Australian Government

Consumer Data Right

Privacy Impact Assessment

Operational Enhancements

Agency Response

July 2023

1. Treasury response to Privacy Impact Assessment – operational enhancements to the Consumer Data Right rules

On 11 July 2023 the Assistant Treasurer and Minister for Financial Services, the Hon Stephen Jones MP (the 'Minister') made the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2023*. The rules make operational enhancements to the *Competition and Consumer (Consumer Data Right) Rules 2020* (CDR rules), including a range of adjustments aimed at improving the usability and transparency of the CDR, particularly in relation to CDR business consumers and service providers.

The operational enhancements follow consultation on the exposure draft amendments to the CDR rules and explanatory materials that occurred between 15 September and 14 October 2022. The consultation included a stakeholder forum on the draft rules that occurred on 28 September, bilateral meetings with a range of stakeholders, and careful consideration of the submissions received in relation to the proposed 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, which 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 likely effect of making the rules on privacy or confidentiality of consumers' information must be considered by the Minister 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 as well as the likely regulatory impact of the making of the CDR rules.

Treasury engaged KPMG to conduct a PIA for the proposed operational enhancements to the CDR Rules to ensure the amendments effectively manage privacy risks and to inform the Minister's decision to make the amendments.

The scope of the PIA is limited to the proposed amendments to the CDR rules insofar as they relate to the proposed operational enhancements measures. The PIA was informed by submissions to the exposure draft amendments and was prepared on the basis that it is a living document that supplements the other independent PIAs that have been conducted for the CDR to date, including for the implementation of the CDR to the banking and energy sectors.

The final PIA and public submissions are now available on the Treasury website.

The PIA included twelve recommendations. This document provides an agency response to each of these recommendations.

Recommendation 1 – scope of business consumer consents

Consider a method to encourage ADRs [(accredited data recipients)] to communicate the scope of the business consumer's consent to unaccredited recipients. The way this could occur (e.g. via the Rules or Guidance) would be open for Treasury to consider.
This recommendation will be **referred** to the Data Standards Body (DSB) for the Data Standards Chair's consideration. The CDR rules allow the Data Standards Chair to make standards in relation to the disclosure of CDR data, and it may be appropriate for standards to be made that would require ADRs to give unaccredited recipients the recommended notification.

Recommendation 2 – deletion and de-identification by unaccredited recipients

Consider a method to require unaccredited recipients to delete or de-identify consumer data once there is no longer a purpose to retain it (e.g. pursuant to APP 11).
Treasury **does not accept** this recommendation. Unaccredited recipients are not regulated under the CDR, and the purpose of the business consumer disclosure consent is to allow business consumers to consent to the disclosure of their data to anyone they choose, irrespective of considerations such as whether the recipient is subject to obligations under the *Privacy Act 1988* (the Privacy Act) in relation to that data. Treasury notes that a review of the Privacy Act, including whether it and its enforcement mechanisms remain fit for purpose, is currently underway.

Recommendation 3 – user testing with unaccredited entities

User testing should be undertaken with unaccredited recipients to determine how they will understand the impact of the consent provided by the business consumer against their ability to use the data.
Treasury **does not accept** this recommendation. The consent given by the business consumer to the ADR does not relate to the unaccredited recipient's use of the CDR data. Rather, the consent is given to the ADR by the business consumer to allow the ADR to disclose the business consumer's CDR data to the unaccredited recipient. Once the CDR data has been disclosed to the unaccredited recipient, the CDR legislation does not regulate their use of the data.

Recommendation 4 – user testing and/or use case development with CDR business consumers

User testing and/or use case development [should be] completed with CDR business consumers to ensure that the business consumer consent processes designed by the DSB are fit for purpose and ensure the correct consent(s) are provided. Such testing should consider whether CDR business consumers fully understand what disclosures they are consenting to, and the extent to which they understand that their disclosure will allow CDR data to be shared with an unaccredited third party (who will not be subject to CDR requirements).
This recommendation will be **referred** to the DSB for the Data Standards Chair's consideration.

Recommendation 5 – defining 'business purpose'

Consider defining 'business purpose' in the CDR Rules. This could focus on the types of 'receiving parties' intended to be in scope for these consents, and how the subsequent use of a business consumer's data can be limited for the purpose specified.
Treasury **does not accept** this recommendation. The business consumer measures recognise that businesses are best placed to determine whether they are sharing data for a business purpose, and to whom their data should be disclosed.

Recommendation 6 – administration of business consumer statements

Consider whether additional rules should be imposed on the administration of business consumer statements, such as a requirement to ensure the statements are retained for regulatory oversight. Stakeholder submissions included suggestions to require the statements to include the name of the receiving party, the scope of the consent, and/or any regulatory or professional standard obligations that the receiving party would be expected to comply with. Some stakeholder submissions indicated a preference that the statements be administered online (such as in dashboards) rather than in paper form.
Treasury **notes** this recommendation. New recordkeeping and reporting requirements have been added in relation to the use of these statements. In addition, retaining a record of the statement itself is required under existing paragraph 9.3(2)(a) of the CDR Rules because it itself constitutes part of the business consumer disclosure consent (new paragraph 1.10A(11)(b)). Treasury therefore considers this aspect of the recommendation is addressed. In relation to the suggestions from stakeholder submissions noted in this recommendation: • The name of the receiving party and the scope of the consent are already required to be presented to the CDR business consumer in the CDR receipt (paragraphs 4.18(2)(a) and (ba)). Treasury therefore considers this aspect of the recommendation is addressed. • The business consumer statement is made by the CDR consumer giving a business consumer disclosure consent to the relevant ADR. Treasury does not consider that it would be beneficial to the consumer to be required to provide information about any

regulatory or professional standard obligations that the receiving party would be expected to comply with (noting that the recipient may not be required to comply with any such standards, depending on their relationship with the CDR business consumer).

Note: The purpose of the business consumer statement is to require that CDR consumers who give a business consumer disclosure consent certify that the consent is given for the purpose of enabling the accredited person to provide them with goods or services in their capacity as a business. This, in turn, is to ensure that the CDR consumer is giving the business consumer disclosure consent as a CDR business consumer, and not as an individual CDR consumer.

- The CDR Rules have been amended to allow the Data Standards Chair to make standards about the processes for obtaining and managing business consumer statements. The recommendation will be referred to the DSB for the Data Standards Chair's consideration, including whether standards should be made to require statements to be provided online.

Recommendation 7 – guidance for business consumers on consent durations

Guidance [should be] issued on the available options for business consumers in providing extended consent for the specified purposes and disclosures available under a BCDC, including how and when it would be appropriate for a consent to be extended, and the circumstances that should prompt any extended consent to be reviewed. It would be open to Treasury to determine the most suitable method to issue business consumers with such guidance.
This recommendation will be **referred** to the Australian Competition and Consumer Commission, the Office of the Australian Information Commissioner, and the DSB to consider developing relevant guidance.

Recommendation 8 – trial products

Consider placing limits on the number of trial products, or amending the definition of trial products to prevent or mitigate opportunistic actions of this nature, noting the benefits of the trials and their intended purpose.
Treasury **does not accept** this recommendation given that trial products can only be offered for a maximum of six months, and to no more than 1,000 customers, before losing their status as a 'trial' (meaning the exemption from CDR obligations is no longer available). Treasury considers these settings offer sufficient mitigations against possible misuse of the exemption. The ACCC will publish guidance in relation to trial products, monitor their use and advise Treasury if trial products are being misused. In terms of risk to individual consumers, it would not be possible for consumers to be locked into ongoing trials for the purpose of preventing them from accessing their CDR data. This is because of the six month limitation on how long a product can be considered a 'trial' product.

Recommendation 9 – CDR representative principal's CDR policy

A requirement [should] be added under CDR Rule 7.2 for the CDR principal's CDR policy to contain details about the countries the CDR representative principal's CDR representatives may disclose to when making a disclosure to an unaccredited OSP [(outsourced service provider)].
Treasury **accepts** this recommendation. A provision has been added to the proposed rules to require, if it is practicable to do so, that CDR representative principals' CDR policies specify the countries in which the direct and indirect OSPs of CDR representatives that may be disclosed CDR data are located.

Recommendation 10 – updating guidance

Guidance materials (such as those issued by the OAIC) [should be] updated to support ADRs in understanding their obligations with respect to OSPs, including but not limited to the circumstances where an OSP must cease use of CDR data.
This recommendation will be **referred** to the OAIC to consider updates to existing guidance relating to OSPs and whether further guidance is needed.

Recommendations 11 and 12 – data breaches

Consider whether additional record keeping and reporting obligations, including in relation to notifiable data breaches, should apply to CDR representatives, OSPs and their principals. ADRs [should] require any unaccredited CDR representatives and OSPs to immediately notify the ADR of a data security breach or information security incident involving CDR data.
Treasury **notes** these recommendations. A range of new recordkeeping and reporting obligations have been added to the proposed rules in relation to CDR representatives and OSPs to improve regulatory oversight. Treasury notes that the CDR Rules already require both CDR representatives and OSPs, via their agreements, to comply with Schedule 2 to the CDR Rules (which relates to CDR data security). However, there may be scope to further amend the rules to strengthen notification requirements for OSP and CDR representative arrangements if the current settings are not considered effective, noting that OSP principals and CDR representative principals may independently choose to include these terms in their contracts.