Australian Government

Office of the Australian Information Commissioner

Submission to Treasury's Consumer Data Right Consent Review and Operational Enhancements Rules Consultation 2024

Submission by the Office of the Australian Information Commissioner

Elizabeth Tydd

Australian Information Commissioner

11 September 2024

OAIC

Introduction

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on Treasury's exposure draft of the Competition and Consumer (Consumer Data Right) Amendment (2024 Measures No. 1) Rules 2024 (draft rules). The draft rules propose specific changes to the *Competition and Consumer (Consumer Data Right) Rules 2020* (CDR rules).

Under Part IVD of the *Competition and Consumer Act 2010* (CC Act), the Secretary of the Treasury must consult the Information Commissioner about the making of draft rules and the Information Commissioner is required to analyse the likely effect of making rules on the privacy or confidentiality of consumers' information.[1]

The OAIC has analysed the measures outlined in the draft rules and considered the accompanying explanatory materials and privacy impact assessment published as part of public consultation. The OAIC is broadly supportive of the majority of measures in the draft rules. Many of the measures are privacy enhancing and will increase choice, transparency and consistency for CDR consumers.

The OAIC's submission primarily focuses on the measures to permit consent bundling, enable pre-selection, and expand the circumstances in which an accredited authorised deposit-taking institution (ADI) can hold CDR data as a data holder, which require careful consideration. The OAIC makes a number of observations and recommendations on these measures, for Treasury's consideration.

Part 1: Key privacy impacts of the proposed changes to consent

1.1 Unlike the regime for personal information handling under the *Privacy Act 1988* (Privacy Act), the CDR regime is premised on consumer consent.

1.2 Consent enables CDR consumers to be the decision makers in the CDR system, placing them in control and ensuring that they can direct where their data goes in order to obtain the most value from it. This is achieved by requiring the consumer's consent for the collection, use and disclosure of their CDR data. Consent must be voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn.[2]

1.3 In addition to consent, the data minimisation principle (as defined at CDR rule 1.8) serves as a further layer of protection for CDR consumers. Data minimisation places accountability on entities to limit the scope and amount of CDR data they may handle in order to provide the goods or services requested by the consumer.

1.4 These protections, when combined with the defined categories of consent (set out in CDR rule 1.10A) and the list of permitted data flows (listed at CDR rule 7.5), reflect some of the key guardrails for how entities may handle consumer data within the CDR ecosystem.

1.5 Treasury has indicated that the amendments to consent aim '*to support uptake of the CDR by facilitating a better consumer experience'*. Noting this policy rationale, the OAIC has identified ways in which some of the proposals can be strengthened to ensure choice and control remain a fundamental feature of the consumer experience, while avoiding consumer fatigue.

[1] Sections 56BQ and 56BR of the CC Act.

[2] CDR rules 4.9 and 4.20C.

1.6 In making these recommendations, the OAIC acknowledges that the CDR regime is a privacy-preserving regime, that consent fatigue may inhibit consumer uptake of the CDR system, and that there is an important balance to be struck between eliciting specific and informed consent, on the one hand, and ensuring the burden doesn't fall on consumers to navigate lengthy consent processes.

1.7 For this reason, the OAIC agrees that consent bundling for collection and use may improve user experience. However, consistent with our submission to the Consent Review Design Paper (October 2023), the OAIC has concerns that some aspects of the CDR regime (particularly participation of non-accredited entities) still leave privacy risks for consumers that need to be mitigated. Some important mitigations include limitations on bundling and pre-selection as outlined below.

1.8 Other changes to consent proposed as part of the draft rules, such as those related to direct marketing and deletion by default, have the potential to improve consumer privacy outcomes in the CDR, or are privacy neutral, and are therefore not discussed in this submission.

Changes to permit bundling

1.9 Proposed changes to permit bundling would enable a consumer to agree to multiple consents to collect, use and disclose CDR data in a single action. Where consents are bundled, the consumer would no longer be able to engage with and choose which particular aspects of the data flow they consent to. A data recipient may therefore issue a bundled request for a consumer's consent to collect, use and disclose their CDR data for potentially multiple purposes, leaving the consumer unable to agree to one aspect without agreeing to another aspect. This would reduce the consumer's control over their CDR data.

1.10 As a mitigation, Treasury has proposed applying the data minimisation principle to bundling to ensure only reasonably needed CDR data, uses and disclosures are captured through a bundled request. This limitation appears to relate to entities minimising the choices within a bundle (datasets, use, duration, and disclosure recipient) but may not cover the scope and size of the bundle itself.

Scope of bundling

1.11 The draft rules would permit consents to be combined but do not narrow or specify a limit to the scope of collection, use and disclosure consents that can be bundled. For example, as currently drafted, the rules may allow an entity to combine consents by asking a consumer to consent to their data being collected, used and disclosed for various different services or purposes, which the consumer has requested. This may include complementary or enhanced services. Large bundles will have a significant impact on consumer comprehension at the time of consent, potentially undermining the voluntary nature of the consent.

1.12 Due to the higher risks associated with disclosure of CDR data (including to unaccredited CDR participants that may not be covered by the Privacy Act), the OAIC considers it critical for consumers to be given the opportunity to pause and to actively engage with a disclosure consent separately before deciding whether to provide that consent. Bundling of disclosure consents is not supported by the Data Standards Body (DSB)'s CX research which, as mentioned in the Design Paper prepared by Treasury and DSB in 2023, did not consider the impact of bundling disclosure consents. The Design Paper also stated there is *'merit in ensuring these*

consents are distinct from any collection and use consents provided by the consumer'. In the absence of supporting evidence, bundling of disclosure consents may be inconsistent with Treasury's policy aim to improve the consumer experience through these amendments to the consent process.

Recommendation 1: The OAIC recommends that changes to allow bundling of disclosure consents should not proceed. Where bundling occurs, the OAIC recommends that there is an overarching restriction on entities bundling consents across multiple or broad purposes. This would ensure consent remains specific as to purpose and mitigate against the risk that an entity can later change its boundaries and practices in a manner that means CDR data collected for one purpose is later used for a different purpose not expected by the consumer. Importantly, such a restriction would preserve the intention of existing processes for amending consent or separately seeking a new consent.

Recommendation 2: The OAIC recommends that Treasury makes explicit that the intent is for bundling to refer to the singular term 'good or service' rather than the plural term 'goods or services'. This would ensure consistency between the explanatory materials and draft rules. Treasury should also ensure that a request that combines multiple requests for consent:

- Provides a consumer with adequate information about the nature of each proposed collection, use and/or disclosure to inform their consent
- tells a consumer the consequences, if any, of not consenting to one or more of the proposed collections, uses and/or disclosures of their CDR data
- provides an ability to opt out of one or more proposed collections, uses and/or disclosures of their CDR data.

Recommendation 3: The OAIC recommends that Treasury should consider introducing appropriate organisational accountability safeguards to support the requirements outlined in recommendations 1-2 above.

Changes to permit pre-selection

1.13 Proposed amendments to permit pre-selection would enable an accredited person or CDR representative, when seeking a CDR consumer's consent, to pre-select for the consumer: the types of data a collection or disclosure consent applies to, who the data may be disclosed to, the specific uses for the collected data, and the period of the consent (duration).

1.14 To replace the consumer engagement that would have previously occurred through active selection, Treasury proposes to require entities to provide an explanation to inform the consumer why the pre-selected options are reasonably needed.

1.15 Due to the risks of consumer disengagement, the OAIC does not support pre-selection, especially pre-selection of disclosure recipients and duration. It is especially critical for consumers to be given the opportunity to pause and to actively engage with selecting these options before deciding whether to provide consent, without undue influence.

Recommendation 4: The OAIC recommends that pre-selection should not proceed.

1.16 If pre-selection is to proceed, the OAIC recognises Treasury's proposed mitigation to replace active engagement with an explanation and agrees the policy intention is better achieved by the phrase '*explaining why each option is reasonably needed*' (as at draft rules, subrule 4.11(3)) rather than the phrase '*how each option presented is reasonably needed*' (as at draft rules, subrule 4.20E(3)). The former phrase avoids the unintended consequence of an entity simply stating that a dataset or use is reasonably needed without further explanation. This change also creates alignment with the requirement for the request process to have regard to the data standards, including any consumer experience guidelines.

1.17 Where pre-selection occurs, there will be a need for assurance that data minimisation has been met. Treasury will need to consider introducing mechanisms to ensure that the limitation on pre-selecting only reasonably needed options, and compliance with the data minimisation principle, is able to be monitored and enforced in practice.

1.18 Retaining the example relating to pre-selection in CDR rules 4.11 and 4.20E is also appropriate, as it clarifies that having un-filled boxes would not be contrary to the CDR rules. Leaving the example in would also benefit an accredited data recipient (ADR) that does not want to change their current business processes or incur costs to move towards pre-selection.

1.19 As for bundling, it will be important to create consistency between the explanatory materials and draft rules by making explicit that the intent is to permit pre-selection in the context of the singular term 'good or service' rather than the plural term 'goods or services'.

Recommendation 5: If Treasury choose to proceed with pre-selection, the OAIC recommends:

- retaining active selection for disclosure recipients and duration,
- using the phrase *'explaining why each option is reasonably needed'*, rather than '*how each option presented is reasonably needed*',
- introducing mechanisms to ensure protections can be monitored and enforced in practice, for example, by increasing record keeping and reporting obligations,
- retaining the example relating to pre-selection in CDR rules 4.11 and 4.20E.

Further information about supporting parties

1.20 In general, the OAIC is supportive of this measure to provide consumers with more information about supporting parties.

Recommendation 6: As raised in our submission to the Consent Review Design Paper in October 2023, the OAIC recommends that Treasury consider whether the proposed amendments can accommodate circumstances where there are future changes to supporting parties. e.g. where an ADR or CDR representative engages an outsourced service provider (OSP) after the consumer has provided consent (where the consumer was not notified that their information may be disclosed to an OSP during the consent flow).

Changes to the data minimisation principle

1.21 The OAIC supports extension of the data minimisation principle to disclosure of CDR data.

1.22 However, the OAIC is concerned that the addition of the phrase *'or to effect the permitted use or disclosure'* in draft rule 1.8(2) may have the unintended effect of allowing entities to use and disclose CDR data without any consideration of data minimisation. This is because the list of permitted uses and disclosures at CDR rule 7.5 is the broadest possible description of consented uses and disclosures within CDR and it could be argued that a maximum range of uses and disclosures are 'reasonably needed' to 'effect' these.

Recommendation 7: The OAIC recommends that Treasury consider a narrower construction of draft rule 1.8(2), to ensure data minimisation relates to the consumer's specific requests and so that compliance with the data minimisation principle can be demonstrated by entities. This will assist data minimisation to function as a layer of consumer protection that applies in addition to consent.

Part 2: Key privacy impacts of the proposed operational enhancements

2.1 The draft rules make a range of changes aimed at supporting use case development and making it easier for businesses to use CDR data. The draft rules cover a range of policy issues, including the circumstances in which an accredited ADI can hold CDR data as a data holder, the process for appointing a nominated representative, obligations for CDR representative principals, account holder control for data sharing requests made by secondary users, and a range of amendments relating to the energy sector.

2.2 With respect to the measures in the draft rules, the OAIC is broadly supportive of the majority of these changes. While the measure to expand the circumstances in which an accredited ADI can hold CDR data as a data holder will require careful consideration, many of the other measures are privacy enhancing and will increase choice, transparency and consistency for CDR consumers. These issues are analysed below.

Expanding the circumstances in which accredited ADIs can hold CDR data as a data holder

2.3 The draft rules propose new conditions that will expand the circumstances in which an accredited ADI can hold CDR data as a data holder,[3] including where a consumer has applied or is applying for a product. Accredited ADIs that elect to meet new conditions involving notification will be required to provide consumers with a notice, before collection of CDR data, that they will hold the data as a data holder.

[3] CDR rules, clause 7.2 of Schedule 3 sets out the existing conditions for an accredited ADI to be a data holder in the banking sector.

2.4 Given accredited persons are subject to the CDR Privacy Safeguards in the CC Act and data holders hold data subject to the Australian Privacy Principles in the Privacy Act,[4] this amendment will shift the privacy framework that applies to certain CDR data by enabling more CDR data to be held outside of the CDR framework.

2.5 The OAIC appreciates the policy intention behind this measure, however, is concerned about the increased fragmentation and complexity that will occur as a result of two privacy frameworks and the impact this will have on both privacy compliance and consumer comprehension as discussed below.

Impact on compliance

2.6 From a compliance perspective, who the conditions apply to and in what circumstances needs to be absolutely clear and well understood to ensure application of the correct privacy framework and the adequate protection of consumer data. Without clear boundaries, there is a risk that accredited ADIs could misapply or misconstrue their obligations, leading to potential non-compliance and inconsistent regulation.

2.7 From the OAIC's understanding, the new conditions in the rules apply only to:

- the banking and not the energy sector[5]
- accredited ADIs and not to other ADRs who may receive similar CDR data from a consumer in similar circumstances
- some but not all collections of CDR data by an accredited ADI as the measure applies where a consumer is applying or has applied for a product, and not where a consumer is comparing products or seeking quotes.

Recommendation 8: To ensure clarity for consumers, entities and regulators, the OAIC recommends Treasury strengthen the draft rules and explanatory materials to be clear about which privacy framework is intended to apply to an accredited ADI and when, including more explicit explanation of the point at which the privacy frameworks change under each condition.

Recommendation 9: For accountability, Treasury should also strengthen record keeping obligations for accredited ADIs and implement civil penalty provisions to cover deliberate non-compliance.

Supporting consumer understanding of the change in privacy framework

2.8 The draft rules require accredited ADIs to inform the consumer that data holder obligations (rather than ADR obligations) apply, and the manner in which they propose to treat the data. The OAIC echoes the findings in the Privacy Impact Assessment and recommends clear and

[4] See the OAIC's Guide to privacy for data holders for more information about when the CDR Privacy Safeguards and Australian Privacy Principles apply to data holders.

[5] CDR rules, clause 9.2 of Schedule 4 sets out the existing conditions for an accredited person to be a data holder in the energy sector.

relevant information be provided to the consumer about the practical implications of the change in privacy framework both in the consent flow *and* in the CDR Policy.

Recommendation 10: While not exhaustive, the OAIC recommends the specific matters that should be brought to the consumer's attention at the time of consent could cover: notification of collection/future collections of data, how CDR data will be used including secondary uses beyond what is consented to, and how the accredited ADI will treat the data after it has been used for the original purpose. This should include a clear statement at the time of collection confirming that the CDR framework does not apply to the handling of the CDR data.

Recommendation 11: The OAIC recommends accredited ADIs who elect to meet the conditions in the rules should clearly address in their CDR Policy how they propose to treat CDR data where they are permitted to hold it as a data holder rather than as an ADR. This will help support consumer understanding and transparency in the way CDR data is being held, particularly given consumers cannot be expected to have a sophisticated understanding of the differences between the CDR privacy framework and the Privacy Act.

Secondary users

2.9 The draft rules remove the obligation to provide an account holder with functionality to stop CDR data being disclosed to a particular ADR in response to a data sharing request made by a secondary user. The amendments would maintain the ability for an account holder to make a secondary user instruction and withdraw that instruction at any time, and enhance this functionality by ensuring it is prominently displayed.

2.10 The OAIC is broadly supportive of this measure, as it centralises and simplifies account holder control through controlling access on a user level, rather than on a per-accredited person basis. While this draft rule would result in a reduction of granular control by the account holder, the OAIC acknowledges that it helps to avoid unintended consequences for the account holder, while still maintaining the key privacy enhancing features of the secondary user obligations.

2.11 To further enhance the proposed secondary user provisions, the OAIC encourages Treasury to consider whether further protections are required where a secondary user shares CDR data to an ADR that the account holder does not wish to share with. For example, if a secondary user shares CDR data with an ADR that the account holder does not wish to share data with, and as a result the account holder withdraws the secondary user instructions, our understanding is that the withdrawal would not automatically cause an existing authorisation enabled by the secondary user to expire. It would only block the secondary user from sharing CDR data from the account in the future.

Recommendation 12: The OAIC recommends that where an account holder withdraws a secondary user instruction, the data holder also informs the account holder how they may stop the sharing of any existing authorisations enabled by the secondary user's data sharing request, to ensure that the ADR is notified and subsequently destroys that CDR data. Alternatively, if the policy intent is for the withdrawal of a secondary user instruction to result in the expiry of an authorisation, that this is clarified in the CDR rules.

Nominated representatives

2.12 The OAIC supports the draft rules regarding nominated representatives, which would introduce an additional requirement on data holders to provide a service for non-individuals or partnerships to appoint nominated representatives. The requirement to ensure that the service would need to be prominently displayed and readily accessible, as well as simple and straightforward to use (draft rules, subrules 1.13(c) and(d)) is also supported. The introduction of these nominated representative requirements would help to ensure there are clear, simple and appropriate arrangements in place for business consumers to appoint nominated persons.

2.13 In addition, the draft rules would require the data holder to offer an online process to allow non-individual and partnership consumers to nominate account administrators as nominated representatives (draft rules, subrule 1.13(1A)). The OAIC supports the decision not to deem an online administrator as a nominated representative under the CDR rules following feedback from stakeholders in response to the design paper. The flexibility provided in the draft rules ensures that account holders can continue to actively take steps to appoint a nominated representative and allows the data holder to appropriately verify the nominated representative based on its own legislative obligations and risk posture.

Part 3: Other compliance risks and issues

3.1 The OAIC have noticed the following internal inconsistencies in wording of the draft rules which should be addressed to avoid compliance risks and confusion amongst entities:

Draft rule/amendment	Inconsistency
4.20D	Should be the same as 4.10
4.20E(3)	Should be the same as 4.11(3)
4.20F(2)	Should be the same as 4.12(2)
4.20O	Should be the same as 4.18
4.20Q(1)(b)	Should be the same as 4.20(1)
4.20Q(2)	Should be the same as 4.18A(2)
4.20V	Should be the same as 4.20AB
Amendment 82	Should relate to 4.20E(1)(note 3)
4.20E(3)(k)(v)	Should be ‘CDR’
9.3(2)(f), 9.3(2A)(i), 9.4 (2)(f)(ii) and 9.4(2A)(e)(v)	References to election to delete should be removed unless there is a reason for continued reporting