choice, transparency and control in the business context.

Secondary users

In the CDR system, only 'eligible' consumers can make consumer data requests for the transfer of their CDR data. In the banking sector, 'eligible' consumers are currently defined as individuals who are 18 years or over and have an open (and online) account with the data holder.[56]

The paper notes that the proposed Rules would broaden the meaning of eligible consumer by allowing non-account holders to share data relating to the account. These users are known as 'secondary users'. Secondary users are those that have account privileges in relation to an account (i.e. secondary cardholders) and would need to be approved by the account holder through a secondary user instruction in order to share CDR data. The draft Rules propose that for the banking sector, an individual with account privileges must be 18 years of age or older and also have the authority to make transactions on the account.

In response to consultation question 26, the OAIC supports extending the CDR to secondary users in the ways outlined in the paper and above.

Scope of account privileges

Consultation question 27 seeks views on whether any other persons should be considered as individuals with account privileges, and therefore be able to qualify as 'secondary users'.

[56] Clause 2.1(2) of Part 2, Schedule 3 of the CDR Rules.

In response, the OAIC supports the proposed definition of 'account privileges' outlined above and think this is an appropriate initial threshold for authorising secondary users. Any future expansions to these arrangements could be considered in light of evidence gathered from stakeholders on the operation of the system, and any benefits for consumers in doing so.

Secondary users on joint accounts

Consultation question 28 seeks views on how the secondary user rules should operate in a joint account context. The OAIC is broadly supportive of the proposal to allow joint account holders to approve secondary users to share CDR data in relation to joint accounts.

Clause 2.1(2)(c) of Part 2, Schedule 3 of the consultation draft of the Rules provides that to qualify as a secondary user in relation to a joint account, a 'pre-approval disclosure option' (which means the approval of just one of the joint account holders is sufficient to authorise CDR data sharing) must be in place for that joint account. However, we consider that a secondary user should be able to be approved to share CDR data in relation to a joint account, regardless of the disclosure option chosen by the account holders. The OAIC therefore recommends that cl 2.1(2)(c) of Schedule 3, Part 2 be amended to include joint accounts that have both pre-approval and co-approval arrangements in place.

The OAIC further recommends that the processes for providing a secondary user instruction be made consistent with the disclosure option selected on the joint account. For example, if a co-approval disclosure option is in place, the OAIC considers that both joint account holders should be required to give the secondary user instruction. Similarly, if a pre-approval disclosure option is in place, it would be appropriate for one of the joint account holders to give the secondary user instruction on the other's behalf.

Recommendation 4(a)

That cl 2.1(2)(c) of Schedule 3, Part 2 be amended to include joint accounts that have both pre-approval and co-approval arrangements in place.

Recommendation 4(b)

That the processes for providing a secondary user instruction be made consistent with the disclosure option selected on the joint account.

Joint accounts

The existing Rules allow CDR data to be shared from joint accounts. Joint account holders can elect to allow data sharing on their behalf by the other account holder, or require that decisions be made

jointly.[57] As outlined in the paper,[58] the proposed Rules seek to enhance consumer control in the context of joint accounts and reduce 'negative friction' in consumer processes.

By way of overall comment, the OAIC supports the proposed amendments to the Rules for joint accounts. In particular, the OAIC supports the general aim of providing the 'non-requesting' joint account holder ('joint account holder B') with more transparency and control in relation to the sharing of their joint CDR data by the other joint account holder ('joint account holder A').

Vulnerable consumers

The proposed Rules also provide for the expansion of existing protections for vulnerable consumers, by allowing a data holder to take the following steps, if they consider this is necessary to prevent physical or financial harm or abuse:

- enable vulnerable consumers to share CDR data on a joint account, as if the account was held in their name alone,[59] and
- refuse to provide a consumer dashboard to the non-requesting joint account holder.[60]

The OAIC appreciates the need to balance the protection of a vulnerable consumer with another consumer's right to privacy (for example, receiving notifications in relation to how their data is handled). The OAIC notes that the Privacy Act framework recognises that the right to privacy is not absolute, and must give way, for example where the entity 'reasonably believes that the collection, use or disclosure is necessary to lessen or prevent a serious threat to the life, health or safety of any individual, or to public health or safety' (Item 1 of the Table, s 16A(1)).

The OAIC therefore supports these draft Rule amendments. However, we would recommend that the ACCC consider whether the wording outlined above from section 16A could be adopted in these Rules (and potentially at other points in the Rules, where the same formulation is used). The OAIC considers that the Privacy Act formulation may be preferable, as it requires the entity to have a 'reasonable belief' as to the necessity of the action to be taken. Further, as most data holders will be APP entities, this would have the additional benefit of increasing consistency and leveraging a data holder's existing frameworks for compliance with their Privacy Act obligations.

Recommendation 5(a)

That the ACCC consider adopting the wording used in s 16A of the Privacy Act at each point in the Rules where the threshold of 'necessary in order to prevent physical or financial harm or abuse' (or a similar formulation) is used.

[57] Depending on what disclosure option they have selected in the data holder's joint account management service.

[58] See sections 7 and 7.1 of the paper.

[59] Clauses 4.13(3)(b)(ii) and 4.13(4)(b) of Schedule 3 to the CDR Rules.

[60] Clause 4.14(4) of Schedule 3 to the CDR Rules. Both of these would be in addition to the current protection in the Rules, where a data holder may refuse to disclose CDR data that relates to a joint account, or update a consumer dashboard, in circumstances where they consider it necessary in order to prevent physical or financial harm or abuse: clause 4.7 of Schedule 3 of the CDR Rules.

Responses to specific consultation questions

Question 30a

The OAIC supports the proposed approach to require data holders to allow consumers to set their preferences (i.e. a disclosure option) as part of the authorisation process. This will provide useful context for the consumer and make the decision-making process more meaningful.

Question 30b

The OAIC strongly supports the proposed approach of allowing 'joint account holder B' to withdraw an approval at any time. This will ensure both joint account holders, regardless of who provides the authorisation, are able to stop CDR data sharing on a joint account.

Question 30c

The approach to joint accounts held by more than two individuals is proposed to be substantially the same as the proposed approach for joint accounts held by two individuals.[61] The OAIC supports the adoption of a similar approach to all joint accounts, as this will ensure regulatory consistency and enhance the ability of regulated entities to comply with their joint account obligations.

Question 30e

The proposed Rules are silent on whether a data holder must display a consumer's history of 'disclosure option selections' as part of the joint account management service or consumer dashboard.[62] The OAIC recommends that data holders be required to show the history of disclosure option selections on the joint account management service and consumer dashboard. This will lead to greater transparency and will also assist consumers to exercise appropriate control over their data sharing arrangements in the CDR system.

Recommendation 5(b)

That the Rules require data holders to show the history of disclosure option selections on a consumer's joint account management service and consumer dashboard.

Question 31

Under the proposed Rules, joint account holder B will not have oversight of any additional disclosures that occur after the initial disclosure from the data holder to the first ADR.[63] (For example, where a joint account holder consents to the ADR on-disclosing the joint account CDR data to a third party such as another ADR or trusted advisor.) The OAIC notes that if the proposed Rules regarding CAP arrangements, ADR to ADR transfers, trusted advisors and disclosure of insights are made as drafted,

[61] See page 40 of the paper.

[62] See page 41 of the paper.

[63] See pages 40 and 41 of the paper.

a large number of additional third parties may enter the CDR system with the result that CDR data is more likely to be further on-disclosed after the initial disclosure.

In light of this, the OAIC recommends that a data holder be required to notify joint account holder B that their joint account CDR data could be further on-disclosed to other third parties, such as another ADR or trusted advisor, in accordance with joint account holder A's consent. This could occur, for example, when the data holder asks joint account holder B to indicate what disclosure option they prefer under clause 4.7(2) of Schedule 3 to the Rules. This will ensure joint account holder B is given some visibility over the possibility of further disclosures, and has the opportunity to refuse to allow CDR data to be shared from the joint account if they are not comfortable with the possibility of further disclosures.

Recommendation 5(c)

That data holders be required to notify joint account holder B that their CDR data could be further on-disclosed to other third parties, such as another ADR or trusted advisor, in accordance with joint account holder A's consent.

Amending consents

Under the existing Rules, if a consumer wishes to amend their consent with an ADR they must first withdraw this existing consent and then provide a new consent to the ADR. The paper explains that the draft Rules aim to allow a consumer to have more control over various aspects of consent, including by allowing them to add or amend uses, data types, accounts, or data holders, and changing the duration for which their data is held.[64] Any amendments to consent would have to be sought in accordance with the existing consent requirements in Division 4.3.2 of the Rules, unless otherwise provided for in the Rules.[65]

The OAIC generally supports a requirement that amendments to consent be sought in broadly the same manner as original consent. This would mean requiring the consumer to undergo the 'full' consent and authorisation 'flow' to amend any aspect of their consent. At the same time, the OAIC appreciates there may be a need to simplify certain aspects of the consent and authorisation flow, to avoid the risk of information overload and enhance the consumer experience. In doing so, the OAIC notes that it is important to ensure any simplification does not impact on a consumer's ability to give consent which is voluntary, express, informed, and specific.[66] The OAIC generally considers an appropriate balance has been struck in the draft Rules.

[64] See section 7.2 of the paper.

[65] CDR Rule 4.12C(2) provides that when seeking an amendment to consent, an ADR may pre-select certain options that the consumer previously consented to. These are the options regarding data types, time periods, which ADRs (if any) data is to be disclosed to, and data deletion elections. The OAIC understands this provides useful context for a consumer by reminding them of the terms of the existing consent.

[66] See the objects of consent, set out in Rule 4.9 of the existing Rules.

Processes for amending consent and authorisation

In light of the above general comments, and in response to consultation question 34, the OAIC considers that the authorisation requirements in Division 4.4 of the existing Rules are fit-for-purpose, and should all be required for the seeking of amendments to authorisation.

In response to consultation question 33, the OAIC recommends that consumers be given the option to amend each category of consent given to an ADR (i.e. not just collection consents and use consents, but disclosure consents as well, including direct marketing consents and research consents). This will ensure consumers can exercise choice and control in relation to all aspects of the handling of their CDR data.

Recommendation 6(a)

That consumers be given the option to amend each category of consent given to an ADR, consistent with the requirements set out in subdivision 4.3.2A of the draft Rules.

Consistent CX

The paper notes that the draft Rules do not take a prescriptive approach, rather they simply authorise ADRs to allow consumers to make amendments to consent. This means ADRs will be able to determine the best approach for their particular good or service.

The OAIC appreciates the need to provide entities with sufficient flexibility to tailor their processes to suit the particular good/service, and the aspect(s) of consent being amended. However, the OAIC considers it will be important to ensure there is not too much divergence within the CDR system, to ensure a broadly consistent consumer experience across ADRs. The OAIC therefore recommends the ACCC work closely with Data61 to ensure the CX standards and guidelines allow for a consistent consumer experience for amending consent, to the extent practicable.

Recommendation 6(b)

That the ACCC work closely with Data61 to ensure the CX standards and guidelines allow for a consistent consumer experience when amending consents.

Informing consumers of their ability to amend consent

The existing Rules require an ADR to provide a consumer with the information listed in Rule 4.11(3) when seeking consent, including information about their ability to withdraw consent. Further, under existing Rule 4.18, an ADR must issue a CDR receipt to the consumer setting out certain matters, including the information provided when seeking consent under Rule 4.11.

The OAIC notes that Rule 4.11(3) does not require an ADR to provide a consumer with information about their ability to amend consent (and that as a result, the CDR receipt would not contain this information either). To ensure that a consumer is informed about the full range of rights they have in

relation to their consent, the OAIC recommends Rule 4.11(3) be amended to require ADRs to present consumers with information about their ability to amend consent (during the consent flow) and instructions for doing so.

Recommendation 6(c)

That draft Rule 4.11(3) be amended to require ADRs to provide consumers with information about their ability to amend consent and instructions for doing so.

Amending consent via the consumer dashboard

The paper notes that there may be some use cases where an ADR would not be able to offer the consumer the option to amend all aspects of the consent. (For example, because the ADR offers a limited service and would not be able to offer the service without the original set of data.) Nevertheless, the ACCC's preference is for ADRs to be required to offer consumers the ability to amend their consent to the extent possible.[67]

As a general comment, and in response to consultation question 32, the OAIC strongly supports the proposal to allow consumers to amend particular aspects of their consent through the ADR's consumer dashboard. This will increase consumer choice, transparency and control, by giving them a mechanism to instigate the amendment process. The OAIC considers the consumer dashboard to be an appropriate place from which to offer this functionality, as it provides important context (for the consumer's decision) as to whether and how to amend their consent.

The OAIC appreciates that ADRs may not always be able to offer consumers the ability to amend all aspects of the original consent. To enhance transparency for consumers, the OAIC recommends that ADRs be required to explain to consumers which aspects of their consent may not be able to be amended, and the reasons for this. This could be done, for example, via the dashboard amending consent functionality.

Recommendation 6(d)

That ADRs be required to explain to consumers which aspects of their consent may not be able to be amended, and the reasons for this.

Adding accounts

The paper notes that the proposed ADR process to allow consumers to add or remove an account will necessarily require re-direction to the data holder.[68] The paper further notes that this could occur through existing 'oAuth' endpoints, and that the Data Standards Chair may amend existing data standards or create new data standards to enable technical amendments to consent in future.

[67] See pages 42 and 43 of the paper.

[68] See page 43 of the paper.

From a security perspective, the OAIC strongly supports the requirement for ADRs to re-direct consumers to the data holder's (authorisation) processes in order to add an account. However, it is unclear from the paper as to how this will occur, and whether there are existing data standards to support this. Noting that Rule 4.22 requires a data holder to seek a consumer's authorisation in accordance with the data standards, it appears a new or amended data standard will be required to achieve the intended outcome. The OAIC therefore recommends the ACCC work with the Data Standards Chair to ensure there are appropriate data standards to give effect to this proposal.

Recommendation 6(e)

That the ACCC work with the Data Standards Chair to ensure the data standards are amended, or new data standards are made, to ensure that ADRs are required to re-direct consumers to the data holder's (authorisation) processes when adding accounts.

Separate consents

The paper outlines proposed changes to the Rules that will enable separate consents to be obtained, in relation to (1) the collection and (2) the use of CDR data. This is different to the approach taken in the existing Rules, in which a single consent is obtained covering both the collection and use of data. The paper notes that re-framing the Rules in this manner will create more flexibility for ADRs, and enable more granular consent options.[69]

The OAIC notes that the draft Rules also propose to introduce four kinds of 'disclosure consents'.[70] The draft Rules further divide these (and collection and use consents) into 'categories' of consents.[71] Rule 4.11(1)(c) requires an ADR to ask for the consumer's express consent for particular matters in relation to each category of consent. As a result, we note that navigating the consent flow will become more complex for consumers and regulated entities.

Need for effective CX standards and guidance to reduce complexity of the consent flow

By way of general comment, and in response to consultation question 35, the OAIC supports the increased consumer control that the separate consents approach will provide. However, we consider that there is a risk of consumer confusion resulting from the additional complexity of the consent flow, which needs to be appropriately mitigated. The OAIC therefore recommends that clear and effective consumer experience (CX) standards and guidelines are developed to support an ADR's processes for seeking and amending separate consents, and to ensure a simple and straightforward consumer experience. In this regard, the OAIC strongly supports the requirement in Rule 4.10 for an ADR's consent processes to be in accordance with the CX standards, and to have regard to the CX guidelines.

---

[69] See section 7.3 of the paper.

[70] The disclosure consent could be for the disclosure of CDR data for direct marketing, disclosure of CDR data to another ADR or trusted advisor, or the disclosure of insights derived from CDR data to any third party: CDR Rule 1.10A.

[71] CDR Rule 1.10A.

The OAIC also understands from the paper that the approach in the existing Rules of a combined 'use and collection consent' was informed by earlier CX findings.[72] In light of this, the OAIC also recommends that the ACCC work with Data61 to undertake further CX research on the proposed separate consent rules, to test consumer reactions to each aspect of the separate consent approach (i.e. the consent flow, the consumer dashboard, withdrawing consent etc).[73] The OAIC further recommends that the prototypes tested cover all types and categories of consents arising out of the changes proposed in the draft Rules (i.e. not only collection consent and use consent, but also disclosure consent as outlined above).

Regarding consultation question 36, please see the OAIC's response in 'Transfer of CDR data between ADRs'[74] above regarding the related question 15.

Recommendation 7(a)

That clear and effective CX standards and guidelines be developed to support an ADR's processes for seeking and amending separate consent, and to ensure a simple and straightforward consumer experience.

Recommendation 7(b)

That the ACCC work with Data61 to undertake further CX research on the proposed separate consent rules, to test consumer reactions to each aspect of the separate consent approach.

'Point in time' redundancy approach

Under Privacy Safeguard 12, an ADR is required to delete or de-identify redundant CDR data in accordance with the Rules.[75] However, under the existing Rules CDR data may become redundant at different points in the CDR data life cycle, depending on how a consumer withdraws authorisation, and whether or not the consumer is sharing data from one or multiple data holders. Section 7.4 of the paper notes that the current arrangements may create confusion for consumers, and do not support consistent messaging about how deletion and de-identification works in the CDR system.

For these reasons, the ACCC is proposing a 'point in time' redundancy approach in the draft Rules. Such an approach would mean that all CDR data related to the good or service would become

[72] See section 7.3 of the paper.

[73] In relation to withdrawing consents, the OAIC understands from Rules 1.14 and 4.11(1)(c) that ADRs would need to allow consumers to withdraw each 'category' of consent set out in Rule 1.10A(2) separately.

[74] Under the 'Disclosure consents' subheading.

[75] Section 56EO(2) of the Competition and Consumer Act. Redundant CDR data is data that an ADR no longer needs for any purpose permitted under the Rules or the privacy safeguards.

redundant at the same point in time, that is, either immediately upon the consumer withdrawing their collection and use consents, or at the end of the usual 12-month period.

The OAIC understands from page 46 of the paper that this 'point in time' approach is intended to benefit consumers, by ensuring they do not withdraw a use consent without an informed understanding of the consequences. However, consistent with the separate consents outlined above and in the next section, this will also mean that in order to fully withdraw consent for an ADR to handle their CDR data, a consumer would need to take multiple steps (i.e. withdraw both their collection and use consents).

Risk of consumer confusion

The OAIC appreciates the policy objectives behind the 'point in time' approach. However, and in response to consultation questions 37 and 38, the OAIC considers the 'point in time approach' may be confusing for consumers. Consumers may not understand the different outcomes that may flow from withdrawing a particular type of consent and how to fully withdraw consent to handle their CDR data, if that is what they are seeking to do.

By way of general comment, and in addition to the specific recommendations outlined below, the OAIC recommends the ACCC work with Data61 to ensure that clear and effective CX standards and/or guidelines are developed to support an ADR's processes for communicating the 'point in time' approach to consumers. This will help to ensure a straightforward consumer experience and ensure that consumers have choice, transparency and control in relation to the handling of their CDR data.

The OAIC further considers there is a need to explore the impact of the 'point in time' approach on disclosure consents, as outlined below.

Recommendation 8(a)

That the ACCC work with Data61 to ensure that clear and effective CX standards and/or guidelines are developed to support an ADR's processes for communicating the 'point in time' approach to consumers.

Notifying a consumer that they may withdraw their use consent

Where a consumer withdraws their 'collection consent',[76] draft Rule 4.18A requires an ADR to notify the consumer that they may also withdraw their use consent. Withdrawing both the collection and use consents will mean the ADR has to stop all handling of the consumer's CDR data. This notification must occur in writing outside of the consumer dashboard. In response to consultation question 39, the OAIC strongly supports the notification requirement proposed by Rule 4.18A and the proposed methods of delivery.

[76] Technically this is not a collection consent, but an 'authorisation' given by the consumer for their data holder to allow the ADR to collect their CDR data. Where a consumer withdraws the authorisation given to the data holder, their collection consent with the ADR automatically expires.

The OAIC further recommends that the following additional requirements be included in Rule 4.18A:

- A requirement for ADRs to provide the notification in Rule 4.18A as soon as practicable after the collection consent expires. This will ensure that a consumer is able to fully stop an ADR from handling their CDR data, as soon as possible,[77] and
- A requirement for ADRs to include the following statements in the Rule 4.18A notification:
  - a statement that the consumer's collection consent has expired, but their use consent continues, and
  - a statement outlining what the implications of withdrawing the use consent will be for the consumer.

Recommendation 8(b)

That draft Rule 4.18A be expanded to require ADRs to (1) provide the notice as soon as practicable after the collection consent expires; and (2) include additional statements in the Rule 4.18A notice to explain to the consumer that their use consent will continue (and the implications of withdrawing a use consent).

Impact on disclosure consents

Under the proposed draft rules, a consumer may provide an ADR with a 'disclosure consent' in addition to collection and use consents.[78] The OAIC understands that, among other things, this will allow an ADR to disclose CDR data to a third party in order to provide the specific good or service that the consumer has requested.

Where a disclosure consent is needed to provide the relevant good or service requested, the OAIC understands that the consumer would need to withdraw all three types of consents (collection, use and disclosure) in order to fully stop the ADR from handling their CDR data. CDR data would therefore only become 'redundant' and be required to be deleted or de-identified under Privacy Safeguard 12, once all three consents have been withdrawn (or otherwise expired).

In light of the above, the OAIC makes the following recommendations.

Recommendation 8(c)

[77] For example, where a consumer withdraws authorisation from the data holder, with the intent of fully 'cancelling' their good or service with the ADR, but is not aware that withdrawal of authorisation only results in the automatic expiry of the collection consent (meaning the ADR can continue to use any previously collected CDR data).

[78] The disclosure consent could be for the disclosure of CDR data for direct marketing, disclosure of CDR data to another ADR or trusted advisor, or the disclosure of insights derived from CDR data to any third party: CDR Rule 1.10A.

That draft Rule 4.18A be expanded to require the ADR to notify the consumer that they may also withdraw their disclosure consent (and explain the implications of doing so). (In addition to the proposals in Recommendation 8(b).)

Recommendation 8(d)

That the draft Rules clarify that a disclosure consent would automatically expire if both the collection and use consents are withdrawn.

Recommendation 8(e)

That the draft Rules be amended to require ADRs to notify consumers that if they withdraw their disclosure consent, this will not fully stop an ADR from handling their data unless they also withdraw their collection and use consents.

Using CDR data for research

The draft Rules would permit an ADR to use CDR data for general research in accordance with the consumer's consent.[79] The OAIC acknowledges that allowing ADRs to use CDR data for research activities may fulfil many of the policy objectives behind the CDR, including increasing competition, driving innovation, and allowing entities to more easily comply with their regulatory obligations.

However, it also represents a significant shift in the direction of the CDR, from a system that generally limits the use of CDR data to providing goods or services for the consumer's benefit, to one where ADRs can use CDR data for their own commercial purposes. It also raises a number of potential privacy risks for individuals, given that CDR data may be subject to data aggregation and other analysis and used to build rich and granular insights about a consumer for the purposes of the research.

Importance of transparency to ensure consent to research is informed

While consumers have the option to consent to the use of their CDR data for research, the data analytics activities that may be used in such research projects can be difficult to explain and understand, which may mean a consumer's consent to research is not genuinely informed. It will therefore be important that ADRs are transparent with consumers about how their CDR data will be used, and that this is communicated in a way that is easy for them to understand.

[79] See draft Rule 7.5(1)(aa)(i).

Under the draft Rules, if a consumer consents to research the ADR must provide them with a link to the CDR policy which must describe:

- the research to be conducted, and
- any additional benefit that may be offered to the consumer in exchange.[80]

The OAIC is generally supportive of this, however we consider that the broad nature of this information may not be sufficient to ensure that consumers can give voluntary, informed and specific consent.[81]

To ensure consumers are genuinely informed of the consequences of providing consent to research, the OAIC recommends that the ACCC consider whether the Rules should provide greater particularity in terms of ADR transparency about their research, either when seeking consent or in the CDR policy. This could include information about:

- the specific purposes for which the ADR uses such research (for example, to conduct market research on its customers to inform the development of new products)
- the types of CDR data used in research, and
- any potential consequences for the consumer (for example, that their de-identified data from the research may be disclosed and sold).

Recommendation 9(a)

That the ACCC consider how the draft Rules permitting research using CDR data could provide for greater transparency, either when seeking consent or in the CDR policy.

Appropriately limiting the scope of research activities

The OAIC notes that the draft Rules permit general research, which is defined as 'research by the ADR that does not relate to the provision of goods or services to any particular CDR Consumer'.[82] In the OAIC's view, the definition of general research under the draft Rules may be too broad, as it does not place any limits on the purposes that research may be conducted for, to ensure they remain consistent with the policy objectives of the CDR system and retain consumer trust.

To ensure that research activities conducted are appropriated limited in scope, the OAIC recommends that the Rules specifically prescribe the types of research activities permitted. Examples of permitted research activities could include:

[80] See draft Rule 4.11(3)(ca).

[81] In line with the objects for consent, as outlined in Rule 4.9.

[82] See the definition of 'general research' in draft Rule 1.7.

- research by an ADR regarding new services or products
- business development, or
- methodologies to enhance regulatory compliance (see further below) or reduce compliance costs.

This would also assist consumers and ADRs to understand the types of research activities that are expected to be conducted under this Rule.

Recommendation 9(b)

That the draft Rules prescribe permitted purposes for which research may be conducted, to ensure that research practices remain consistent with the overall policy objectives of the CDR and retain consumer trust.

Disclosure of research (and other CDR) information

The paper notes that an ADR would only be able to disclose or sell CDR data if it is de-identified in accordance with the CDR data de-identification process. However, under Privacy Safeguard 6, the OAIC notes that ADRs can also disclose information where required or authorised by law (which does not require consent).[83] Research activity by an ADR may therefore lead to unexpected outcomes for consumers, where the research aims to meet regulatory obligations, and those obligations require or authorise the disclosure of CDR data. For example, if an ADR is conducting research to help it meet its regulatory obligations (such as research regarding compliance methodology for anti-money laundering or responsible lending obligations), and that research reveals that the consumer may have made unlawful transactions on their account, the ADR may be authorised, or even required, to disclose that CDR data.

The OAIC notes that this is an existing risk in the CDR framework that may be amplified by the introduction of the research Rules. The OAIC therefore recommends that the ACCC generally consider how the Rules could be amended to require ADRs to inform consumers about the relevant laws that may permit a use or disclosure of CDR data, which has not been consented to by the consumer. This could occur when seeking consent and/or within the CDR policy.

Recommendation 9(c)

That the ACCC consider whether the draft Rules need to be amended, to provide a requirement for ADRs to outline relevant laws that may permit a use or disclosure of CDR data which has not been consented to by the consumer.

[83] See section 56EI(1)(c) of the Competition and Consumer Act.

Additional benefits offered to consumers to obtain consent

The draft Rules provide that the CDR Policy should outline any 'additional benefits' to be provided to a CDR consumer when consenting to the use of their CDR data for research.[84] The OAIC acknowledges that the ability to offer consumers an additional benefit may encourage them to participate in research (for example, by offering the consumer a discount on additional products or services).

However, the OAIC also notes the importance of ensuring that consent is voluntary, express, informed, and specific. [85] The OAIC therefore recommends that the Rules clarify that providing consent for research activities cannot be made a pre-condition for the performance of the good or service (similar to the protection provided for trusted advisor consents).

Further, the OAIC recommends that the ACCC include additional safeguards, to ensure that ADRs do not unfairly penalise consumers who do not consent to research activities (for example, by effectively making the product or services they are seeking more expensive). One way to do this may be to provide that any additional benefits to be provided to consumers in exchange for a research consent, are not directly related to the product or service being provided.

Recommendation 9(d)

That the draft Rules permitting the use of CDR data for research be amended to clarify that giving consent to research cannot be made a pre-condition of providing the good or service.

Recommendation 9(e)

That the ACCC amend the research-related Rules to provide additional safeguards, to prevent ADRs from unfairly penalising consumers who do not consent to research.

[84] See draft Rule 4.11(3)(ca).

[85] See Rule 4.9.

Attachment A – Recommendations

1. Recommendations related to 'Restricted accreditation'

a. That the ACCC and OAIC review the existing co-regulatory approach to compliance and enforcement in light of the anticipated increase in CDR participation posed by restricted accreditation, to ensure the approach is appropriately integrated, robust and targeted to identify and mitigate potential risks.

b. That the ACCC evaluate the sensitivity or relative risk of particular data with reference to a broader range of factors, when determining what data sets should be accessible via the limited data model of restricted accreditation.

c. That the limited data model of restricted accreditation initially be applied on a sector-specific basis only.

d. That draft Rules be amended to clarify what form the data enclave must take, and what responsibilities the principal and enclave provider would have in the CAP arrangement (for example, in Rules 5.1B and Schedule 2).

e. That draft Rule 5.1B(2)(ii) be amended to require that a principal may only 'handle' CDR data through an enclave provider, and within a data enclave.

f. That the draft Rules be amended to require enclave providers to expand the scope of their information security assurance reports, to include processes specific to the management of data enclaves (for example, in clause 2.1 of Schedule 1).

g. That the ACCC further consider what information security provisions in Schedule 2 to the Rules should apply to a principal, having regard to the data handling activities of a principal in the proposed data enclave model.

h. That the draft Rules be amended to specify the minimum steps which must be taken (and the arrangements that must be put in place) by sponsors in relation to their affiliates, for the purposes of Rule 5.1D(6) and clause 2.2(7) of Schedule 2 to the Rules.

i. That all of the information security requirements in Schedule 2 to the Rules should apply to affiliates, regardless of the specific arrangement in place between an affiliate and their sponsor.

2. Recommendations related to 'Expanding how ADRs can work together'

a. That draft Rule 1.10B be amended to prescribe minimum requirements that should form part of all CAP arrangements.

b. That the draft Rules be amended to expressly require a party to a CAP arrangement to notify the other party of the withdrawal or expiry of a consumer's consent/authorisation. This could be done in draft Rule 1.10B, as per Recommendation 2(a).

c. That draft Rule 1.10B be amended to specify that the obligations in Rules 4.18–4.20 need only be discharged by the provider.

d. That draft Rule 1.14 be amended to specify that the obligations relating to the consumer dashboard need only be discharged by the provider.

e. That the ACCC consider whether there may be other obligations that should be discharged by only one of the ADRs (rather than both).

f. That the processes for seeking consent in the Rules continue to be supported by robust consumer experience standards and guidelines, such that consumers can easily understand the differences between consents to collect and use, and consent to disclose.

g. That draft Rule 7.5(3)(a)(iv) be amended to include additional privacy protections for consumers, such as requiring promoted goods or services to have a nexus with the existing good or service, and a prohibition on promoting or recommending goods or services where the ADR considers they are likely to be inappropriate for the consumer.

h. That Rule 7.2 be amended to require ADRs to include information about relevant commercial arrangements (those that facilitate ADR to ADR transfers) in their CDR policy.

3. Recommendations related to 'Disclosures to non-accredited third parties'

a. That the draft Rules be amended to ensure CDR data may only be provided to a trusted advisor outside the CDR system where that trusted advisor is subject to the Privacy Act.

b. That draft Rule 1.10C(2)(h) be amended to set out the relevant factors that should be taken into consideration when prescribing additional types of trusted advisors in the future.

c. That the draft Rules be amended to ensure consumers are clearly informed that the CDR privacy protections will not apply to disclosures to trusted advisors.

d. That the ACCC consider whether the Rules should provide for a secure method of data transfer between ADRs and trusted advisors.

e. That the ACCC and relevant agencies consider the impact of the draft CDR insights Rules on the policy objectives of the Part IIIA framework, and determine whether the CDR Rules framework is the appropriate vehicle to introduce such a policy change.

f. That the draft Rules relating to CDR insights be amended to describe purposes for which insights data cannot be disclosed.

g. That the draft Rules relating to CDR insights be amended to prescribe the entities that can (or cannot) receive and handle CDR insights.

h. That the draft Rules prohibit the disclosure of CDR insights to entities that are not covered by the Privacy Act.

i. That the ACCC consider whether additional consumer consent and notification requirements are required in relation to CDR insight disclosures.

j. That draft Rule 7.5(aa)(ii) be amended to provide that the relevant insight must be in relation to the consumer only.

k. That draft Rule 1.7(1)(c) be amended so that it is consistent with the wording of the de-identification rule in 1.17.

l. That the draft Rules be amended to require disclosures of CDR insights to occur only via a secure mechanism.

4. Recommendations related to 'Secondary users'

a. That cl 2.1(2)(c) of Schedule 3, Part 2 be amended to include joint accounts that have both pre-approval and co-approval arrangements in place.

b. That the processes for providing a secondary user instruction be made consistent with the disclosure option selected on the joint account.

5. Recommendations related to 'Joint accounts'

a. That the ACCC consider adopting the wording used in s 16A of the Privacy Act at each point in the Rules where the threshold of 'necessary in order to prevent physical or financial harm or abuse' (or a similar formulation) is used.

b. That the Rules require data holders to show the history of disclosure option selections on a consumer's joint account management service and consumer dashboard.

c. That data holders be required to notify joint account holder B that their CDR data could be further on-disclosed to other third parties, such as another ADR or trusted advisor, in accordance with joint account holder A's consent.

6. Recommendations related to 'Amending consents'

a. That consumers be given the option to amend each category of consent given to an ADR, consistent with the requirements set out in subdivision 4.3.2A of the draft Rules.

b. That the ACCC work closely with Data61 to ensure the CX standards and guidelines allow for a consistent consumer experience when amending consents.

c. That draft Rule 4.11(3) be amended to require ADRs to provide consumers with information about their ability to amend consent and instructions for doing so.

d. That ADRs be required to explain to consumers which aspects of their consent may not be able to be amended, and the reasons for this.

e. That the ACCC work with the Data Standards Chair to ensure the data standards are amended, or new data standards are made, to ensure that ADRs are required to re-direct consumers to the data holder's (authorisation) processes when adding accounts.

7. Recommendations related to 'Separate consents'

a. That clear and effective CX standards and guidelines be developed to support an ADR's processes for seeking and amending separate consent, and to ensure a simple and straightforward consumer experience.

b. That the ACCC work with Data61 to undertake further CX research on the proposed separate consent rules, to test consumer reactions to each aspect of the separate consent approach.

8. Recommendations related to 'Point in time redundancy approach'

a. That the ACCC work with Data61 to ensure that clear and effective CX standards and/or guidelines are developed to support an ADR's processes for communicating the 'point in time' approach to consumers.

b. That draft Rule 4.18A be expanded to require ADRs to (1) provide the notice as soon as practicable after the collection consent expires; and (2) include additional statements in the Rule 4.18A notice to explain to the consumer that their use consent will continue (and the implications of withdrawing a use consent).

c. That draft Rule 4.18A be expanded to require the ADR to notify the consumer that they may also withdraw their disclosure consent (and explain the implications of doing so). (In addition to the proposals in Recommendation 8(b).)

d. That the draft Rules clarify that a disclosure consent would automatically expire if both the collection and use consents are withdrawn.

e. That the draft Rules be amended to require ADRs to notify consumers that if they withdraw their disclosure consent, this will not fully stop an ADR from handling their data unless they also withdraw their collection and use consents.

9. Recommendations related to 'Using CDR data for research'

a. That the ACCC consider how the draft Rules permitting research using CDR data could provide for greater transparency, either when seeking consent or in the CDR policy.

b. That the draft Rules prescribe permitted purposes for which research may be conducted, to ensure that research practices remain consistent with the overall policy objectives of the CDR and retain consumer trust.

c. That the ACCC consider whether the draft Rules need to be amended, to provide a requirement for ADRs to outline relevant laws that may permit a use or disclosure of CDR data which has not been consented to by the consumer.

d. That the draft Rules permitting the use of CDR data for research be amended to clarify that giving consent to research cannot be made a pre-condition of providing the good or service.

e. That the ACCC amend the research-related Rules to provide additional safeguards, to prevent ADRs from unfairly penalising consumers who do not consent to research.