

16 May 2019

Ms Sarah Court
Commissioner
Australian Competition and Consumer Commission
GPO Box 3131
Canberra ACT 2601

Dear Ms Court,

Exposure draft of the Competition and Consumer (Consumer Data) Rules 2019 for consultation

The Office of the Victorian Information Commissioner (OVIC) is pleased to provide a submission to the Australian Competition and Consumer Commission (ACCC) in response to the exposure draft of the Competition and Consumer (Consumer Data) Rules 2019 for the banking sector (CDR Rules).

OVIC is the primary regulator for information privacy, information security and freedom of information for the state of Victoria. As Information Commissioner, I have a strong interest in matters that may impact Victorian consumers' information privacy and one of my functions under the *Privacy and Data Protection Act 2014* is to make public statements on such matters.¹

OVIC has followed the implementation of the Consumer Data Right (CDR) with interest, previously making submissions to the Commonwealth Treasury in relation to the *Treasury Laws Amendment (Consumer Data Right) Bill 2018 (the CDR Bill)* and to the ACCC in relation to the CDR Rules Framework, late last year. Our submission in relation to the current exposure draft CDR Rules will focus primarily on the privacy safeguards proposed under the rules, particularly, provisions relating to consumer consents, de-identification, information security and oversight of the CDR system.

Consent

A key theme in OVIC's previous submission to the ACCC on the CDR Rules Framework² was consent, raising concerns that the traditional consent model may not be appropriate in the context of the CDR, given the difficulty for consumers to provide fully informed consent for the use of their personal information in a complex transactional environment. In our previous submission to the ACCC, OVIC raised the need to move away from traditional consent models and instead focus on establishing a minimum standard of protection, as a modern approach to consent provisions.

¹ Under s 8C(1)(f) of the *Privacy and Data Protection Act 2014*.

² Available here: <https://ovic.vic.gov.au/wp-content/uploads/2018/10/Submission-to-the-ACCC-on-the-Consumer-Data-Right-Rules-Framework-2018-.pdf>.

It is positive to see that the draft CDR Rules go some way to establishing minimum standards for consumer protection. For example:

- It is positive that Rule 1.8 stipulates that the right of a consumer to withdraw consent to collect or use CDR data or exercise the option to terminate cannot be altered by a CDR contract (as defined under Rule 1.8(1)).
- It is positive to see that the draft CDR Rules account for the withdrawal (or revocation, in accordance with Rule 5.14) of a consumer's consent to collect CDR data, through the concurrent expiry of the authorisation to disclose CDR data (under Rules 4.11 and 4.25(1)(b)). However, implementation of these provisions will rely heavily on effective communication between accredited persons and data holders. Further guidance on these communication channels would be helpful, particularly for consumers at the point of communicating the withdrawal of their consent in writing or via the consumer dashboard. Also, I am concerned that confusion may arise where a consumer has withdrawn consent to collect CDR data (and the authorisation to disclose CDR has expired) and their corresponding consent to use CDR data remains current (under Rule 4.18). More information on the operation of these provisions would be helpful.
- OVIC supports the ongoing notification requirements under Rules 4.14 and 4.20, as a way to ensure transparency and currency of consent.
- It is pleasing to see the inclusion of a 'data minimisation' principle under Rule 1.7 and subsequent obligations under Rule 4.10 (asking CDR consumer to give consent to collect CDR data) and Rule 4.16 (asking CDR consumer to give consent to use CDR data) for accredited persons to consider data minimisation when collecting and using CDR data on the basis of consent.

OVIC queries why 'capacity' is not included as an element of consent under Rules 4.10 and 4.16, in the way that other factors, such as 'voluntary', 'informed', and 'specific', are.³ If 'capacity' is a matter dealt with by way of legislation, it would be helpful to reference the appropriate section of the relevant legislation to provide context for readers, and include it in the list of elements under Rules 4.10 and 4.16, for completeness. In relation to capacity to consent, OVIC's previous submission to the ACCC in relation to the CDR Rules Framework considered consent of mature minors, recommending that minors be excluded from the initial implementation of the CDR.⁴ Whether capacity to consent is already dealt with under legislation or not, the CDR Rules should offer some clarity on whether minors will be excluded from the initial implementation of the CDR.

De-identification

Rule 7.8 requires accredited data recipients to decide whether de-identification or destruction is the most appropriate method for the purposes of clause 56EO(2) of the CDR Bill, having regard to Data61's *De-identification Decision-Making Framework (DDM Framework)*. While de-identification can have many benefits, it is not a panacea for protecting the privacy of personal information for records of specific individuals or transactions. Further, the option to de-identify CDR data for the purposes of Rule 7.8 implies an assumption that de-identification will be successful. The risk of re-identification should be assessed according to the downstream uses for the data and in reality, the re-identification risk relating to external uses of the data can never really be known. As noted in the DDM Framework, "(d)e-identification is an exercise in risk management, rather than an exact science."⁵ The DDM Framework then goes on to say "(t)o de-identify effectively, entities must consider not only the data itself, but also the environment the data

³ 'Capacity' is regarded as a key element of consent. See discussion of consent in OVIC's *Guidelines to the Information Privacy Principles*, available here: <https://ovic.vic.gov.au/book/key-concepts/#Consent>.

⁴ See paragraph 5 of OVIC's submission, available here: <https://ovic.vic.gov.au/wp-content/uploads/2018/10/Submission-to-the-ACCC-on-the-Consumer-Data-Rights-Rules-Framework-2018-.pdf>.

⁵ See page 3 of the foreword of the DDM Framework, available here: <https://publications.csiro.au/rpr/download?pid=csiro:EP173122&dsid=DS3>.

will be released into...(i)n all cases, for data to be considered 'de-identified', the risk of reidentification in the data access environment must be very low" (that is, no reasonable likelihood of de-identification).⁶ Since the risk of re-identification cannot be known when data recipients release data, this threshold is unlikely to be able to be met.⁷ The well documented cases of re-identification of data derived from personal information demonstrate that entities need to be cognisant of, and take into consideration, the risk of re-identification when making decisions under Rule 7.8.⁸

The option to de-identify CDR data also poses the risk of having a large volume of data derived from personal information perceived to be outside the remit of the *Privacy Act 1988* (where an accredited data recipient has determined that the identity of an individual is not reasonably ascertainable from the data). Given the volume of CDR data that will be generated, OVIC is concerned about the potential for data derived from personal information to be perceived to go unregulated under privacy law.

OVIC recommends the ACCC consider inserting a positive obligation under the CDR Rules for accredited data recipients to add metadata when receiving CDR data, indicating the source of the data (which may not be the individual to whom the data refers). Presumably, many if not most of the accredited data recipients would be running data lakes providing a whole of customer viewpoint, and on the assumption that data has been appropriately de-identified, would likely combine data holdings and potentially provide this to third parties. These third parties can engage in re-identification if they wish, using other datasets they hold. As a result, OVIC is concerned that at present, CDR data may not be managed and tracked properly, hindering the ability for consumers to exercise their information rights under the CDR scheme. For example, how would a consumer exercise their rights under privacy safeguard 13 – correction of CDR data, where the data has been integrated into a data lake, without a meta tag and presumed de-identified?

Considering the limitations of de-identification in practice, OVIC recommends that destruction be the preferred option for the purposes of Rule 7.8 and clause 56EO(2) of the CDR Bill, taking into account any record keeping obligations under the CDR Framework or otherwise. OVIC also recommends that accredited data recipients consider engaging subject matter experts before undertaking de-identification activities, such as data scientists and work closely with the Office of the Australian Information Commissioner (OAIC) and Data61 to assess whether de-identification is even a feasible option for the purposes of the CDR data.

Information security

It is positive that the provisions of Schedule 1 of the draft CDR Rules contemplate the changing nature of security threats to some extent. For example, Rules 1.3 – 1.7, outlining the steps accredited data recipients⁹ need to take to comply with privacy safeguard 12, require accredited data recipients to review measures under each step at least annually, or as soon as practicable or in time with emerging threats and vulnerabilities. This goes some way to ensuring the measures under the draft CDR Rules are able to keep pace with technological advancement and changes in the security environment. The capacity for the CDR Rules Framework to respond adequately to changing security threats was a point of discussion at early roundtables hosted by the Treasury that OVIC attended. It is pleasing to see that the draft CDR Rules incorporate stakeholder views and require accredited data recipients to adapt to changing vulnerabilities and threats.

⁶ See page 4 of the foreword to the DDM Framework.

⁷ See page 10 of the DDM Framework, where the authors note "'(d)e-identified' information must carry a very low risk of re-identification having regard to all the circumstances of the particular case."

⁸ Most notably, the re-identification of the MBS/PBS datasets by researchers at Melbourne University, Dr Vanessa Teague, Dr Chris Culhane and Dr Ben Rubinstein. See: <https://pursuit.unimelb.edu.au/articles/the-simple-process-of-re-identifying-patients-in-public-health-records>.

⁹ As well as outsourced service providers or accredited persons, under Rule 1.2.

Given that Victoria is the only jurisdiction in Australia with a legislative data security regime, other jurisdictions and sectors may not have the same security awareness or literacy. Therefore, clear guidance will be necessary to assist accredited data recipients in implementing the minimum standards for privacy safeguard 12. Further, while the OAIC has an essential role to play in auditing practices in accordance with the privacy safeguards under the scheme, the guidance offered in these instances will be reactive. Increased security training and awareness across designated sectors will be crucial to the success of the CDR.

Governance provisions under the draft CDR Rules

It is positive to see that the draft CDR Rules set out an audit role for the OAIC, as raised in our previous submission in relation to the CDR Rules Framework.¹⁰ However, a clear delineation of the OAIC and the ACCC's jurisdiction to audit compliance with the privacy safeguards in practice will be required, given that both bodies have such powers in relation to the privacy safeguards, in different circumstances (under Rules 9.6(1) and (2)). Examples of instances where the ACCC may audit compliance with the privacy safeguards (to the extent they relate to the CDR Rules) could help clarify the jurisdiction between the two bodies, for the purposes of the CDR Rules.


While the reporting requirements to the ACCC and the Australian Information Commissioner under Rule 9.4 are a positive measure to increase oversight of the CDR in practice, it would be helpful for the draft CDR Rules to provide express requirements for executive oversight of compliance with the privacy standards. Similar requirements for senior management oversight of the implementation of security governance in relation to CDR data (under Schedule 1, Step 1.3(1)) could be included under other privacy safeguards. For example, requirements for senior management review and endorsement of policies about the management of CDR data (required under clause 56ED of the CDR Bill and Rule 7.2: Rules related to privacy safeguard 1 – open and transparent management of CDR data) would bolster privacy governance arrangements for CDR entities. OVIC recommends privacy policies be reviewed at least annually and would suggest a similar requirement in relation to Rule 7.2 (where permitted by the enabling legislation).

Given the dissolution of the House of Representatives, clarity on whether there will be another opportunity to comment on the draft CDR Rules, or other elements of the CDR Framework, would be appreciated.

Thank you for the opportunity to comment on the exposure draft of the CDR Rules. OVIC will continue to follow the implementation of the CDR across designated sectors with interest.

I have no objection to this letter being published by the ACCC without further reference to me. I also propose to publish a copy of this letter on OVIC's website but would be happy to adjust timing to allow the ACCC to collate and publish submissions proactively.

If you have any questions concerning the above, please don't hesitate to contact Emily Arians, Senior Policy Officer, at emily.arians@ovic.vic.gov.au.

Yours sincerely, 

Sven Bluemmel
Information Commissioner

¹⁰ See paragraph 8 of OVIC's submission, available here: <https://ovic.vic.gov.au/wp-content/uploads/2018/10/Submission-to-the-ACCC-on-the-Consumer-Data-Right-Rules-Framework-2018-.pdf>.