OAIC Submission to Treasury’s CDR Rules Amendments (Version 3) Consultation

Submission by the Office of the Australian Information Commissioner

30 July 2021



Angelene Falk
Australian Information Commissioner and Privacy Commissioner

Contents

[Overview 2](#_Toc78562287)

[Recommendations 4](#_Toc78562288)

[New pathways to participation 4](#_Toc78562289)

[CDR insights 5](#_Toc78562290)

[Trusted advisers 5](#_Toc78562291)

[Joint accounts 5](#_Toc78562292)

[About the OAIC and our role in the CDR system 6](#_Toc78562293)

[Comments on issues raised in the exposure draft Rules 7](#_Toc78562294)

[New pathways to participation 7](#_Toc78562295)

[CDR insights 16](#_Toc78562296)

[Trusted advisers 19](#_Toc78562297)

[Joint accounts 20](#_Toc78562298)

[Direct to consumer obligations 24](#_Toc78562299)

## Overview

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the exposure draft Version 3 Consumer Data Right rules amendments (draft Rules) and explanatory materials. We understand this proposed package of amendments to the *Competition and Consumer (Consumer Data Right) Rules 2020* (current Rules) aims to facilitate greater participation in the Consumer Data Right (CDR) system by reducing barriers to participation, as well as providing consumers with more options regarding how to use their CDR data, and who it can be shared with.

The proposed amendments cover a wide range of policy issues, including proposals to allow new participation pathways, disclosure of CDR data to trusted advisers, disclosure of CDR insights to non-accredited entities in certain circumstances, and amending the data sharing model for joint accounts. As outlined in the OAIC’s earlier submission to the Australian Competition and Consumer Commission’s (ACCC’s) consultation on these matters,[[1]](#footnote-1) if implemented these proposals would mark a significant expansion of the CDR system, particularly in relation to the type and number of actors who may participate. Further, they represent a recalibration of existing CDR privacy settings, transforming the existing ‘closed’ CDR system into something more ‘open’.

The functions of the Australian Information Commissioner (Commissioner) generally include examining proposed enactments that may have an adverse effect on the privacy of individuals and minimising such effects.[[2]](#footnote-2) Under Part IVD of the *Competition and Consumer Act 2010* (Cth), the Commissioner must also be consulted before CDR rules are made on the likely effect of making the instrument on the privacy or confidentiality of consumers’ information.[[3]](#footnote-3)

The OAIC makes this submission to provide our current consideration of the impacts of the draft Rules on the privacy of individuals and how any adverse effects may be minimised.

The CDR legislation includes strong privacy protections. In a number of respects the CDR provides protection beyond the current *Privacy Act 1988* (Cth) (currently the subject of a review by the Attorney General’s Department)[[4]](#footnote-4) and has alignment with certain additional protections in international privacy frameworks such as the EU’s General Data Protection Regulation (GDPR).[[5]](#footnote-5) The CDR contains robust accountability measures, for example entities engaging in the CDR system must generally be accredited in order to participate, providing strong assurance for Australians that their data will be protected. CDR is also based on an express consent model that seeks to give consumers increased choice and control over their personal information. These settings ensure that Australians can have trust and confidence in the privacy and security of the CDR system supporting uptake, growth and data driven innovation in the public interest.

In seeking to achieve the current consumer and competition policy objectives of the draft Rules, the OAIC considers the regulatory settings warrant careful calibration to ensure the privacy foundations of the CDR, which support its success, are not diminished. Having strong privacy and security protection and mitigation strategies is necessary not only for protecting consumers’ information, but also for maintaining public confidence in the integrity of the CDR system. In addition, as Australia seeks to be a world-leading digital economy and society,[[6]](#footnote-6) maintaining CDR privacy settings that provide commensurate protection with international data protection frameworks will support future global interoperability.

The OAIC welcomes the focus of the draft Rules and explanatory materials on incorporating privacy protections. However, the OAIC recommends that some proposals should be reconsidered or further refined to ensure the privacy risks can be appropriately mitigated. For example, the CDR insights proposal (which allows accredited data recipients (ADRs) to disclose CDR data outside the CDR system with the consumer’s consent) includes some privacy measures to help protect consumers’ privacy, such as the inclusion of prescribed purposes and other restrictions that limit what CDR data can be disclosed. However those that receive insights may not be subject to the Privacy Act, leaving the handling of that personal information unregulated. The issue of regulatory gap may also arise in relation to trusted advisers.

The OAIC also considers that the accreditation process is an important part of the assurance framework and that any adjustments must retain its overall integrity. This framework ensures entities are ‘fit and proper’ to handle CDR data, and are subject to a comprehensive suite of privacy, information security and reporting obligations. The independent assessment by the ACCC holds participants to account and can be relied upon by consumers to inform their consent. The OAIC therefore recommends a cautious approach be taken in relation to new pathways for participation where entities can handle CDR data without undertaking the accreditation process. If the CDR representative model is introduced, it is important that a consistent level of protection applies to these entities in relation to a consumers’ CDR data (when compared with accredited persons). In particular, it is important that the OAIC, as the co-regulator for the scheme, is able to enforce any breaches of the privacy safeguards or privacy/confidentiality-related Rules by the unaccredited representative against their accredited principal, so that consumers are able to access individual remedies for such breaches. In this regard, the OAIC considers that the proposed amendments leave some ‘gaps’ in accountability, and therefore some further refinements will need to be made to ensure these protections and policy goals are achieved.

The draft Rules also propose a changed approach to data sharing from joint accounts - from the current model which requires both (or all) joint account holders to agree in advance about how data will be shared from these accounts - to an ‘opt-out’ approach to data sharing from joint accounts. This would allow data holders to share a non-requesting joint account holder’s CDR data without their express consent. The OAIC supports the continuation of the current ‘opt-in’ model as affording privacy protection in line with better practice. If the opt-out model is implemented, we would recommend further safeguards be included to assist in mitigating some of the relevant privacy risks to the extent possible.

The OAIC also notes generally that the proposed package of amendments may result in additional complexity for consumers and regulated entities, particularly when navigating whether they are operating within or outside of the CDR regulatory framework for disclosures of CDR data to unaccredited third parties. It is therefore critical that entities and consumers are assisted to clearly understand when the CDR protections apply, as well as how the CDR data must be handled once it has left the CDR system. Guidance (such as CX guidelines) will have a key role to play in reducing potential consumer confusion and improving the ability for regulated entities to comply with their obligations. The OAIC therefore welcomes the draft Rules’ consideration of the CX standards when formulating this package of amendments, to help ensure these matters are made clear to the consumer.[[7]](#footnote-7) The OAIC will also update the CDR Privacy Safeguard Guidelines as required, to assist regulated entities to understand and comply with their CDR privacy obligations.[[8]](#footnote-8)

In addition, as the proposed amendments 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. We are therefore committed to working closely with ACCC as co-regulators to ensure that any new privacy, security or general compliance risks are identified and appropriately mitigated.

The OAIC also understands that Treasury has engaged an external legal provider to conduct a Privacy Impact Assessment (PIA) on the expansion of the CDR system, which includes the proposed amendments in the draft Rules. We strongly support Treasury’s decision to conduct this PIA, and recommend that Treasury has regard to its recommendations as it works towards finalising Version 3 of the Rules.

The OAIC provides further detailed comments and recommendations regarding the draft Rules below, and we are available to discuss our submission with Treasury.

## Recommendations

### New pathways to participation

1. That Treasury address the omissions in the CDR representative framework regarding a CDR representative’s compliance with the privacy safeguards and a principal’s liability for its representative’s actions, to give effect to the intended policy outcome that CDR data handled by a representative is subject to the same requirements and protections that apply to CDR data handled by unrestricted accredited persons. Adopting the solution proposed by the OAIC (under the ‘Privacy Safeguards’ sub-heading) would result in a simpler (as well as more privacy-protective) model.
2. That draft Rule 4.3B be amended to provide that a principal breaches Rule 4.3B if its representative fails to comply with Division 4.3 of the Rules in relation to service data of a CDR consumer as if it were an accredited person, regardless of whether the representative’s actions in relation to the service data are in accordance with the CDR representative arrangement.
3. That Treasury insert a restriction in draft Rule 1.10AA to prohibit a CDR representative from collecting CDR data from a CDR participant, except from its principal in accordance with a CDR representative arrangement.
4. That draft Rule 1.10AA be amended to prohibit CDR representatives from entering into a CDR outsourcing arrangement. In the event that this limitation is not made, the CDR Rules should clearly and expressly attribute liability to the accredited principal in a situation where a representative’s outsourced service provider breaches the CDR regulatory framework.
5. That the draft Rules be amended to make a principal liable for any collection of CDR data by an OSP or its subcontractors (regardless of whether that collection is in accordance with the CDR outsourcing arrangement), and that the written arrangement in Rule 1.10(2)(b) be expanded to impose restrictions on an OSP’s collection of CDR data, and requirements for the collection of that data which are equivalent to the requirements that apply to accredited persons’ collecting of CDR data.
6. That the draft Rules be amended to clarify either that only the affiliate needs to provide the dashboard and notifications in Privacy Safeguard 5 and Subdivision 4.3.5 of the Rules, or that where one party to a sponsorship arrangement provides these notifications and the dashboard, the other need not do so.

### CDR insights

1. That ADRs are prohibited from disclosing CDR insights to entities not covered by the Privacy Act. Further, that Treasury considers whether there are other types of entities to which ADRs must not disclose CDR insights under the draft Rules.
2. As an additional transparency measure, that the draft Rules be amended to require ADRs to provide a copy of the CDR insight to the consumer through the dashboard (or otherwise require ADRs to provide the consumer with visibility of the insight), as soon as practicable.

### Trusted advisers

1. That the draft Rules be amended to ensure CDR data may only be provided to a trusted adviser outside the CDR system where that trusted adviser is subject to the Privacy Act.
2. As an additional transparency measure, that the draft Rules be amended to require ADRs to provide a copy of any CDR data disclosed to a trusted adviser to the consumer through the dashboard (or otherwise require ADRs to provide the consumer with visibility of the data disclosed to the adviser), as soon as practicable.

### Joint accounts

1. That draft Rule 4A.6 be amended such that the notification must be provided at least 7 days prior to joint accounts being in scope (rather than 7 days ‘after’), and so that data holders are required to provide this notification via their ordinary method for contacting each joint account holder (to give effect to the intent expressed in the Explanatory Materials).
2. That the notifications in draft Rule 4A.16 be amended to ensure all joint account holders understand they are able to independently exercise their right to ‘opt-out’ of data sharing. (Specifically, by inserting a requirement for the data holder to inform the joint account holder of the implications of the events outlined in draft Rule 4A.16(1)(a) or 4A.16(1)(b) (as relevant), and that the account holder may change to a non-disclosure option (with instructions for how to do so).)
3. That the Rules require consumer experience data standards to be developed to support consumer understanding of key joint account notifications in draft Rules 4A.6 and 4A.16.
4. That Treasury amend the CDR Rules to allow each joint account holder to request that the ADR delete any joint CDR data that has already been shared, as a matter of priority once this is technically feasible.
5. That draft Rule 4A.13(2) be amended to allow each joint account holder to withdraw their approval in the same manner that the requesting joint account holder may withdraw their authorisation in Rule 4.25.

## 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 system together with the ACCC. The OAIC enforces the privacy safeguards contained in Part IVD of the *Competition and Consumer Act 2010* (Cth) (Competition and Consumer Act) as well as the privacy and confidentiality related rules. In addition, the OAIC has a number of statutory advisory and guidance functions under the CDR framework. For example, the OAIC provides advice to the Minister and CDR agencies on the privacy implications of making rules and designating a potential sector,[[9]](#footnote-9) and makes guidelines on the operation of the privacy safeguards.[[10]](#footnote-10)

The OAIC is also responsible for undertaking strategic regulatory and 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 as regulator of the privacy aspects of the CDR system is to ensure that the system’s robust data protection and privacy framework, and effective accountability mechanisms ensure consumers’ CDR data (personal information) is protected.

## Comments on issues raised in the exposure draft Rules

### New pathways to participation

The draft Rules seek to lower barriers to participation by creating three new pathways by which participants can engage with the CDR regime. The new pathways are:

* the CDR representative model
* allowing unaccredited outsourced service providers to collect CDR data on a participant’s behalf, and
* the sponsored level of accreditation.

The OAIC understands the underlying policy objective of reducing barriers to participation in the CDR. However, the OAIC would be concerned if any new pathways to participation were to create or increase privacy risks that are unable to be appropriately mitigated. As such, the OAIC seeks to ensure that any new pathways to participation are implemented in a way that ensures the privacy and security risks are minimised and managed across the scheme, such that a consistent and appropriate level of protection exists for consumers’ CDR data (regardless of which type of participant is handling that data), and the overall integrity of the privacy protections in the CDR system is maintained.

Accreditation is a key privacy protection that is foundational to the CDR system – it ensures, amongst other things, that entities have been assessed as ‘fit and proper’ to receive and handle CDR data.[[11]](#footnote-11) In addition, once accredited, entities are subject to a comprehensive suite of privacy obligations (notably the 13 privacy safeguards, including information security requirements under Privacy Safeguard 12 and transparency requirements under Privacy Safeguard 1) and must regularly report on their compliance with the minimum information security controls.[[12]](#footnote-12) Accreditation also acts like a trust mark as accredited entities have been independently assessed by the ACCC and is important for establishing and retaining consumer trust in the CDR system.

In light of the above, the OAIC strongly supports the policy intention for each new pathway to maintain trust and confidence in the CDR by ensuring that any use or disclosure of CDR data by sponsored affiliates, CDR representatives or outsourced service providers is subject to the same requirements and protections that apply to unrestricted accredited persons.[[13]](#footnote-13) For the reasons outlined below, the OAIC considers that further amendments need to be made in order for this policy intention to be realised in the case of CDR representatives and unaccredited outsourced service providers. The OAIC makes several recommendations in the sections below that are aimed at achieving the policy intent.

The OAIC also notes that the new pathways to participation in the CDR system will likely mean that a greater number of entities start to enter the system. Further, many of these new participants may be smaller entities (those with an annual turnover of less than $3 million).[[14]](#footnote-14) These entities may not have been covered by the *Privacy Act 1988* (Cth) (Privacy Act) prior to accreditation (in the case of the sponsored level of accreditation), or may not be covered by the Privacy Act at all (in the case of CDR representatives and unaccredited outsourced service providers). This may result in varied levels of privacy regulatory maturity and compliance in the CDR system moving forward, as well as differential privacy protections for CDR consumers. The privacy impacts of these new settings should therefore be monitored closely, and subject to review and potential amendment in the future. The OAIC will also work closely with ACCC as co-regulators to monitor and identify new privacy, security or compliance risks to the extent appropriate through our compliance and enforcement activities, including through the OAIC’s assessments program.

#### Representative model of accreditation

The draft Rules propose to introduce a CDR representative model. This model enables unaccredited persons to use CDR data to provide goods and services to consumers in circumstances where they are in a CDR representative arrangement with an unrestricted accredited person who is liable for their activities. An unaccredited person who is in a CDR representative arrangement would be known as the ‘CDR representative’ of the ‘principal’ accredited person.

As outlined above, the OAIC is of the view that the accreditation process is an important part of the assurance framework. Noting Treasury’s intention to reduce barriers to participation in the CDR, if the CDR representative model is introduced the OAIC seeks to ensure consumers’ CDR data is protected in the same way that it would be if handled by an accredited person. The OAIC considers it imperative that as a co-regulator for the scheme, we are able to enforce breaches of any privacy safeguards or privacy/confidentiality-related Rules by the CDR representative, allowing consumers to access individual remedies for such breaches.

In light of this, the OAIC strongly supports the policy intention for any use or disclosure of CDR data by CDR representatives to be subject to the same requirements and protections that apply to unrestricted accredited persons.[[15]](#footnote-15) However, based on our understanding of the draft Rules, we consider there are some significant omissions which result in this policy intention not being fully achieved. Importantly, the representative is not required to comply with the full set of privacy safeguards that an accredited person is subject to, and it is unclear to what extent enforcement action could be taken by the OAIC and/or ACCC in relation to the principal in the event of a consumer complaint involving Privacy Safeguards 1, 5, 8, 9 or 10 (or equivalent/related Rules). The OAIC therefore considers that the liability framework needs to be strengthened to ensure a consistent level of protection for CDR data.

As a general observation, the OAIC also notes the proposed principal-CDR representative framework is complex (in terms of how the draft Rules interact with each other, and with Part IVD of the Competition and Consumer Act), and may result in confusion for regulated entities. The OAIC considers that our proposed solution for addressing the omissions in the CDR representative framework (as outlined in the following section) has the benefit of resulting in a simpler (as well as more privacy-protective) model.

##### Privacy Safeguards

A CDR representative would be required by contract to comply with Privacy Safeguards 2, 4, 11, 12 and 13 (draft Rule 1.10AA). The draft Rules provide that the principal will be taken to have breached the relevant Rule under Privacy Safeguards 2, 4, 11, 12 or 13 where its CDR representative fails to comply with the corresponding privacy safeguard in the Competition and Consumer Act (see, eg, draft Rules 7.3(2) and 7.3A). In addition, the OAIC understands that a principal would, in pragmatic terms, be liable for a breach of Privacy Safeguards 6 and 7 where the representative uses or discloses data other than in accordance with a permitted use or disclosure (due to draft Rule 7.6(4)).[[16]](#footnote-16) Further, because of draft Rules 4.3A and 4.3B, we note that a CDR representative will have to comply with the same requirements that apply to accredited persons under Privacy Safeguard 3.

While the OAIC supports the inclusion of these protections, there is no clear policy rationale for a CDR representative to comply only with a subset of privacy safeguards and not all the privacy safeguards, and why a principal will be liable for breaches by its representative in relation to particular safeguards only.

Given a representative is not required to comply with Privacy Safeguards 1, 5, 8, 9 or 10 by its written arrangement with the principal (see draft Rule 1.10AA), and no additional Rules are proposed to be made under these safeguards to attribute liability to the principal (see Part 7), consumers would not be able to complain about a representative’s failure to comply with Privacy Safeguards 1, 5, 8, 9 or 10 (or equivalent/related rules). The OAIC would also be unable to take any regulatory or enforcement action in this regard either, as there would not have been a breach of a privacy safeguard or privacy/confidentiality-related Rule (see s 56ET(1)). This means that there will be a significant inconsistency in the privacy protections available to consumers, based solely on whether their data is handled by an accredited person or a CDR representative. This does not appear to meet the policy objective of ensuring the same requirements and protections apply to these types of participants.

For this reason, the OAIC recommends that Treasury addresses the omissions regarding a CDR representative’s compliance and a principal’s liability for its representative’s actions, to give effect to the intended policy outcome. One option to rectify this would be to require the representative to comply with the ‘outstanding’ privacy safeguards (1, 5, 8, 9 and 10) as part of the written arrangement under draft Rule 1.10AA, and either:

* insert Rules under each of the relevant privacy safeguards to provide that the principal will be taken to have breached the relevant privacy safeguard-related Rule where its CDR representative fails to comply with the corresponding privacy safeguard in the Competition and Consumer Act (in a similar manner to the draft Rules that are proposed to be inserted in Part 7),[[17]](#footnote-17) and/or
* introduce a liability mechanism to ensure that principals are directly liable for any actions of a CDR representative that, if done by the principal themselves, would breach a privacy safeguard or privacy/confidentiality related Rule.

The section below outlines why compliance with the omitted privacy safeguards is important.

The OAIC notes that for the purposes of this submission, we have focused our analysis of the CDR representative liability model on the privacy safeguards and related Rules. Given the operational complexity of the CDR representative model, the OAIC considers it is important for Treasury to undertake a detailed review of those privacy/confidentiality-related Rules which have not been made under a privacy safeguard, to ensure there are no other gaps from a compliance or liability perspective. For example, the OAIC notes that further consideration should be given to the obligation to provide a consumer dashboard in Rule 1.14.[[18]](#footnote-18)

###### Rationale for CDR representatives being required to comply with Privacy Safeguards 1, 5, 8, 9 and 10

The OAIC considers that a CDR representative should be required to comply with Privacy Safeguard 1. This is the bedrock principle that ensures the open and transparent handling of CDR data and underpins a CDR representative’s compliance with all other arrangement requirements, by requiring the representative to take reasonable steps to implement practices, procedures and systems that will ensure its compliance with the CDR regulatory framework.[[19]](#footnote-19)

Under the draft Rules, the representative would be required to adopt and comply with the principal’s CDR policy (draft Rule 1.10AA), and the principal would be responsible for dispute resolution as the accredited person (Rule 5.12). While we support these arrangements as a minimum, the OAIC considers that a CDR representative should be required to develop and maintain its own CDR policy, given that their data handling practices may not necessarily align with their principal’s, especially in relation to the purposes for which data is collected and processes for correcting data. We further consider the CDR representative should be responsible for dispute resolution in the first instance, given they will be handling the data and have the consumer-facing relationship (and in the event a consumer wishes to make a complaint, the representative would likely be the entity subject to the consumer’s complaint and have the information relevant to resolve the dispute).[[20]](#footnote-20) Requiring CDR representatives to comply with Privacy Safeguard 1 would achieve these aims, as this safeguard requires entities to have a CDR policy and take reasonable steps to implement processes that enable it to deal with consumer complaints.

The OAIC further considers that a CDR representative should be required to comply with Privacy Safeguards 5 and 10, by notifying consumers of data collected/disclosed in accordance with the arrangement.[[21]](#footnote-21) Currently, the principal would be required to provide these notifications in relation to data collected for its representative,[[22]](#footnote-22) and data disclosed by the representative to an accredited person.[[23]](#footnote-23) We note that this would not appear to align with the policy intention for the representative to have the consumer-facing relationship, as outlined in the note to draft Rule 1.10AA.

As noted above, draft Rule 7.6(4) provides that any use or disclosure of service data by a CDR representative will be taken to have been by its principal. While the OAIC supports the inclusion of this liability mechanism, we note that there are some gaps in how a representative’s use and disclosure of CDR data is regulated. Notably, while a principal would (in practical terms) be liable for a representative’s actions where they would constitute a breach of Privacy Safeguards 6 or 7 (because of the effect of Rule 7.6 in combination with Rule 7.5, which provides that CDR data cannot be used other than for a ‘permitted use or disclosure’, as outlined in footnote 12) they would not be liable for a representative’s breach of Privacy Safeguards 8 or 9.[[24]](#footnote-24) These safeguards are not given operation by the CDR Rules – rather, they operate as additional restrictions on what accredited persons can do with CDR data,[[25]](#footnote-25) and so CDR representatives will need to be under a positive obligation to comply with these to ensure that equivalent protections apply in relation to activities by CDR representatives.

##### Enforcing breaches of the consent Rules in Division 4.3

Privacy Safeguard 3 provides that an accredited person must not seek to collect CDR data unless in response to a ‘valid request’ and in accordance with all relevant CDR Rules (e.g. those contained in Division 4.3).[[26]](#footnote-26) Draft Rule 4.3A sets out what constitutes a ‘valid request’ in the context of a CDR representative arrangement, while draft Rule 4.3B requires a principal to ensure that its representative complies with Division 4.3 when seeking the consumer’s consent.

If a representative collected CDR data in breach of Privacy Safeguard 3 or the related Rules (including Division 4.3), or in the event of a consumer complaint about the representative’s seeking of consent, the OAIC would be able to find the principal in breach of draft Rule 4.3B where the principal did not ensure its representative’s compliance with Division 4.3.

While the OAIC appreciates the liability mechanism in draft Rule 4.3B, we note there is a risk that the OAIC would not be able to take regulatory action where the principal did, for example, take steps to ensure its representative’s compliance in accordance with the requirement in draft Rule 4.3B, but the representative nonetheless conducted itself in a manner that breached Division 4.3. To ensure a consistent level of protection for CDR data, the OAIC recommends that, consistent with the drafting of the deeming provisions proposed to be inserted under other privacy safeguards,[[27]](#footnote-27) draft Rule 4.3B be amended to provide that a principal breaches Rule 4.3B if its representative fails to comply with Division 4.3 of the Rules in relation to service data of a CDR consumer as if it were an accredited person, regardless of whether the representative’s actions in relation to the service data are in accordance with the CDR representative arrangement.

##### Prohibition on collection

The OAIC understands that while it is the CDR representative that would seek the consumer’s consent for collection of CDR data, it is the principal that would collect that data (see the note to draft Rule 1.10AA).

For clarity, the OAIC recommends that Treasury insert a restriction in draft Rule 1.10AA to prohibit a CDR representative from collecting CDR data from a CDR participant, except from its principal in accordance with a CDR representative arrangement.

##### Use of outsourced service providers

Draft Rule 1.10AA(2)(c)(iv)(C) implies that a CDR representative would be allowed to engage an outsourced service provider (‘OSP’). The OAIC does not consider that CDR representatives should be permitted to engage an OSP because it undermines one of the key benefits of the current OSP framework, that attributes liability to the principal for all uses of CDR data by the OSP (in a situation where the principal is usually an unrestricted accredited person) (see Rule 7.6(2)).

Where an OSP engaged by a representative engages in conduct that breaches the CDR regulatory framework, it would not be effective to hold the unaccredited representative to account. This is because the CDR system does not directly impose any obligations or restrictions upon the representative.[[28]](#footnote-28)

In light of this, and to ensure a consistent level of protection for CDR data, the OAIC recommends at this stage that draft Rule 1.10AA be amended to prohibit CDR representatives from entering into a CDR outsourcing arrangement. In the event that this limitation is not made, the OAIC would recommend that the CDR Rules clearly and expressly attribute liability to the accredited principal in a situation where a representative’s OSP breaches the CDR regulatory framework.

|  |  |
| --- | --- |
|  |  |
| **Recommendation 1**That Treasury address the omissions in the CDR representative framework regarding a CDR representative’s compliance with the privacy safeguards and a principal’s liability for its representative’s actions, to give effect to the intended policy outcome that CDR data handled by a representative is subject to the same requirements and protections that apply to CDR data handled by unrestricted accredited persons. Adopting the solution proposed by the OAIC (under the ‘Privacy Safeguards’ sub-heading) would result in a simpler (as well as more privacy-protective) model. |
|  |  |

|  |  |
| --- | --- |
|  |  |
| **Recommendation 2**That draft Rule 4.3B be amended to provide that a principal breaches Rule 4.3B if its representative fails to comply with Division 4.3 of the Rules in relation to service data of a CDR consumer as if it were an accredited person, regardless of whether the representative’s actions in relation to the service data are in accordance with the CDR representative arrangement. |
|  |  |

|  |  |
| --- | --- |
|  |  |
| **Recommendation 3**That Treasury insert a restriction in draft Rule 1.10AA to prohibit a CDR representative from collecting CDR data from a CDR participant, except from its principal in accordance with a CDR representative arrangement. |
|  |  |

|  |  |
| --- | --- |
|  |  |
| **Recommendation 4**That draft Rule 1.10AA be amended to prohibit CDR representatives from entering into a CDR outsourcing arrangement. In the event that this limitation is not made, the CDR Rules should clearly and expressly attribute liability to the accredited principal in a situation where a representative’s OSP breaches the CDR regulatory framework. |
|  |  |

#### Collection by unaccredited outsourced service providers

The draft Rules allow an unaccredited outsourced service provider (OSP) to collect data on behalf of an accredited person who is the principal in a CDR outsourcing arrangement (draft Rule 1.10)(2)). By contrast, the current Rules allow only *accredited* OSPs to collect CDR data. The liability mechanism for OSPs is currently Rule 7.6(2), which provides that any use or disclosure of service data by an OSP under a CDR outsourcing arrangement is taken to have been by the principal (regardless of whether that use or disclosure is in accordance with the arrangement).

While the current Rule 7.6(2) makes a principal liable for any use or disclosure of service data by an OSP, there do not appear to be any current or proposed draft Rules that would make the principal liable for the *collection* of service data by an OSP. It therefore appears that there would be no avenue for the OAIC to take regulatory action against the principal in the event that an unaccredited OSP collected CDR data in breach of Privacy Safeguard 3 or the related Rules, or in the event of a consumer complaint in relation to the unaccredited OSP’s collection of their data.

This differs to the situation for accredited OSPs: currently, should an accredited OSP collect data in a manner that breaches Privacy Safeguard 3 or the related Rules, the OAIC would be able to enforce this breach against the accredited OSP, given they are an accredited person and subject to all the obligations of an accredited person.

Further, while the written arrangement in Rule 1.10(2)(b) places restrictions on an OSP’s use and disclosure of service data, it does not regulate an OSP’s *collection* of that data. This means that an OSP’s collection of CDR data would be unregulated. Again, this differs to the situation for accredited OSPs, who would be bound by the usual restrictions that apply to accredited persons when collecting CDR data (including the data standards).

To address these gaps, and to ensure a consistent level of protection for CDR data, regardless of whether a principal chooses to use an accredited or unaccredited OSP, the OAIC recommends that the Rules be amended to:

* make clear that the principal is liable for any collection of CDR data by an OSP or its subcontractors, regardless of whether that collection is in accordance with the CDR outsourcing arrangement, and
* expand the requirements for the written arrangement in Rule 1.10(2)(b) to:
	+ cover instances where data will be or has been collected by the OSP (e.g. 1.10(2)b)(v) to make clear that the OSP must not outsource collection otherwise than under a further CDR outsourcing arrangement), and
	+ impose the same requirements on an unaccredited OSP’s collection of CDR data as those that apply to accredited persons (including accredited OSPs) (e.g. relevant data standards).

|  |  |
| --- | --- |
|  |  |
| **Recommendation 5**That the draft Rules be amended to make a principal liable for any collection of CDR data by an OSP or its subcontractors (regardless of whether that collection is in accordance with the CDR outsourcing arrangement), and that the written arrangement in Rule 1.10(2)(b) be expanded to impose restrictions on an OSP’s collection of CDR data, and requirements for the collection of that data which are equivalent to the requirements that apply to accredited persons’ collecting of CDR data. |
|  |  |

#### Sponsored level of accreditation

The draft Rules would allow a person to become accredited to the sponsored level and become an ‘affiliate’ of a person at the unrestricted level of accreditation (known as a ‘sponsor’). The accreditation criteria for affiliates would be the same as for unrestricted accreditation except in relation to the evidencing of information security compliance (see Rule 5.5 and page 4 of the Exposure Draft Explanatory Materials). A sponsor would have obligations including to take reasonable steps to ensure the affiliate complies with its CDR obligations (draft clause 2.2 of Schedule 1).

As outlined above, the OAIC is of the view that the accreditation process is an important part of the assurance framework. As such, we strongly support the requirement for an affiliate to be accredited and fulfil the obligations of an accredited person in the CDR regime (including, but not limited to, compliance with the privacy safeguards and consent rules). This will ensure a consistent level of protection for CDR data, regardless of the accreditation model chosen. We also support the deeming provision in draft Rule 7.6(3), which ensures any data collected by a sponsor at the affiliate’s request is taken to have also been collected by the affiliate, as well as the proposed additional restrictions on affiliates, including that an affiliate must not engage an outsourced service provider to collect CDR data on its behalf (draft Rule 5.1B).

We understand that a person at the sponsored level would not be required to provide an independent assurance report against the information security requirements of the CDR (as is required at the unrestricted level). Instead, an affiliate would provide an attestation and self-assessment of its information security capability.[[29]](#footnote-29) Given the importance of the information security requirements to the protection of CDR data and compliance with Privacy Safeguard 12, it is critical that the affiliate model does not result in greater privacy risks (for example, any failures of an affiliate to comply with Privacy Safeguard 12). If this model is implemented, the privacy impacts should be monitored closely, and the relevant rules should be subject to review and potential amendment in the future. The OAIC also intends to monitor this to the extent appropriate with the ACCC as co-regulators through the development of a targeted assessments (audit) program for persons accredited at the sponsor level.

The OAIC further understands that where a sponsor collects CDR data at the request of its affiliate, both the sponsor and affiliate would have obligations to notify the consumer of this collection under Privacy Safeguard 5. This is because the notification requirement in Privacy Safeguard 5 is triggered where data is collected in accordance with Privacy Safeguard 3[[30]](#footnote-30) – the sponsor would have collected in accordance with Privacy Safeguard 3, while the affiliate would have been taken to have also collected that data (as a result of draft Rule 7.6(3)). In such a situation, we note it is also unclear which party would provide and update the consumer dashboard (under Rules 1.14 and 4.19) or provide the notifications in Subdivision 4.3.5 of the Rules.

Given our understanding that the policy intent is for the affiliate to have the direct consumer relationship,[[31]](#footnote-31) the OAIC considers it would be appropriate for the affiliate, rather than the sponsor, to provide these notifications and the dashboard to the relevant consumers. The OAIC therefore recommends that the Rules be amended to clarify either that only the affiliate needs to provide these notifications and the dashboard, or that where one party to a sponsorship arrangement provides these notifications and the dashboard, the other need not do so. This will avoid a situation of notification fatigue (where both parties provide the same notification), as well as a situation where a sponsor is in breach of Privacy Safeguard 5 or another notification requirement (for failing to notify where its affiliate did).

|  |  |
| --- | --- |
|  |  |
| **Recommendation 6**That the draft Rules be amended to clarify either that only the affiliate needs to provide the dashboard and notifications in Privacy Safeguard 5 and Subdivision 4.3.5 of the Rules, or that where one party to a sponsorship arrangement provides these notifications and the dashboard, the other need not do so. |
|  |  |

### CDR insights

The draft Rules introduce the concept of a CDR insight, and permit ADRs to disclose a ‘CDR insight’ outside the CDR system to a non-accredited entity, provided the consumer consents and it is for one of the specific purposes listed.[[32]](#footnote-32) We understand this proposal aims to enable a safer and more efficient way for consumers to share certain insights obtained from their CDR data to receive goods and services, and reduce the need to share detailed records or passwords to facilitate access to their information.[[33]](#footnote-33)

While we acknowledge and support the privacy protections already in place, we consider that further enhancements could be made to ensure there are appropriate limits on the disclosure of CDR insights outside the CDR system, and that consumers are fully informed of the potential consequences.

Limitations to protect consumers

Once an ADR discloses a CDR insight outside the CDR system, the CDR data would no longer be subject to the privacy protections within the CDR system (such as the privacy safeguards).

The OAIC is supportive of the narrow drafting which seeks to limit the disclosure of insights by reference to specified purposes, namely:

* to identify the consumer
* to verify the consumer’s account balance
* to verify the consumer’s income, or
* to verify the consumer’s expense.[[34]](#footnote-34)

We also welcome the proposed amendments which provide that even if an insight disclosure consent is given, the accredited person is not permitted to disclose the CDR insight if it includes or reveals sensitive information about the consumer within the meaning of the Privacy Act.[[35]](#footnote-35)

However, it is important to note that even with these protections, the proposed CDR insights model may continue to raise significant privacy risks, particularly for vulnerable consumers. While the draft Rules limit what CDR data an ADR can disclose by reference to a specific purpose, they do not limit the purpose for which that CDR insight can be used once it is outside the CDR system (as non-accredited entities are not subject to the protections under the CDR framework).

This means that a non-accredited entity may use or disclose a CDR insight in a way which is inconsistent with the prescribed purposes for CDR insight disclosures, or inconsistent with the consumer’s consent. For example, if an ADR discloses a CDR insight to a non-accredited entity to verify the consumer’s account balance in order to assess their ability to pay for a specific good or service, once it is disclosed the recipient may use or disclose the insight for another purpose (or in addition to the original stated purpose, may put it to additional, unexpected purposes). For example, the recipient may use the insight to profile the consumer and target them with advertising on unrelated goods and services, or sell this data to third parties. In addition to being outside the consumer’s reasonable expectations, CDR insights could be used and disclosed for disadvantageous or harmful purposes (for example, by encouraging low-income consumers to buy inappropriate goods or services, with higher cancellation rates or late payment fees), in turn creating reputational risks for the CDR system. While consumers would need to consent to the disclosure of the CDR insight, a consumer’s ability to provide their free and fully informed consent with an understanding of the potential consequences for such a disclosure, particularly vulnerable consumers, will be impacted where the recipient is not bound by any additional regulatory obligations such as the Privacy Act. The OAIC notes that it will not be able to regulate the behaviour of the non-accredited entity and the subsequent use of the insight, under the CDR legislative scheme.

The OAIC therefore recommends that that ADRs be prohibited from disclosing CDR insights to entities that are not covered by the Privacy Act and the Australian Privacy Principles (APPs). This would help to ensure that non-accredited entities are subject to a baseline level of privacy obligations for their use of CDR data (for example, the requirement under APP 1 to be open and transparent in their management of data, and the requirement in APP 6 to only use and disclose data for permitted and lawful purposes). This would help ensure the non-accredited entity uses the CDR insight in the way in which the consumer expects, and ensures that consumers have access to individual redress mechanisms, compliance and oversight by the OAIC, and data breach notification requirements. One possible solution would be for the Rules to require ADRs to take reasonable steps to ensure they only disclose CDR insights to APP entities. Guidance could be given by the OAIC/ACCC on examples of reasonable steps that entities could take for the purposes of such a Rule.

We also suggest Treasury consider whether there are any other types of entities to which an ADR should not disclose insights, where there may be elevated impacts or risks to consumers. For example, whether there should be a prohibition against an ADR disclosing certain CDR insights to a consumer’s employer.

Transparency measures

We support the proposed consumer transparency measures in the draft Rules which aim to ensure the consumer understands what the CDR insight would reveal or describe, and make it clear to the consumer that their CDR data will be leaving the CDR system if disclosed as an insight. Specifically:

* the requirement for an accredited person to give an explanation of the CDR insight to the consumer when seeking the insight disclosure consent that makes it clear what the CDR insight would reveal or describe,[[36]](#footnote-36)
* that CX standards will be made about how insight disclosure consents are obtained, and ensure the consumer understands their data will leave the CDR system,[[37]](#footnote-37)
* the requirement for an ADR to update the consumer’s dashboard as soon as practicable with a description of the CDR insight, to whom it was disclosed and when the CDR data was disclosed,[[38]](#footnote-38) and
* the requirement for an ADR to notify consumers about how they can request further information about the CDR insight that has been disclosed.[[39]](#footnote-39)

While the OAIC is supportive of the above transparency arrangements, we consider that these measures could be strengthened. In particular, we consider that the insight itself should be visible to the consumer through the dashboard as soon as practicable. This would allow a consumer who disagrees with the CDR insight to quickly withdraw their consent, make a complaint about the accuracy of the insight, or request for corrected CDR data to be re-disclosed. As currently drafted, the consumer dashboard only shows ‘a description of the CDR insight and to whom it was disclosed’.[[40]](#footnote-40) While we acknowledge the challenges outlined in the explanatory materials regarding presenting a CDR insight,[[41]](#footnote-41) we consider that CX research could help to inform how to meaningfully provide this information to the consumer.

In addition, we note that the CX standards regarding CDR insights will play a critical role in ensuring the consumer is fully aware of the potential consequences of their decision to share data with a non-accredited entity.

|  |  |
| --- | --- |
|  |  |
| **Recommendation 7**That ADRs are prohibited from disclosing CDR insights to entities not covered by the Privacy Act. Further, that Treasury considers whether there are other types of entities to which ADRs must not disclose CDR insights to under the draft Rules. |
|  |  |

|  |  |
| --- | --- |
|  |  |
| **Recommendation 8**As an additional transparency measure, that the draft Rules be amended to require ADRs to provide a copy of the CDR insight to the consumer through the dashboard (or otherwise require ADRs to provide the consumer with visibility of the insight), as soon as practicable. |
|  |  |

### Trusted advisers

The draft Rules allow the disclosure of CDR data by an ADR to a ‘trusted adviser’ with the consumer’s consent. This proposal allows consumers to share their CDR data with their professional adviser so they can receive professional services. We support a number of privacy-enhancing aspects of the current drafting, for example that trusted advisers are narrowly prescribed in the draft Rules to include specific classes of professionals that are expected to be able to provide significant consumer benefits and are subject to professional or regulatory oversight.[[42]](#footnote-42) We also support the requirement that disclosures to trusted advisers are subject to CX standards being made.[[43]](#footnote-43)

However, similar to the CDR insights proposal, these amendments will allow the disclosure of CDR data outside the CDR system, where trusted advisers with an annual turnover of less than 3 million do not have to comply with the privacy safeguards or privacy/confidentiality-related Rules, and consumers may not have access to individual redress mechanisms for a breach of their privacy. We therefore consider that CDR data provided to trusted advisers outside the CDR system should be subject to a baseline level of protection, being the protections in the Privacy Act.[[44]](#footnote-44)

In addition, some of the OAIC’s recommendations raised above regarding transparency for the disclosure of CDR insights outside the CDR system are also relevant for the disclosure of the CDR data to a trusted adviser outside the system. In particular, it is important to ensure that consumers are able to easily see the CDR data that is being disclosed to their trusted adviser either through the dashboard or another secure mechanism. The CX standards will also have a critical role in ensuring the consumer is fully aware of the potential consequences of their decision to disclose CDR data outside the system.

|  |  |
| --- | --- |
|  |  |
| **Recommendation 9** That the draft Rules be amended to ensure CDR data may only be provided to a trusted adviser outside the CDR system where that trusted adviser is subject to the Privacy Act. |
|  |  |

|  |  |
| --- | --- |
|  |  |
| **Recommendation 10**As an additional transparency measure, that the draft Rules be amended to require ADRs to provide a copy of any CDR data disclosed to a trusted adviser to the consumer through the dashboard (or otherwise require ADRs to provide the consumer with visibility of the data disclosed to the adviser), as soon as practicable. |
|  |  |

### Joint accounts

The draft Rules establish an economy-wide ‘opt-out’ approach to data sharing from joint accounts, which would allow CDR data to be shared with only one joint account holder’s consent by default. By contrast, the current Rules require both/all joint account holders to ‘opt-in’ to data sharing, by setting their data sharing preferences in advance. These arrangements currently apply only to the banking sector.

The OAIC understands that Treasury’s policy intention is to reduce consumer friction that may lead to unfulfilled data sharing requests. The OAIC acknowledges that balance needs to be struck between strong privacy protection and the interests of entities in carrying out their functions or activities.[[45]](#footnote-45) Evidence of the impact of the current joint accounts consent model on the ability of CDR entities to engage with the CDR and provide goods and services to CDR consumers should inform whether the impact on privacy can be objectively assessed as reasonable, necessary and proportionate to achieve a legitimate policy objective.[[46]](#footnote-46) Based on the information available to us and the current operation of the Rules,[[47]](#footnote-47) joint account holders appear to have a number of options currently available to them to facilitate the sharing of their joint account data in a way that does not on their face appear unduly burdensome on CDR entities.

In light of the existing mechanisms available to facilitate sharing of joint account data in the CDR system and without clear evidence to evaluate whether they are deficient, the OAIC therefore continues to prefer the current ‘opt-in’ joint account data sharing model, noting that this model is more privacy-enhancing. The proposed opt-out approach would allow data holders to share a non-requesting joint account holder’s CDR data without their express consent (or prior approval). This is inconsistent with the fundamental principle of express consent for data sharing that is central to the operation of the CDR system. It would also appear contrary to both Australian and international best practice regarding consent, where the trend is towards requiring a positive act by an individual to indicate consent.[[48]](#footnote-48)

In the event that an opt-out model is implemented, the OAIC considers it is imperative that data holders are required to inform consumers as soon as possible of the default CDR data sharing settings and the implications of that arrangement, so they have a reasonable opportunity to opt-out (if that is their preference) before any CDR data is shared in relation to their joint account.

More generally, the OAIC also considers that all joint account holders should have a level of choice and control over the sharing of their joint account CDR data that is consistent with the choice and control all individual account holders otherwise have over the sharing of their data under the CDR system. This is important given the privacy harms that may flow from the sharing of joint account CDR data, which include rich, potentially invasive insights being derived from that data about the non-requesting joint account holder, which could impact on the goods/services available to that party in future, and/or be used or on-disclosed (including sold) in ways that the non-requesting joint account holder would not expect.

The OAIC acknowledges that there are protections for vulnerable consumers in both the existing and proposed Rules (e.g. Rule 4.7, draft Rules 4A.14, 4A.15 and 4A.16). Notwithstanding these, the OAIC considers that the general privacy risks of an opt-out model, in which data may be shared without the other account holders’ consent, are increased for vulnerable consumers. This is a further factor which suggests the current opt-in model is preferable from a privacy perspective.

#### Notification requirements

The OAIC notes the importance of clear, informative and timely notifications from data holders so that all joint account holders understand what is happening with their joint account CDR data and what their rights are at key points in the data sharing flow. On this basis, we generally support the notification requirements proposed to be inserted by Part 4A of the draft Rules.

In particular, the OAIC strongly supports the intention to require data holders to notify joint account holders of the default data sharing setting, and how to change this when a joint account is opened or, for existing accounts, at least 7 days prior to joint accounts being in scope for sharing under the Rules, and through the data holder’s ordinary method for contacting each joint account holder (draft Rule 4A.6, page 22 of the Explanatory Materials). This will help ensure a consumer is informed as soon as possible of the default CDR data sharing settings and its implications, so they have a reasonable opportunity to opt- out before any CDR data is shared in relation to their joint account.

To give effect to the intent expressed in the Explanatory Materials, the OAIC recommends that draft Rule 4A.6 be amended such that the notification must be provided at least 7 days *prior* to joint accounts being in scope(rather than 7 days ‘after’),[[49]](#footnote-49) and so that data holders are required to provide this notification via their ordinary method for contacting each joint account holder.

Further, to ensure all joint account holders understand and are able to exercise their right to ‘opt-out’ of data sharing, the OAIC recommendsthat the approval notifications in draft Rule 4A.16 be amended to also require the data holder to inform the joint account holder of the implications of the events outlined in draft Rule 4A.16(1)(a) or 4A.16(1)(b) (as relevant), and that the account holder may change to a non-disclosure option (with instructions for how to do so).

The above notifications proposed by draft Rules 4A.6 and 4A.16 must be provided in accordance with the data standards. Given the importance of CX standards in supporting consumer understanding, the OAIC recommendsthat the Rules explicitly require such ‘data standards’ to include *CX standards*.

The OAIC also notes that even with these safeguards in place, there will still be a risk that notifications are not received, particularly in the context of vulnerable consumers (for example, in a situation where a partner controls all actions and communications in relation to the joint account). Given these notifications are the key mechanism through which joint account holders will be made aware of the default data sharing settings and their rights, the OAIC would encourage Treasury to consider how it can work with data holders to increase the likelihood of these notifications being received by vulnerable consumers.

#### Right to request deletion

As outlined above, the OAIC considers that each joint account holder should have a level of choice and control over the sharing of their joint account CDR data that is consistent with the choice and control all individual account holders would otherwise have over the sharing of their data under the CDR system.

The OAIC understands that under the current Rules and draft Rules, only the requesting joint account holder can request the ADR to delete their joint account CDR data. Further, should a non-requesting joint account holder remove an approval (under the current Rules) or change from a pre-approval to a non-disclosure option (under the draft Rules) after data has been shared, this would only stop data being shared in the future – it would not prohibit the ADR from using or disclosing the data already shared, nor require the ADR to delete/de-identify the CDR data. This means that, under both the current and draft Rules, the only way for a non-requesting joint account holder to ensure their joint account CDR data is deleted is to ask the requesting joint account holder to exercise their right to deletion (and for that requesting joint account holder to agree to do so).

The OAIC considers that this disparity of deletion rights should be addressed. While we understand that at present it may not be technically possible to give effect to a non-requesting joint account holder’s request to delete their CDR data,[[50]](#footnote-50) the OAIC recommends that Treasury amend the Rules to enable each joint account holder to request that the ADR delete any joint CDR data that has already been shared, as a matter of priority once this is technically feasible. In the context of the proposed ‘opt-out’ model, a right to request deletion for all account holders would provide an additional layer of protection where a consumer does not ‘opt-out’ of joint account data sharing prior to the data being shared (which could occur for a number of reasons, including where a consumer does not realise they can – for example due to notification fatigue – or does not appreciate the privacy implications of sharing joint CDR data), but later wishes they had exercised this right.[[51]](#footnote-51)

#### Withdrawing approvals

Draft Rule 4A.13(2) provides that a joint account holder may withdraw an approval at any time using their consumer dashboard. To achieve consistency with the existing methods by which the requesting joint account holder may withdraw their authorisation (in Rule 4.25), the OAIC recommendsthat draft Rule 4A.13(2) be amended to allow each joint account holder to withdraw their approval by using a simple alternative method of communication made available by the data holder for that purpose.

|  |  |
| --- | --- |
|  |  |
| **Recommendation 11**That draft Rule 4A.6 be amended such that the notification must be provided at least 7 days prior to joint accounts being in scope (rather than 7 days ‘after’), and so that data holders are required to provide this notification via their ordinary method for contacting each joint account holder (to give effect to the intent expressed in the Explanatory Materials). |
|  |  |

|  |  |
| --- | --- |
|  |  |
| **Recommendation 12**That the notifications in draft Rule 4A.16 be amended to ensure all joint account holders understand they are able to independently exercise their right to ‘opt-out’ of data sharing. (Specifically, by inserting a requirement for the data holder to inform the joint account holder of the implications of the events outlined in draft Rule 4A.16(1)(a) or 4A.16(1)(b) (as relevant), and that the account holder may change to a non-disclosure option (with instructions for how to do so).) |
|  |  |

|  |  |
| --- | --- |
|  |  |
| **Recommendation 13**That the Rules require consumer experience data standards to be developed to support consumer understanding of key joint account notifications in draft Rules 4A.6 and 4A.16. |
|  |  |

|  |  |
| --- | --- |
|  |  |
| **Recommendation 14**That Treasury amend the CDR Rules to allow each joint account holder to request that the ADR delete any joint CDR data that has already been shared, as a matter of priority once this is technically feasible. |
|  |  |

|  |  |
| --- | --- |
|  |  |
| **Recommendation 15**That draft Rule 4A.13(2) be amended to allow each joint account holder to withdraw their approval in the same manner that the requesting joint account holder may withdraw their authorisation in Rule 4.25. |
|  |  |

### Direct to consumer obligations

We understand that the draft Rules propose to indefinitely defer direct to consumer obligations in clause 6.6 of Schedule 3 to allow for further consultation. The OAIC supports further consultation and in principle supports the ability for consumers to directly access their own data. We recommend that careful consideration should be given to how direct access could be facilitated in future, and in particular what privacy risk mitigation strategies need to be put in place to protect consumers and retain consumer trust.

1. OAIC’s submission to the ACCC’s draft CDR Rules Expansion Amendments and associated consultation paper, 2 November 2020, available at [www.oaic.gov.au/engage-with-us/submissions](http://www.oaic.gov.au/engage-with-us/submissions). [↑](#footnote-ref-1)
2. See s 28A(2)(a) of the Privacy Act, which outlines the ‘monitoring related functions’ of the Commissioner including in relation to the examination of proposed enactments. [↑](#footnote-ref-2)
3. See ss 56BQ and 56BR of the Competition and Consumer Act. [↑](#footnote-ref-3)
4. See the Attorney-General’s Department’s website for further information. [↑](#footnote-ref-4)
5. For example, the CDR provides individuals with the right to request the deletion of their CDR data, a direct right to bring an action for damages caused by, among other things, a contravention of the CDR’s privacy safeguards, an express consent basis for the collection, use and disclosure of CDR data, and a strong role for accreditation (certification) - all of which have corresponding obligations under the GDPR system. [↑](#footnote-ref-5)
6. See the Australian Government’s Digital Economy Strategy. [↑](#footnote-ref-6)
7. Rules 7.5A requires that disclosures to trusted advisers, or disclosures of CDR insights to non-accredited entities are subject to CX standards. Under 8.11(1) and 8.11(1)(1A), these CX standards must require ADRs to explain to a consumer that their data will leave the CDR system when it is disclosed. [↑](#footnote-ref-7)
8. The OAIC’s CDR Privacy Safeguard Guidelines outline how the Information Commissioner will interpret and apply the privacy safeguards when exercising the functions and powers relating to the privacy safeguards under Part IVD of the *Competition and Consumer Act 2010*. The OAIC’s CDR Privacy Safeguard Guidelines are available at [www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines](http://www.oaic.gov.au/consumer-data-right/cdr-privacy-safeguard-guidelines/). [↑](#footnote-ref-8)
9. The OAIC has a number of formal statutory functions under Part IVD of the *Competition and Consumer Act 2010* (Cth) in relation to the making of rules and designation of a potential sector. For example, being consulted about the making of proposed rules and potential designated sectors (sections 56AD(3) and 56BQ), analysing the privacy impacts in relation to the making of proposed rules and potential sectors to be designated, when consulted (sections 56BR and 56AF), and producing a report about an instrument to designate a sector (section 56AF). [↑](#footnote-ref-9)
10. Under section 56EQ, the Information Commissioner must make guidance for the avoidance of acts or practices that may breach the privacy safeguards. [↑](#footnote-ref-10)
11. CDR Rule 5.12(2)(a). [↑](#footnote-ref-11)
12. See Schedule 1 to the CDR Rules. [↑](#footnote-ref-12)
13. Exposure Draft Explanatory Materials, p. 4. [↑](#footnote-ref-13)
14. 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. [↑](#footnote-ref-14)
15. Exposure Draft Explanatory Materials, p. 4. [↑](#footnote-ref-15)
16. Rule 7.6(1) provides that an ADR must not use or disclose CDR data other than in accordance with a permitted use or disclosure (for example, those permitted uses and disclosures outlined in Rule 7.5). Draft Rule 7.6(4) provides that any use or disclosure of service data by a CDR representative will be taken to have been by its principal, including any use or disclosure that occurs outside the scope of the CDR representative arrangement.

The OAIC understands this to mean that where a CDR representative uses service data other than in accordance with a permitted use or disclosure, the principal would be in breach of Rule 7.6(1) (a civil penalty provision). Based on our reading of this Rule, a breach of Rule 7.6(1) would be a breach of a Rule that relates to the ‘privacy or confidentiality of CDR data’, thereby triggering the OAIC’s regulatory and enforcement powers including the ability to receive and investigate individual complaints (see 56ET(1)). [↑](#footnote-ref-16)
17. See the following draft Rules in relation to the privacy safeguards that a CDR representative is required by contract to comply with (i.e. Privacy Safeguards 2, 4, 11, 12 and 13): draft Rules 7.3(2), 7.3(3), 7.3A, 7.10A, 7.11(2), 7.12(3) and 7.15A. This option would require insertion of similar Rules under Privacy Safeguards 1, 5, 8, 9 and 10. [↑](#footnote-ref-17)
18. The OAIC understands that the principal would be required to provide the dashboard to consumers in the context of a CDR representative arrangement. This is because the obligation to provide a dashboard is enlivened where an accredited person makes a consumer data request on behalf of that consumer (and it is the principal who will be making that consumer data request in response to a valid request received by their representative: see Rule 1.14(1)(a), draft Rules 4.4(1)(a) and 4.3A).

We note that this would not appear to align with the policy intention for the representative to have the consumer-facing relationship, as outlined in the note to draft Rule 1.10AA, and as implied by draft Rule 4.3B(l) (which provides that the notifications in subdivision 4.3.5 of the Rules may be given to a consumer by the representative). [↑](#footnote-ref-18)
19. Section 56ED(2)(a) of the Competition and Consumer Act. [↑](#footnote-ref-19)
20. We note that if the matter is not resolved and a complaint was to be made to the OAIC, the principal would be the respondent (as it is the principal that is intended to be liable for breaches of the CDR regulatory framework by its representative). As such, relevant commercial arrangement between the parties would need to make provision to enable the principal to meet its statutory obligations (for example, by requiring the representative to provide the principal with access to relevant information needed to respond). [↑](#footnote-ref-20)
21. See sections 56EH and 56EM of the Competition and Consumer Act. In relation to disclosure, rhe OAIC understands that a CDR representative would be authorised to disclose a consumer’s CDR data to an accredited person in accordance with CDR Rules 7.5(1)(ca) and/or 7.5(1)(g): see draft Rule 7.5(1)(h). [↑](#footnote-ref-21)
22. This is because the obligation under Privacy Safeguard 5 is enlivened where CDR data is collected in accordance with Privacy Safeguard 3 (and it is the principal, rather than the representative, that collects CDR data): see section 56EH of the Competition and Consumer Act. [↑](#footnote-ref-22)
23. This is because where an accredited data recipient is a CDR principal, a disclosure of service data by a CDR representative is taken to be a disclosure by the CDR principal: see draft Rule 7.9(5). [↑](#footnote-ref-23)
24. This is because Rule 7.6 only prohibits a principal from using or disclosing CDR for purposes other than permitted purposes. (Whereas Privacy Safeguards 8 and 9 operate as additional restrictions on an ADR’s use or disclosure of CDR data.) [↑](#footnote-ref-24)
25. See sections 56EK and 56EL of the Competition and Consumer Act. [↑](#footnote-ref-25)
26. See section 56EF of the Competition and Consumer Act. [↑](#footnote-ref-26)
27. See draft Rules 7.3(2), 7.3(3), 7.3A, 7.10A, 7.11(2), 7.12(3) and 7.15A. [↑](#footnote-ref-27)
28. See, eg, draft Rule 1.10AA. [↑](#footnote-ref-28)
29. Exposure Draft Explanatory Materials, p. 4. [↑](#footnote-ref-29)
30. See section 56EH of the Competition and Consumer Act. [↑](#footnote-ref-30)
31. See the examples of the potential applications of sponsored accreditation on page 7 of the Exposure Draft Explanatory Materials. [↑](#footnote-ref-31)
32. The draft Rules add a new type of disclosure consent under draft Rule 1.10(A)(1), ‘an insight disclosure consent’. If a consumer provides an insight disclosure consent, this permits an ADR to disclose CDR data to any person, provided the disclosure is for one of the specified purposes contained in draft Rule 1.10A(3). [↑](#footnote-ref-32)
33. Exposure Draft Explanatory Materials, p. 16. [↑](#footnote-ref-33)
34. Draft Rule 1.10A limits an ADR’s disclosure of a CDR insight by reference to the four purposes specified under draft Rule 1.10A(3). [↑](#footnote-ref-34)
35. Rule 7.5A(5). [↑](#footnote-ref-35)
36. Draft Rule 4.11(3)(ca)). [↑](#footnote-ref-36)
37. Draft Rule 8.11(1A). [↑](#footnote-ref-37)
38. Draft Rule 1.14(3)(ea) and draft Rule 7.9(4). [↑](#footnote-ref-38)
39. Draft Rule 9.3(2). [↑](#footnote-ref-39)
40. Draft Rule 1.14(3). [↑](#footnote-ref-40)
41. The Exposure Draft Explanatory Materials state that a copy of each insight itself are not required to be included on the ADRs consumer dashboard in light of such detailed information potentially crowding dashboards and making them overly difficult to engage with (p. 18). [↑](#footnote-ref-41)
42. Draft Rule 1.10A provides that a consumer can consent to an ADR disclosing a consumer’s CDR data to a nominated trusted adviser. Draft Rule 1.10C provides that an accredited person can invite a CDR consumer to nominate one or more prescribed trusted advisers: qualified accountants, lawyers, tax practitioners, BAS agents, licensed financial advisers or planners, financial counsellors or residential mortgage brokers. [↑](#footnote-ref-42)
43. Draft Rule 8.11(1). [↑](#footnote-ref-43)
44. Prescribed trusted advisers, such as those in the legal, accounting and management services and the finance industries are included in the top 5 industry sectors reporting data breaches to the OAIC as reported on page 6 of the [Notifiable Data Breaches Report](https://www.oaic.gov.au/assets/privacy/notifiable-data-breaches-scheme/statistics/2020-2/Notifiable-Data-Breaches-Report-July-Dec-2020.pdf) between July to December 2020. While some trusted advisers with an annual turnover exceeding $3 million would already be covered by the Privacy Act, the privacy risks attach to the sensitivity of the information held by such advisers, rather than turnover amount. [↑](#footnote-ref-44)
45. In providing policy advice on privacy matters, the OAIC generally notes the objects of the *Privacy Act 1988* (set out in s 2A of that Act), which include the need to ‘recognise that the protection of the privacy of individuals is balanced with the interests of entities in carrying out their functions or activities’. [↑](#footnote-ref-45)
46. See the Attorney-General’s Department’s [template](https://www.ag.gov.au/rights-and-protections/human-rights-and-anti-discrimination/human-rights-scrutiny/statements-compatibility-templates#:~:text=A%20Statement%20of%20Compatibility%20is,Civil%20and%20Political%20Rights%20(ICCPR)) for a Statement of Compatibility for a Bill or Legislative Instrument that raises human rights issues. Page 2 of this template suggests that, when assessing the likely impact on the rights engaged, it should be explained why the limitation on the right is ‘reasonable, necessary and sufficiently precise to ensure that it addresses only those matters that it is intended to capture as well as any relevant safeguards’. Relevant considerations include ‘whether there are less restrictive alternatives for achieving the objective and whether they have been tried and whether sufficient regard been paid to the rights and interests of those affected’. [↑](#footnote-ref-46)
47. The Rules currently provide joint account holders with two options – ‘pre-approval’ and (where offered by the data holder) ‘co-approval’. Both joint account holders need to select an option in order for data to be shared from that account. Under the pre-approval model, one joint account holder can elect to authorise the other account holder(s) to consent to sharing their data on their behalf. Under the ‘co-approval’ model, all joint account holders must individually provide consent to data sharing. Where no option is selected, or where joint account holders select different options, data cannot be shared from that account. [↑](#footnote-ref-47)
48. For example, under Article 20 of the General Data Protection Regulation, individuals have a right to data portability, but only where consent has been given (and processing is by automated means). Similarly, [Singapore](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.pdpc.gov.sg%2F-%2Fmedia%2FFiles%2FPDPC%2FPDF-Files%2FLegislation-and-Guidelines%2FPDPC-Public-Consultation-Paper-on-Data-Portability-and-Data-Innovation-Provisions-(220519).pdf&data=04%7C01%7Cathena.jayaratnam%40oaic.gov.au%7C8154f757d2254301f57e08d94b39b7d7%7Cea4cdebd454f4218919b7adc32bf1549%7C0%7C0%7C637623533533302201%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=9SscM%2BNwuypgZeqsVZ9T%2FqmcBTpgq6ws4FNF6c8nawE%3D&reserved=0) and [New Zealand](https://aus01.safelinks.protection.outlook.com/?url=https%3A%2F%2Fwww.mbie.govt.nz%2Fbusiness-and-employment%2Fbusiness%2Fcompetition-regulation-and-policy%2Fconsumer-data-right%2F&data=04%7C01%7Cathena.jayaratnam%40oaic.gov.au%7Cc05ccc25a1154311153f08d94b401a7a%7Cea4cdebd454f4218919b7adc32bf1549%7C0%7C0%7C637623560960413359%7CUnknown%7CTWFpbGZsb3d8eyJWIjoiMC4wLjAwMDAiLCJQIjoiV2luMzIiLCJBTiI6Ik1haWwiLCJXVCI6Mn0%3D%7C1000&sdata=ljOJDUcsZNnbbrU%2FBOVOfqrXfDDiw96p%2F7kytDszGMY%3D&reserved=0) have placed emphasis on the importance of consumer choice and control in the development of their respective data portability rights. In the Australian context, a number of reviews including the ACCC’s *Digital Platforms Inquiry Final Report*, have recommended that consent requirements be strengthened, including the potential to require consent for all handling of personal information and the need to ensure consent is valid, i.e. freely given, specific, unambiguous and informed, and in particular is not the result of pre-selected default settings or ‘bundled’ consent (see e.g. Recommendation 16c). [↑](#footnote-ref-48)
49. See draft Rule 4A.6(2)(b). [↑](#footnote-ref-49)
50. This is due to technical difficulties in enabling a data holder to provide this information to an ADR, outside of the context of a data holder responding to an ADR’s request for data collection. [↑](#footnote-ref-50)
51. See also [Chapter B (Key concepts)](https://www.oaic.gov.au/privacy/australian-privacy-principles-guidelines/chapter-b-key-concepts/) of the OAIC’s APP Guidelines, which provides that use of an opt-out mechanism to infer an individual’s consent will only be appropriate in limited circumstances, as the individual’s intention in failing to opt-out may be ambiguous. The extent to which an individual who opts out at a later time will, as far as practicable, be placed in the position as if they had opted out earlier, is a factor to consider when determining the appropriateness of an opt-out mechanism: paragraph B.40. [↑](#footnote-ref-51)