Australian Government

Office of the Australian Information Commissioner

CDR Consent Review – CDR rules and data standards design paper

Submission by the Office of the Australian Information Commissioner

Angelene Falk

Australian Information Commissioner and Privacy Commissioner

4 October 2023

OAIC

Introduction

The Office of the Australian Information Commissioner (OAIC) welcomes the opportunity to comment on the CDR Consent Review – CDR rules and data standards design paper (design paper). We understand Treasury and the Data Standards Body (DSB) intend to use feedback received through this consultation to inform their review of consent requirements in the Competition and Consumer (Consumer Data Right) Rules 2020 (CDR rules) and data standards (standards).

The OAIC supports this consultation and the CDR consent review. Conducting a review of consent processes helps ensure CDR rules and standards are fit for purpose, support the objects of the CDR and CDR consents,[1] and operate as intended. As recognised in the design paper, a core component of the consent review must be ensuring key consumer protections, including privacy and security protections, are maintained when changes to consent are considered.[2] This reflects that strong privacy and information security protections are a fundamental element of the CDR.[3]

The design paper includes proposals about a range of policy issues relevant to consent, as well as matters for future consideration. In the time available and noting concurrent CDR consultations, this submission focuses on the proposals regarding consent bundling, preselection of datasets and supporting parties. The submission builds on advice the OAIC has previously provided to Treasury about the critical role consent plays in supporting consumer trust in the CDR.[4]

Consistent with the requirements in section 56BR of the *Competition and Consumer Act 2010* (Competition and Consumer Act), if and when future rules are developed to implement the proposals in the design paper, the Information Commissioner will analyse and advise on the privacy impacts of those rules.

General feedback

Consent is a key part of the CDR privacy framework. It enables consumers to be the decision makers in the CDR, ensuring that they can make informed decisions regarding collection, use and disclosure of their CDR data in order to obtain the most value from it.[5] Consent processes also contribute to ensuring consumers have knowledge of, and choice and control over, how information about them is handled by businesses that collect it through the CDR.[6] Noting the important connection between privacy and consent, the OAIC provides the following general feedback regarding the design paper.

---

[1] *Competition and Consumer Act 2010* (Competition and Consumer Act), s 56AA; CDR rule 4.9.

[2] CDR Consent Review - CDR rules and data standards design paper (treasury.gov.au): 'The Treasury and the Data Standards Body (DSB) are reviewing the Competition and Consumer (Consumer Data Right) Rules 2020 (the CDR Rules) and Data Standards (standards) for consent to support a better consumer experience while maintaining key consumer protections.'

[3] Explanatory Memorandum, *Treasury Laws Amendment (Consumer Data Right) Act 2019*, paragraph 1.6: 'Strong privacy and information security provisions are a fundamental element of the CDR.'

[4] See also Statutory Review of the Consumer Data Right - Report (treasury.gov.au) (Statutory Review Report), finding 2.2: 'the consent process is central to CDR's realisation of informed consumer decision making and delivery of consumer benefits'.

[5] See Privacy Safeguard Guidelines, Chapter C: Consent, paragraphs C.1–C.2.

[6] See also the OAIC's submission to the Privacy Act Review Issues Paper (Part 5) and submission to the Privacy Act Review Discussion Paper (Part 9), which include analysis relevant to privacy self-management, notice and consent.

Research and engagement

The design paper cites input from a range of sources that suggest existing consent processes may not be meeting consumers' needs. In light of this feedback, the OAIC supports consideration of measures to improve the CDR consent process for consumers. However, we consider that further research and engagement should be undertaken before progressing the proposals in the design paper.

The design paper refers to and draws upon research conducted by DSB for the purposes of the consent review.[7] That research included surveys, unmoderated prototype tasks and moderated prototype interviews. While the survey stage of the research presented four written scenarios,[8] the prototype tasks involved one scenario. That scenario related to an accredited data recipient (ADR) seeking consent to collect and use banking data. It did not involve non-banking or cross-sectoral use cases, one-off consents, CDR representatives, or disclosure consents.[9] The research also returned indeterminate results for preselection,[10] and appears to have presented a noncompliant current-state consent flow for bundling.[11]

Given the range of CDR use cases, which involve different types of consumers and participants and different levels of risk to the consumer, a one-size-fits-all approach to consent may not be appropriate. For example, an ongoing consent related to a financial management service is likely to have different considerations and consequences for a consumer when compared to a one-off consent related to a short-term consumer credit contract ('pay day loan').[12] Use cases involving a CDR representative may have different issues to use cases involving only an ADR.[13] Some consumers may be less likely or less able to engage with or understand the implications of providing their consent, including consumers experiencing vulnerability. Combining datasets across sectors may present risks that do not arise when information sought is from a single data holder. It is our view that Treasury and DSB must consider a broader and more reflective range of use cases in the CDR and whether there are some use cases for which proposed measures to simplify consent processes carry a higher risk for consumers than should be tolerated.

To ensure the proposals in the design paper will meet consumers' needs and best support the objects of the CDR, we suggest further research be conducted on the proposed measures. We recommend this include further research on preselection and bundling proposals, and regarding different CDR use cases, such as complex or emerging use cases and use cases involving different CDR participants. We

[7] Consent Review Research Report (Q3 2022, R1-3).

[8] Finance management, comparison tool, loan application, and lease application use cases.

[9] Although noting the design paper refers to 2021 research regarding disclosure consents.

[10] The CX research has not demonstrated clear support for this measure and we are concerned about the impact allowing preselection of datasets will have on consumer understanding and engagement with the consent flow as well consumer control over their data sharing to receive a particular good or service.

[11] The CX research for bundling of consents tested consumer responses to bundled collection and use consents, concluding that it matched consumers' mental models. It did not test consumer responses to an unbundled consent flow.

[12] See Consumer Data Right rules – expansion to the non-bank lending sector | Treasury.gov.au.

[13] For example, when a CDR representative receives a consent related to information held by a data holder, their CDR principal will collect that information on the CDR representative's behalf. CDR representatives and ADRs are also subject to different levels of oversight (e.g., ADRs are subject to an accreditation process, while CDR representatives are not).

also suggest the research consider use cases involving higher risk or sensitive datasets and seek to understand how the proposed changes are likely to impact consumers experiencing vulnerability.[14]

We recommend this analysis also include examination of consumer experience in the real-world environment, including through further direct engagement with consumers and their representatives, to better understand how consumers interact with the existing consent flow and ensure the measures are appropriately targeted and fit for purpose.

Recommendation 1: Treasury and DSB undertake further research to support the proposed measures, including how the measures will impact consumer control and informed consent in complex or emerging use cases, and those involving sensitive information, and the risks associated with different entities who may handle CDR data.

Recommendation 2: Treasury and DSB further consider the consumer experience in the real-world environment through direct engagement with consumers and their representatives, to better understand how consumers engage with the existing consent flow and ensure the measures are appropriately targeted and fit for purpose.

Privacy Impact Assessment

It will be important that Treasury's planned Privacy Impact Assessment (PIA) consider the privacy impacts of each proposal in the design paper.[15] As well as considering the particular proposals, we recommend the PIA analyse the combined impact of the proposals on consumers' privacy. This should include impacts on active consumer engagement in the consent process, such as understanding what is being consented to, what data is being collected and for what purpose(s). The PIA should also consider circumstances where a CDR consent facilitates the handling of any high risk or sensitive data sets.

Consistent with a privacy-by-design approach, Treasury should conduct the PIA early, so it can inform the development of any draft rules. We suggest Treasury also revisit previous CDR PIAs to consider how changes to the consent model may impact on the issues and mitigation measures identified in those assessments.[16]

Recommendation 3: Treasury's planned PIA consider the feedback in this submission and other feedback received to the design paper at an early stage, to inform the development of any CDR rules.

[14] The CX research noted that further research on consumer control would be beneficial, particularly as the CDR expands to support other sectors, use cases, and action and payment initiation. We support this recommendation.

[15] See Guide to undertaking privacy impact assessments | OAIC and Privacy (Australian Government Agencies – Governance) APP Code 2017.

[16] This reflects Treasury's commitment to treat CDR PIAs as living documents: Consumer Data Right PIA - Agency Response (treasury.gov.au), 5.

Recommendation 4: Treasury revisit previous CDR PIAs to consider how changes to the consent model may impact on the issues and mitigation measures identified in those assessments.

Interaction with other settings and processes

Alongside and as part of the analysis suggested above, we recommend Treasury and the DSB consider the interaction between consent proposals and the broader CDR operating environment. In particular, we recommend further analysis regarding:

- **the impact of proposed changes on the CDR privacy framework as a whole**, to ensure overall CDR privacy settings remain proportionate to the risks. Consent is only effective in giving individuals choice and control if used appropriately and alongside other privacy protections.[17] We therefore recommend analysis include a focus on ensuring the right balance is struck between privacy self-management and the obligations on entities to ensure CDR data is handled appropriately.[18] It should also include consideration of whether existing compliance and monitoring obligations remain appropriate (for example, whether accredited persons and CDR representatives should be subject to additional record-keeping or reporting obligations).[19]
- **the interaction between proposed changes and the proposals in the Privacy Act Review**. As noted in the design paper, the Privacy Act Review Report proposed amendments to consent settings in the *Privacy Act 1988* (Privacy Act). Accredited persons and some CDR representatives are APP entities,[20] and CDR-specific privacy settings operate in conjunction with the Privacy Act.[21] We therefore recommend Treasury consider whether the consent review is best progressed now or at a later stage, so that opportunities to streamline and harmonise the CDR and the Privacy Act to reduce regulatory friction may be considered.

Thorough examination of the design paper proposals at an early stage will ensure any changes meet consumer needs and do not result in unintended consequences. Ultimately, this will support consumer trust, confidence, and engagement with the CDR in the long-term.

[17] See OAIC submission to Privacy Act Review Issues Paper, 70, in relation to limitations of consent.

[18] See, for example, the proposed obligations in Chapters 12, 13 and 15 of the Privacy Act Review Report 2022 (ag.gov.au).

[19] We note that this recommendation may align with proposal 15.1 of the Privacy Act Review Report 2022 (ag.gov.au), that an APP entity must determine and record the purposes for which it will collect, use and disclose personal information at or before the time of collection. See also Article 30 of the GDPR which requires entities to record, amongst other things, the purposes for which they process personal data, the types of personal data processed and the parties to whom it is disclosed.

[20] The Privacy Act applies to most organisations with an annual turnover of more than $3 million, including accredited persons and CDR representatives that meet this threshold. While the Privacy Act does *not* usually apply to businesses with an annual turnover of $3 million or less (small business exemption), in relation to the CDR, it does apply to small business operators that are accredited persons, for personal information that is not CDR data: subs 6E(1D), Privacy Act. This means that accredited persons will be APP entities, provided no other Privacy Act exemption applies.

[21] Explanatory Memorandum, [1.296]: 'It is useful to understand how the Privacy Safeguards work in conjunction with the Privacy Act 1988 and APPs.'

Recommendation 5: Treasury and DSB consider the interaction between consent proposals and the broader CDR framework, including in relation to overall CDR privacy settings, and developments in the privacy landscape outside the CDR.

Feedback on proposed measures

The proposals in the design paper are likely to impact CDR consumer privacy and confidentiality. Based on the information available, the OAIC considers the measures related to supporting parties, deletion by default and dark patterns have the potential to improve consumer privacy outcomes in the CDR. We have outlined some initial feedback in relation to supporting parties below. The OAIC will provide further feedback on the specifics of these proposals, and the other proposals in the design paper, as further detail becomes available (for example, if these proposals proceed to draft rules).

The OAIC is concerned about the privacy impacts of the proposal to expressly permit bundling of CDR consents (Issue 1) and to allow ADRs and CDR representatives to preselect datasets in the consent flow (Issue 2). In our view, there is a risk that these proposals could have the unintended effect of undermining consumer engagement and comprehension of the consent they are being asked to provide and, when taken together, may result in reduced consumer control and poorer consumer outcomes. We have outlined specific feedback on these proposals below.

Measure 1: Bundling of consents

The design paper proposes to amend the existing prohibition on bundling consents with other directions, permissions, consents or agreements in the CDR Rules to expressly permit ADRs and CDR representatives to bundle collection and use consents that are reasonably required for the provision of the requested service. Treasury has also sought feedback on bundling disclosure consents.

We appreciate that CDR products or services are likely to require a collection and use consent, and that bundling these consents may be intuitive for consumers. The appropriate level of specificity when seeking consent may also be affected by factors such as the sensitivity of the information involved and whether the collection or use would be reasonably expected by the consumer.[22] However, bundling of consents carries risk and, in some circumstances, has the potential to undermine the voluntary nature of consent.[23]

Based on the information presented in the design paper, the OAIC does not support the proposal to bundle CDR consents. If this measure is progressed, we recommend a limited approach to consent bundling and suggest Treasury consider whether additional safeguards are needed, including to address the following matters.

Definition of 'reasonably required'

In the design paper Treasury has proposed to expressly permit the bundling of consents that are 'reasonably required for the provision of the requested service'. This is different to the proposal for pre-selection in the design paper, which would only permit pre-selection of datasets that are

[22] APP guidelines, Chapter B: Key concepts, B.53. See also: Privacy Act Review Report 2022 (ag.gov.au), 105.

[23] APP guidelines, Chapter B: Key concepts, B.39 and B.40

'essential' for the service. We recommend Treasury clearly explain the distinction between these two terms ('reasonably required' and 'essential') including the risk of complexity for participants where there are two different standards proposed.

Further, Treasury should consider adopting a narrow definition of 'reasonably required for the provision of the requested service' and consider whether safeguards are needed to support this requirement. For example, this could include record keeping or reporting obligations for participants, such as to document why the consent being requested is reasonably required to provide the requested service. We expect targeted guidance would also be needed to support compliance.

In circumstances where collection and use are not both required for the product or service (this might arise where an ADR or CDR representative collects CDR data for the sole purpose of disclosing it to a trusted adviser), we recommend bundling is taken not to be 'reasonably required'.

Collection and use must be clearly explained

The CDR rules require that, when seeking a consumer's collection or use consent, an ADR or CDR representative must inform the consumer of how the collection or use complies with the data minimisation principle, including how the collection is reasonably needed, and use would not go beyond what is reasonably needed.[24]

As use cases in the CDR become increasingly complex, involving multiple and/or primary and secondary uses, there may be a risk that consumers do not always have visibility of, or are not always adequately informed of, the specific uses to which their CDR data will be put. This may be amplified in a bundled consent flow where collection and use consents are bundled as a single consent and where datasets are preselected (see below Measure 2: Pre-selected and actively selected options). We are concerned that a reduction in positive friction would reduce consumer engagement in the consent flow.

The OAIC recommends that if, contrary to our submission, the proposal to bundle consents is progressed, Treasury and the DSB ensure related settings remain appropriate to ensure the objects of consent in the CDR rules are upheld, for example consent is informed, including in relation to the information provided and language used in the consent flow.

Bundling should be limited to collection and use consents

Bundling should not be extended to disclosure consents. In our view, disclosure consents present increased risks to consumers, noting disclosures may be made to trusted advisers and other unaccredited entities which are not subject to CDR privacy and security obligations, and may also not be subject to the Privacy Act.[25] As such, we consider it essential for consumers to be given the opportunity to consider these consents separately before deciding whether to provide a disclosure consent. We note direct marketing and deidentification consents, by their nature, are not required for the provision of a product or service and should not be subject to bundling.

[24] CDR rule 4.11(3)(c). For CDR representatives, see also CDR rule 4.3A.

[25] For example, if the unaccredited entity is covered by the small business operator exemption, the Privacy Act will not apply.

Non-CDR permissions

We do not support combining CDR consents with non-CDR permissions in a single consent flow. As outlined in the paper, there is a risk that the consumer may misunderstand the application of the protections provided under the CDR or mistakenly attribute these to the non-CDR consents.

Recommendation 6: The current proposal to allow bundling of consents should not be progressed. If contrary to our submission this is progressed, a limited approach should be taken, informed by the issues raised in this submission.

Measure 2: Pre-selected and actively selected options

The design paper proposes that, instead of requiring a consumer to actively select each dataset in the consent flow, ADRs and CDR representatives would be allowed to pre-select or clearly indicate the datasets that are essential for the service to function.

Generally, consumers make a deliberate and intentional choice to participate in the CDR. Active selection of datasets is a valuable way of securing consumer engagement in the consent flow and ensuring consent is both properly informed and expressly provided. This friction can help ensure the consumer understands and is comfortable with the consent they are providing. For example, if a consumer decided not to actively select a particular dataset and as a result was not able to be provided with a service, this would engage a consumer in making a deliberate choice about whether they are comfortable with sharing that additional personal information with the ADR or CDR representative to be able to proceed with receiving a service.

While we do not support the preselection proposal in the design paper, if contrary to this submission this measure is progressed, we recommend Treasury and DSB consider the following matters.

Definition of 'essential'

Should Treasury proceed with this measure, we recommend a narrow definition of what is 'essential' for a service/product. Depending on the service being offered, there may be scope or discretion on the part of the ADR or CDR representative in identifying what information is an essential dataset for the purposes of a service. Creating a pause at this point in the consent flow allows consumers to properly consider whether they are comfortable that the datasets requested by the ADR or CDR representative are needed for the requested product or service, and whether they wish to proceed with the consent.

We are concerned there may be a risk that ADRs or CDR representatives will determine that datasets are 'essential' to provide a premium or optimal service to the consumer, even where a more limited or basic service could be provided with a more limited range of CDR data from the consumer.

We recommend Treasury consider whether additional safeguards are required to ensure ADRs and CDR representatives, in designing their platforms or services, only pre-select essential datasets for each service. Additional guidance may also be required to ensure only those datasets that are clearly essential for a service to function are being preselected and to maintain compliance with the data minimisation principle.

Pre-selection of duration

The pre-selection measure would also allow ADRs or CDR representatives to specify the duration of a consent, where a particular duration is reasonably required for the requested service to function. This reflects that some goods and services may require specific or minimum durations to function.

We support allowing consumers to select the duration of time their data is shared, noting this aligns with the intention of the CDR for consumers to be able to have control over how their data is shared and used in the CDR. We note that the CX research did not identify clear support for this measure, finding that the evidence was indeterminate and noting mixed responses from consumers about the degree to which control over duration is important in the consent flow.

If progressed, we suggest that settings regarding the duration of consent ensure consumers will not be influenced into thinking a particular duration must be selected, where other options for duration are available.

Recommendation 7: The current proposal to allow preselection of datasets should not be progressed. However, if contrary to our submission it is progressed, Treasury and DSB should amend the proposal to address the issues raised in this submission.

Measure 4: Supporting Parties

The design paper proposes to clarify the existing notification requirements during the consent flow, so consumers are notified about which supporting parties may access the consumer's CDR data based on the relevant supporting parties at the time of consent.

We support the proposal to align consent information requirements for supporting parties in the CDR. Presenting this information during the consent flow helps to support informed consent and increases transparency for the consumer regarding who would be able to access, use and disclose their data if shared. To ensure consumers are adequately informed about potential future changes to supporting parties, we support a combined requirement that consumers are:

- informed about potential future changes to supporting parties at the time of providing consent, **and**
- notified of changes to supporting parties after consent is provided, including that the consumer can withdraw or update their consent at any time.

Requiring the consumer to be informed of the possibility of changes to supporting parties at the time of consent, and notified of the changes after consent is provided, allows the consumer to consider the changes to the parties who may access, use or disclose their data and decide if they want to continue providing an ADR or CDR representative with their consent.

In relation to outsourced service providers (OSPs), we only support the notification proposal where the consumer was informed that their data may be disclosed to an OSP during the consent flow. The rules currently require an ADR or CDR representative to inform a consumer that their information may

be handled by an OSP as part of the consent flow.[26] A decision by an ADR or CDR representative to engage an OSP without first notifying the consumer of their intent to do so in the consent process may impact the informed nature of the consumer's consent. In these situations, it may be appropriate for an ADR or CDR representative to obtain the consumer's consent to disclose their CDR data to a supporting party. We suggest Treasury consider this issue as part of progressing this measure.

Recommendation 8: Treasury should consider amendments to the supporting parties proposal, to address the impact of an ADR or CDR representative engaging an 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).

[26] CDR rule 4.11(3)(f). For CDR representatives, see also CDR rule 4.3A.