OVIC
Office of the Victorian Information Commissioner

t 1300 00 6842
e enquiries@ovic.vic.gov.au
w ovic.vic.gov.au

PO Box 24274
Melbourne Victoria 3001

Our ref: D20/19120

29 October 2020

CDR Rules Team
Australian Competition and Consumer Commission

By email only: ACCC-CDR@accc.gov.au

Dear CDR Rules Team

Submission in response to Consultation Paper on *CDR rules expansion amendments* – September 2020

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide this submission to the Australian Competition and Consumer Commission (**ACCC**), in relation to its Consultation Paper (**the paper**) on the Consumer Data Right (**CDR**) rules expansion amendments. This submission will also reference the *Update 2 to CDR Privacy Impact Assessment Stakeholder Consultation Document* (October 2020) prepared by Maddocks (**Maddocks PIA**).

As the primary regulator for information privacy in Victoria with administration over the *Privacy and Data Protection Act 2014*, OVIC has followed the progress and implementation of the CDR regime with interest, and welcomes the opportunity to comment on the proposed changes to the CDR Rules.

The key point raised in this submission relates to OVIC's concern that the ever-increasing complexity of the CDR regime, as a result of these and other past or future amendments, will likely have an adverse impact on consumers' ability to exercise meaningful consent, which underpins the CDR legislative framework.

General comments

1. The paper outlines extensive proposed amendments to the CDR Rules, from new tiers of accreditation and new types of consumer consents, to enabling consumers to disclose CDR data and 'insights' to non-accredited persons, amongst others. OVIC recognises that these changes are designed to provide greater flexibility and control to consumers wishing to share CDR data. However, OVIC is concerned that the proposed changes will add further complexity to an already complicated system, not only for consumers, but also for the various entities participating in the CDR regime.

2. The introduction of new information flows, concepts, and types of entities able to collect CDR data (or 'insights') increases the risk that consumers will not be able to fully understand how the CDR system works; for example, who is collecting their CDR data, who is holding it, or to whom it is being disclosed. Without a proper understanding of the various information flows that occur with their data, it is unlikely – if not impossible – that consumers will be able to provide truly informed, and therefore meaningful consent. This is problematic given that consent forms the basis of the CDR framework. While there are legislative requirements under the *Competition and Consumer Act 2010* (Cth) and CDR Rules that are intended to ensure transparency, there is a strong likelihood that consumers will still find it difficult to understand which entities are involved in collecting, using and

disclosing their CDR data, particularly where an entity does not have a direct relationship with the consumer.

3. Similarly, the introduction of additional types of consents raises the risk of further complicating the consent process for consumers. While OVIC supports the intention of the new categories of consent to provide greater and more granular control to consumers, this must be balanced against the potential for consent fatigue and information overload, factors that are of increasing concern to privacy regulators globally.

4. CDR participants are also at risk of finding the expanded rules and their corresponding obligations difficult to navigate, especially where an entity occupies multiple roles within the CDR system. The growing complexity of the CDR regime is particularly problematic in relation to persons accredited to a restricted level. The proposed changes to the accreditation framework assume a high level of maturity in data management within the Australian commercial sector, yet there is little to no evidence that such a level of stewardship currently exists in many companies. Many entities seeking a restricted accreditation may lack the data governance and technical ability to operationalise and effectively comply with the practicalities of the CDR safeguards designed to protect consumers and their data, such as the data minimisation principle.[1]

5. Further, as the Maddocks PIA notes, many are unlikely to have familiarity complying with complex legislative frameworks and information handling obligations.[2] This increases the potential risk that consumers' CDR data is not appropriately protected. To this end, OVIC highlights the need for clear and comprehensive guidance to assist CDR entities in understanding and complying with the relevant obligations of each different role within the system.

Restricted level: affiliate restriction

6. As the ACCC further refines the CDR Rules, OVIC suggests consideration of the manner in which affiliates with multiple sponsors will be able to identify and separate data from a particular sponsor within a larger dataset, where required; for example, for the purposes of deleting or de-identifying CDR data from one sponsor. This likely raises issues of feasibility not only in terms of affiliates' technical ability, but also the costs involved. Most data-rich businesses now use expansive 'data lakes', yet meta-tagging of this data is often patchy and ill-defined, and remediating this issue is rarely undertaken at any scale. As noted in the paper, separating data within a larger dataset may result in significant costs, including costs associated with meta-tagging CDR data upon collection to indicate its source.[3]

7. The paper notes that persons accredited at the affiliate level would be subject to a targeted audit program to be developed by the ACCC and the Office of the Australian Information Commissioner as part of these regulators' general compliance activities. OVIC emphasises the importance of ensuring that such a program is adequately funded in order for it to work effectively. OVIC also queries whether such a program would have sufficient powers, for example in precluding the use of commercial in confidence agreements between parties as a shield from an audit.

CDR data for sale and research purposes

8. The proposed changes permit Accredited Data Recipients (**ADRs**) to seek a consumer's express consent to use their CDR data for the purposes of general research. Where CDR data is used for research purposes, OVIC would support a requirement, as noted in the Maddocks PIA, for ADRs to

---

[1] As raised in a previous OVIC submission to the ACCC in response to the *Consultation paper on facilitating participation of third party service providers in the CDR regime*, 7 February 2020, available at https://ovic.vic.gov.au/privacy/submissions-and-reports/submissions/.
[2] Page 45 of the Maddocks PIA.
[3] Page 45 of the paper.

use de-identified CDR data – noting, however, that de-identification is contextual and has its limitations. Failing to establish (and enforce) appropriate restrictions on what datasets may be combined with other data may lead to de-identification being meaningless.[4]

9. Additionally, if the use of CDR data for research purposes is based on consent, consumers should accordingly be able to withdraw such consent in the future (or, in the context of the CDR, amend their consent to remove the use of their CDR data for research purposes).

10. The proposed changes also enable an ADR to seek a use consent to de-identify some or all of a consumer's CDR data for the purposes of disclosing the data, including by selling it. While the CDR Rules require additional information relating to de-identification to be presented to consumers when seeking their consent (including that the de-identified data will be disclosed, by sale or otherwise, to one or more other persons),[5] it should be clear to the consumer whether their CDR data (albeit de-identified) will in fact be sold. Notwithstanding point 3 above, there may be value to consumers if they were able to expressly consent – or not – to the sale of their de-identified CDR data, given some may be uncomfortable with the sale of such data, but would otherwise agree to its disclosure.

11. Another point to consider is whether consumers will have sufficient information to make an informed decision regarding their consent to de-identify CDR data for the purposes of its disclosure, regardless of by sale or otherwise. In particular, without an awareness of the specific context in which that de-identified data may be combined with other datasets, consumers may have a false sense of comfort regarding the potential risks of this sharing.

Thank you for the opportunity to consult and provide comment on the Consultation Paper and draft CDR Rules. I have no objection to this submission being published by the ACCC without further reference to me.

If you would like to discuss this submission, please do not hesitate to contact me directly or my colleague Tricia Asibal, Senior Policy Officer at [redacted].

Yours sincerely

Sven Bluemmel
Information Commissioner

[4] OVIC has raised its concerns around de-identificaiton in a previous submission to the ACCC, in relation to the exposure draft of the CDR Rules 2019, dated 16 May 2019, available at https://ovic.vic.gov.au/resource/submission-to-the-accc-on-the-exposure-draft-of-the-consumer-data-right-rules-banking/.

[5] Rule 5.15(b).