Australian Government

Consumer Data Right

Privacy impact assessment

Consent review rule changes and operational enhancements

Treasury response

November 2024

Background

On 6 November 2024, the Assistant Treasurer and Minister for Financial Services, the Hon Stephen Jones MP (the Minister) made the ***Competition and Consumer (Consumer Data Right) Amendment (2024 Measures No. 1) Rules 2024*** which amends the *Competition and Consumer (Consumer Data Right) Rules 2020* (CDR rules). The amendments include changes to the consent rules and operational enhancements which seek to improve the consumer's consent experience and to improve the usability of the CDR.

The rules follow consultation on exposure draft amendments to the CDR rules and explanatory materials that occurred between 9 August and 9 September 2024. The consultation included a stakeholder forum held on 23 August 2024, bilateral meetings with a range of stakeholders, and careful consideration of the submissions received in relation to the proposed consent rule changes and operational enhancements.

The *Privacy (Australian Government Agencies – Governance) APP Code 2017* requires a privacy impact assessment (PIA) to be conducted for all high privacy risk projects. The PIA must identify impacts on the privacy of individuals and set out recommendations for managing, minimising, or eliminating that impact.

Under the *Competition and Consumer Act 2010* (CCA), the Minister must consider the likely effect of making the rules on the privacy or confidentiality of consumers' information before making the CDR rules. This must be considered alongside a range of other matters, including:

- the likely effect of making the instrument on the interests of consumers,
- the efficiency of relevant markets,
- promoting competition,
- promoting data driven innovation,
- any intellectual property in the information to be covered by the instrument,
- the public interest, and
- the likely regulatory impact of the making of the CDR rules.

Treasury engaged Mills Oakley to conduct a PIA for the proposed consent rule changes and operational enhancements, to ensure the amendments effectively manage privacy risks and to inform the Minister's decision to make the amendments.

The PIA was informed by submissions to the Consent Review and Operational Enhancements design papers, policy specifications, and draft rules. It was prepared on the basis that it supplements the other independent PIAs that have been conducted for the CDR to date, including for the implementation of the CDR in the banking and energy sectors.

The final PIA is available on the Treasury website.

The PIA included 10 recommendations. This document provides Treasury's response to each of these recommendations.

PIA recommendations and Treasury response

Recommendation 1: Bundling of consents

The Treasury consider whether 'reasonably needed' is sufficiently narrow to avoid function creep and the inadvertent expansion of consent requests. If the term will be interpreted narrowly and supports an inference that the consent request must be essential to provide the product or service, this could be addressed in guidelines that Treasury has indicated it intends to explore with OAIC and the ACCC.

Treasury notes this recommendation. The concept of something being 'reasonably needed' is generally understood as an objective test and is commonly used in legislation on that basis. Treasury has included guidance to this effect in the explanatory statement, including that this test would not be met if the consent was only useful or preferable for a data recipient to have.

Treasury will also work with the Australian Competition and Consumer Commission (ACCC), and the Office of the Australian Information Commissioner (OAIC) to consider if further guidance material is needed for CDR participants to make an objective assessment.

Recommendation 2: Bundling of consents

Treasury consider whether excluding disclosure consents from consent bundling usefully reinforces transparency requirements about the parties with whom a CDR consumers' [sic] data is shared.

Treasury does not accept this recommendation. Treasury's view is the rules have been amended to include mechanisms that better achieve the desired outcome, while also improving the consumer consent experience.

The rules extend the data minimisation principle to the disclosure of CDR data. That is, the data recipient cannot disclose the collected data beyond what is reasonably needed to provide the requested good or service. The data minimisation principle applies to all consents regardless of whether they have been bundled.

When asking for a consent, the data recipient must either allow the consumer to clearly indicate or seek the consumer's agreement to the person to whom the CDR data would be disclosed. Further, the data recipient must provide the consumer an explanation of why that disclosure does not exceed what is reasonably needed to provide the requested good or service to the CDR consumer.

Recommendation 3: Bundling of consents

As an alternative to Recommendation 2, Treasury consider a measure that gives CDR consumers the right to object to bundled consents which would trigger an obligation for the accredited person or ADR to explain the basis for the conclusion that the consents are essential to provide the product or service. A right to object, in this context, could conceivably be aligned with Privacy Act reforms, in the event a right to object to certain privacy practices is progressed by the Australian Government.

Treasury does not accept this recommendation. The CDR is an opt-in system that gives consumers control over their own data. Consumers have a right to object to bundled consents by not providing

their consent. As noted in Treasury's response to Recommendation 1, it is not sufficient for a consent to be only useful or preferable for a data recipient to have.

Data recipients are also already required to explain why each collection, use, or disclosure consent complies with the data minimisation principle. As such, Treasury's view is there is little benefit to implementing a 'right to object' as outlined in this recommendation.

Recommendation 4: Pre-selection of consent options

Subject to Recommendation 3, Treasury consider whether guidelines and CX Standards would be an appropriate vehicle to clarify (a) whether a consumer can override pre-selected options and (b) the level of detail necessary to explain why a pre-selected option is necessary to deliver the product or service.

Treasury does not accept this recommendation. Treasury does not consider it necessary for guidelines and CX standards to clarify whether a consumer can override pre-selected options. As noted in Treasury's response to Recommendation 3, consumers have a right to object to a pre-selected consent by not providing their consent; and a consent cannot be requested simply because it would be useful or preferable for a data recipient to have.

Data recipients are required to explain why a consent complies with the data minimisation principle, whether it has been pre-selected or not. As such, Treasury's view is it is not necessary to require accredited persons to provide consumers the option to override a pre-selected consent.

Recommendation 5: Providing information about the withdrawal of consent

Treasury consider whether guidance, such as in CX Standards, might encourage an Accredited Person to tell consumers, as part of a consent flow, where to find further information about withdrawing consent.

Treasury notes this recommendation. Information about withdrawing consent is important. However, Treasury notes findings from the DSB's Consent Review Research[1] show consumers value this information being accessible in the CDR receipt, as artefacts that can be accessed later if needed. The rules would only require data recipients to advise the consumer, at the time of consent, that the consent can be withdrawn at any time. Information on how a consent can be withdrawn would be provided in the CDR receipt, which must be provided as soon as practicable after the consumer provides a consent.

Recommendation 6: Dark patterns

Treasury's regulatory response (if any) to mitigate the risk of dark patterns being used in CDR user experience design patterns and consent/authorisation architecture should be informed by the Privacy Act reforms on this issue.

Treasury agrees in principle with this recommendation. Treasury will consider this in developing any future regulatory response to mitigate the risk of dark patterns (otherwise known as deceptive patterns) being used in CDR user experience design patterns and consent/authorisation architecture.

[1] Consent Review Research Report (Q3 2022, R1-3) – July 2023.

Recommendation 7: Dark patterns

Treasury consider supporting any regulatory response or guidance material about avoiding dark patterns with visual examples of what is not permitted (i.e. an illustrative example of a dark pattern in a CDR context).

Treasury agrees in principle with this recommendation. Treasury will consider this in developing any regulatory response. If guidance material is required, Treasury will engage with the DSB, ACCC, and OAIC as appropriate.

Recommendation 8: Accredited authorised deposit-taking institution (accredited banks) holding CDR data as a data holder

Noting that the Treasury has narrowed the scope of the proposal such that the data in question has been obtained in connection with an application to acquire a product or service, Treasury may wish to consider whether the CDR consumer's decision (and autonomy over the CDR data) would be assisted by an explanation by the ADI about the *practical consequences* of consenting to the ADI holding the data as a data holder.

Treasury agrees with this recommendation. It is important that consumers understand how the accredited bank would hold their data. Treasury notes while the PIA's findings echo the feedback from the OAIC, other stakeholders indicated an explanation of the way data is held by an ADI would be overly technical, increase friction and would not support the ordinary CDR consumer's understanding.

Treasury has simplified the information an accredited bank is required to provide as part of a notification, requiring CDR consumers to be informed that their data will be held in accordance with the accredited bank's usual data holding practices for consumer data.

Recommendation 9: Deferral of data holder obligations for an ADR who becomes a small energy retailer

Treasury consider the feasibility of a regulatory and enforcement strategy that is calibrated to support small retailers meet their CDR obligations rather than defer the application of those obligations.

Treasury does not accept this recommendation. The ACCC and the OAIC determine the CDR enforcement strategy. The *ACCC/OAIC Joint Compliance and Enforcement Policy for the Consumer Data Right* sets out how these agencies will address conduct, including in relation to failure to meet compliance dates. The policy sets out the strategies that the regulators will use to foster compliance with CDR obligations, and the application of these strategies in the context of small retailers is appropriately left to the ACCC and OAIC.[2]

Treasury considers it appropriate to provide additional time for an ADR that becomes a small retailer to become compliant with CDR data holder obligations. This would be consistent with the approach taken if a small retailer becomes an ADR.

[2] ACCC/OAIC Compliance and Enforcement Policy for the Consumer Data Right – October 2023.

Recommendation 10: Products for the energy sector

Treasury consider the combined and sequential operation of:

- the deferred application of CDR Rules for certain cohorts; and
- the exemption for trial products/plans;

on an individual customer whose CDR experience is that their CDR data is not protected by the full suite of CDR rights and protections. One way this risk might be avoided is to ensure that a small energy retailer cannot offer only trial plans.

Treasury does not accept this recommendation. If an electricity retailer decides to supply a trial plan under the exemption mechanism, it is intended that CDR data in relation to consumers on the plan is not to be shared while the plan is a 'trial product'. This necessarily means potential privacy issues associated with CDR data sharing would not be enlivened in respect of the consumer while they are on the plan.

Treasury notes it would not be possible for an electricity retailer to avoid CDR data sharing obligations by exclusively supplying plans under the exemption mechanism. In all National Electricity Market jurisdictions, a retailer is required to make a standing offer available to customers. The restrictions of the exemption mechanism, including with respect to customer volume and the duration of the trial period, are incompatible with a standing offer.