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: D20/63

7 February 2020

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

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

Dear Ms Court

Consultation paper on facilitating participation of third party service providers in the Consumer Data Right regime

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide the attached submission in response to the Australian Competition and Consumer Commission's (**ACCC**) consultation paper on facilitating the participation of third party service providers in the Consumer Data Right (**CDR**) regime. Thank you for providing an opportunity to consult on this matter.

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

If you have any questions about the attached submission please contact myself or my colleague Tricia Asibal, Senior Policy Officer at tricia.asibal@ovic.vic.gov.au. We look forward to consulting with the ACCC once again following release of the draft rules in March 2020.

Yours sincerely

Sven Bluemmel
Information Commissioner

Office of the Victorian Information Commissioner

Submission to the Australian Competition and Consumer Commission

Introduction

The Office of the Victorian Information Commissioner (**OVIC**) administers two pieces of legislation – the *Freedom of Information Act 1982* (Vic) and the *Privacy and Data Protection Act 2014* (**PDP Act**). This provides OVIC with regulatory oversight of freedom of information, information privacy, and information security for the state of Victoria. In light of this remit, OVIC has a strong interest in matters that impact the information privacy of Victorians. One of the Information Commissioner's functions under the PDP Act is to make public statements on such matters.[1]

The introduction and ongoing development and implementation of the Consumer Data Right (**CDR**) has been of particular interest to OVIC, given its potential implications for the privacy of consumers – including Victorians – participating in the scheme.[2] While OVIC recognises there are benefits to consumers in enabling greater access to and control over their data as intended by the CDR framework, ensuring consumers' privacy is protected is also paramount. Safeguarding the right to privacy is all the more crucial in a data economy where individuals' data is highly valuable, and its misuse has the potential to cause significant harm.

This submission outlines OVIC's views in relation to the questions posed in the Australian Competition and Consumer Commission's (**ACCC**) Consultation paper, *Consultation on how best to facilitate participation of third party service providers* (**the paper**). The submission makes reference to the current proposed CDR rules, released in August 2019 (**CDR rules**).[3] Our comments are organised around key themes we have identified in the paper.

Intermediaries

Accreditation model

The paper notes that 'accommodating intermediaries within the CDR regime will support increased uptake of CDR' and provide flexibility for potential accredited data recipients.[4] OVIC acknowledges that there is a potential role for intermediaries to assist in or facilitate the collection (and possibly use) of CDR data on behalf of accredited data recipients. However, we are of the view that providing for the use of intermediaries within the CDR system should not undermine the existing privacy protections in place for CDR data. Consumers' CDR data should be adequately and consistently protected, regardless of whether it is collected and used by an accredited data recipient or by an intermediary, and irrespective of the model adopted for regulating intermediaries.

---

[1] Section 8C(1) of the PDP Act.

[2] OVIC has previously made submissions to the Australian Competition and Consumer Commission (**ACCC**) in relation to the CDR Rules Framework and the exposure draft of the CDR Rules released in March 2019. These submissions can be found on OVIC's website at https://ovic.vic.gov.au/privacy/submissions-and-reports/submissions/.

[3] Where a specific Rule is referred to in this submission, that Rule refers to the proposed CDR Rules, released in August 2019.

[4] On page 3.

Notwithstanding, should the CDR regime be expanded to accommodate for intermediaries, OVIC would support, in principle, an accreditation model for regulating intermediaries. Requiring intermediaries to become accredited provides assurance to CDR consumers that these entities have met certain criteria as outlined in the proposed CDR rules, and are capable of meeting the obligations required of accredited persons – for example, being a fit and proper person to manage CDR data,[5] or undertaking steps to protect CDR data from misuse, interference, loss, and unauthorised access, modification or disclosure.[6] In turn, this could build consumer trust and acceptance regarding the use of intermediaries. Another benefit of an accreditation model is that the onus would not be on CDR consumers to inform themselves of the trustworthiness of an intermediary, or an intermediary's ability to adequately protect CDR data, as this would form part of the accreditation process.

OVIC also broadly prefers an accreditation model on the basis that under section 6E(1D) of the *Privacy Act 1988* (**Privacy Act**), where a small business operator holds an accreditation under subsection 56CA(1) of the *Competition and Consumer Act 2010* (**CC Act**), the Privacy Act will apply to personal information held by the small business operator that is not CDR data, as if the small business operator were an 'organisation' under the Privacy Act. Under this provision, it would appear that accredited intermediaries that fall within the definition of a small business operator would be obliged to comply with the Australian Privacy Principles (**APPs**) in relation to personal information that is not CDR data, where that intermediary may not otherwise have been subject to the Privacy Act and the APPs. This provides another level of assurance to consumers that any personal information held by an accredited intermediary that is not CDR data will carry the protections provided under the APPs.

Criteria for accreditation

Should an accreditation model for intermediaries be adopted, OVIC supports an accreditation criteria for intermediaries that is the same or similar to that which applies for accreditation at the 'unrestricted' level[7] – that is, an intermediary, if accredited, would be able to comply with the obligations set out in Rule 5.12, or similar. In particular, intermediaries should be able to adequately protect CDR data in order to be accredited, for example by taking the steps outlined in Schedule 2 of the proposed CDR rules which relate to Privacy Safeguard 12.

Given the CDR regime relies on consumers trusting various parties, consumers should be confident that any entity handling their CDR data – whether an accredited data recipient or intermediary – is credible and fit to do so. This is particularly important where consumers have no choice in the use of an intermediary by an accredited person. OVIC therefore supports a criterion for accreditation that requires an intermediary to be a 'fit and proper person', or similar, to manage CDR data.[8]

Under Rules 5.12(b) and (c), an accredited person at the unrestricted level is obliged to have 'internal dispute resolution processes that meet the internal dispute resolution requirements in relation to one or more designated sectors', and be a member of 'a recognised external dispute resolution scheme in relation to CDR consumer complaints'. Depending on the nature of the type of goods and services provided, OVIC acknowledges that some intermediaries may not be able to meet this particular obligation. However, even if the criteria for accrediting intermediaries does not include a similar obligation, the CDR rules should still provide recourse mechanisms for CDR consumers in relation to complaints involving their CDR data, where held by an intermediary.

---

[5] Rule 5.12(2)(a).
[6] Rule 5.12(1)(a).
[7] As set out in Rule 5.5.
[8] Per Rule 1.9.

Use of intermediaries

Given that consent underpins the CDR regime and is the only basis on which an accredited person can collect and use CDR data, it is essential that the consent provided by CDR consumers is meaningful. One element of meaningful consent, as set out in Rule 4.9, is that it is informed. As part of the ability to provide informed consent, CDR consumers should be notified where an accredited person uses or intends to use an intermediary (regardless of whether an accreditation or outsourcing model, or both, is adopted), to ensure the consumer has all the relevant information to make their decision. Being transparent about the use of intermediaries when seeking consent can also enhance consumer trust.

If applicable, notifying consumers of the use or potential use of intermediaries at the time of seeking their consent should be included as a requirement under Rule 4.11. Further, the use of and information about intermediaries should also be included in an accredited person's CDR policy, for example as a requirement under Rule 7.2, similar to the requirement to include information about outsourced service providers (Rule 7.2(4)).

OVIC recognises that the aim of the CDR regime is to provide consumers with greater access to and control over their data. However, without the proper controls and a robust, well-resourced regulatory framework in place, there is a risk of excessive and unchecked data sharing, and proliferation of CDR data, including personal information. Accommodating intermediaries and other third party service providers in the CDR regime has the potential to increase this risk; strong controls are therefore needed to ensure that the sharing of CDR data between entities participating in the scheme, accredited or otherwise, adequately protects consumers' privacy. For example, in OVIC's view –

- the CDR rules should include specific provisions relating to the disposal of CDR data held by intermediaries (and similarly, non-accredited third parties, should the CDR system be expanded to include such entities) – for example, requiring intermediaries to comply with the CDR data deletion process under Rule 1.18, where the CDR data held by an intermediary is no longer required by said intermediary to provide a good or service to an accredited person or data recipient.

  OVIC supports deletion of redundant CDR data (per Rule 7.13) held by intermediaries as the preferred default option, rather than de-identification, in light of concerns previously raised by OVIC in relation to the limitations of de-identification and the risks of re-identification, particularly where the potential downstream and external uses of de-identified data are unknown.[9]

- similar notification requirements as those under Rule 7.4 should apply where an accredited person uses an intermediary to collect or use CDR data on its behalf – for example, the accredited person's consumer dashboard should reflect what and when CDR data was collected, and by what intermediary. Equally, data holders should be obliged to update consumer dashboards to indicate what and when CDR data was disclosed to an intermediary, and identify the intermediary to whom CDR data was disclosed, along with the accredited data recipient.[10]

- intermediaries should be subject to the same governance and oversight mechanisms applicable to CDR participants, as provided for under Rule 9.6; and, where an accreditation model is adopted, the Data Recipient Accreditor should be able to audit intermediaries' compliance with any obligations specified under their accreditation criteria, as well as any conditions imposed on their accreditation, similar to Rule 9.7.

---

[9] See OVIC's *Submission to the ACCC on the Exposure Draft of the Consumer Data Right Rules (Banking)*, 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/.
[10] Per Rule 7.9.

- where an intermediary, on behalf of an accredited person, collects CDR data of the type to which the privacy safeguards under Division 5 of the CC Act apply (i.e. CDR data for which there is one or more CDR consumers), the intermediary should generally be required to comply with the safeguards – noting, however, that certain privacy safeguards may not be as relevant for intermediaries as for other CDR entities. Consideration will therefore need to be given to the interaction between an accredited person or data recipient's obligations under the privacy safeguards, and those of an intermediary's (where one is used, and assuming a particular safeguard applies to that intermediary). For example, if Privacy Safeguard 5 (which relates to notification of the collection of CDR data) applies to both accredited persons and intermediaries, this may result in duplicative efforts and multiple notifications to CDR consumers in relation to the same CDR data.

Data minimisation principle

As OVIC has noted in a previous submission,[11] the data minimisation principle under Rule 1.8, which seeks to limit the amount and scope of CDR data collected and used by accredited persons, is a welcome consumer protection, aligning with established privacy principles around collection minimisation and use limitation, and centring around notions of proportionality and reasonableness.[12] OVIC suggests the ACCC consider whether the data minimisation principle should similarly apply to intermediaries collecting and potentially using CDR data, particularly if, for example, intermediaries are enabled to directly request CDR data from data holders on behalf of accredited persons.

More broadly however, although OVIC supports the data minimisation principle in general, we are also of the view that further consideration and testing is needed to ascertain how this principle will work in practice, and the potential challenges both accredited persons and data holders may face in operationalising this principle. This could include, for instance, testing how – or even whether – data holders' systems will comply with CDR requests for only certain and limited types of CDR data, as requested by an accredited person (or possibly intermediary) in line with the data minimisation principle. Given that the data minimisation principle is intended to be an important privacy protection for consumers, it may be misleading if entities within the system were in fact unable to effectively comply with the practicalities of the principle. For example, if a data holder's system is incapable of appropriately meta-tagging records to indicate their provenance, it is likely the information will remain in the holder's data lake, because lack of adequate metadata may prevent identification and redaction of the relevant records. OVIC raised this concern in a previous submission, and again highlights this issue given the technical ability – and feasibility – of some Australian financial services bodies to implement the data minimisation principle in the context of their existing systems is untested and remains to be seen.[13]

Given that determining what is 'reasonably' required or necessary can be open to interpretation in the absence of detailed guidance, there is a potential risk that accredited persons will collect more CDR data than actually needed, with the legitimate belief that that data is reasonably required or necessary to provide a good or service to a CDR consumer. While the obligation under Rule 4.11(3)(c) for accredited persons to explain how the collection and use of CDR data aligns with the data minimisation principle may help to mitigate this risk, OVIC would welcome additional and more specific guidance around what constitutes 'reasonably' needed or required – particularly within the context of specific sectors – to ensure accredited persons (or intermediaries, if applicable) can effectively and consistently adhere to this data minimisation principle.

---

[11] See OVIC's *Submission to the ACCC on the Exposure Draft of the Consumer Data Right Rules (Banking)*, 16 May 2019.
[12] For example, Information Privacy Principles 1.1 and 2.1 under the PDP Act.
[13] See OVIC's *Submission to the ACCC on the Exposure Draft of the Consumer Data Right Rules (Banking)*, 16 May 2019.

Non-accredited third parties

While OVIC appreciates that allowing consumers to consent to accredited persons disclosing their CDR data to non-accredited third parties may have benefits and offer convenience to consumers, once again this places the onus on the consumer to inform themselves about the trustworthiness and ability of a non-accredited third party to protect and appropriately manage CDR data, where that third party is not subject to the same obligations and oversight as other entities within the CDR system. And, as we have seen, individuals face numerous challenges when left to protect their own privacy – for example, bargaining power imbalances, information asymmetries, long and complex privacy policies, behavioural biases and practical constraints, as highlighted in the ACCC's *Digital Platforms Inquiry Final Report*.[14]

As noted above in relation to intermediaries, further expanding the CDR regime to accommodate for non-accredited third parties, absent appropriate controls and a strong regulatory framework in relation to such entities, raises the potential risk of rampant data sharing. Moreover, as OVIC has previously raised, enabling a system where participating entities are subject to different levels of oversight, as non-accredited third parties would likely be, may render governance provisions under the CDR regulatory framework meaningless.[15] The risk to consumers' privacy is further heightened by current gaps in the coverage of the Privacy Act – for example small business operators, a category under which many non-accredited third parties could potentially fall. OVIC therefore queries how the inclusion of non-accredited third parties in the CDR regime will work in practice, particularly in relation to complaint mechanisms and avenues for consumers to seek redress in respect of their personal information, where non-accredited third parties may not be covered by privacy laws (unless bound by legislation under a provision similar to section 6E(1D) of the Privacy Act, for example). Conversely, if some non-accredited parties did fall within the coverage of the Privacy Act, this would result in inconsistent privacy protections for consumers' personal information across different non-accredited third parties.

In OVIC's view, disclosure of CDR data from accredited persons to non-accredited third parties should not be permitted under the rules unless there are adequate controls to limit the sharing of CDR data between accredited persons and non-accredited third parties, strong restrictions around the latter's use and further disclosure of CDR data, and appropriate oversight mechanisms to audit compliance with any privacy and consumer protections applicable to non-accredited third parties. Further, there should be pathways to allow consumers to make privacy complaints in relation to CDR data held by non-accredited parties that includes their personal information.

Conclusion

In light of the significant amount of consumers' CDR data that will likely be collected, used, and potentially extensively disclosed under the CDR regime (including personal and possibly delicate information) – and, moreover, the intention to expand the CDR regime into other sectors of the economy – it is imperative that strong and adequate protections are in place to safeguard the privacy of CDR consumers and minimise the proliferation of data, including that of Victorians.

Importantly, these protections must be feasible and practical for the diverse range of entities that will or intend to participate in the CDR system, including any third party service providers, should they be provided for under the CDR rules. In OVIC's view, the technical feasibility of some protections currently in place are unclear – for example, the practical application of the data minimisation principle, as outlined above. OVIC therefore suggests and would welcome further testing and consideration in regard to this.

---

[14] Australian Competition and Consumer Commission, *Digital Platforms Inquiry Final Report*, June 2019.
[15] See OVIC's *Submission to the ACCC on the Consumer Data Right Rules Framework*, 12 October 2018, available at https://ovic.vic.gov.au/resource/submission-to-the-australian-competition-consumer-commission-on-the-consumer-data-right-rules-framework/.

Finally, as the CDR regime will impact consumers' privacy, it is essential that they have a meaningful pathway for redress in relation to CDR data that includes their personal information. To this end, however, OVIC believes Australia's privacy regime is inadequate as far as unaccredited parties in the CDR system are concerned, given the gaps in the coverage of Australia's privacy legislation.