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: D20/9578

27 July 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 CDR Rules Consultation: *Draft rules that allow for accredited collecting third parties ('intermediaries')*

The Office of the Victorian Information Commissioner (**OVIC**) is pleased to provide a submission in response to the Australian Competition and Consumer Commission's (**ACCC**) consultation on the draft Consumer Data Right (**CDR**) Rules (**Rules**), allowing for accredited collecting parties ('intermediaries') to collect CDR data on behalf of, and provide goods and services to, other accredited parties.

As the primary regulator for information privacy, information security, and freedom of information in Victoria, OVIC continues to take a great interest in the ongoing development and implementation of the CDR regime, and its impact on CDR consumers' privacy. Ensuring that strong privacy protections for CDR consumers are in place will aid the success of the CDR regime, and OVIC welcomes the opportunity to contribute to this discussion and provide feedback on the draft Rules.

This submission will draw on key points raised in OVIC's previous submission to the ACCC in relation to its December 2019 consultation paper on facilitating the participation of third party service providers in the CDR regime (**previous submission**).[1] It also refers to the draft privacy impact assessment update prepared by Maddocks (**PIA Update**), published for consultation concurrently with the draft Rules.

Facilitation of third parties in CDR regime

OVIC welcomes the approach proposed under Rule 1.10A of Combined accredited person (**CAP**) arrangements, in which a third party (**provider**) collecting CDR on behalf of, or using and disclosing CDR data to provide a good or service to, an accredited person (**principal**) must also be accredited themselves. Having providers that are accredited gives assurance to CDR consumers that the third party has met certain criteria that demonstrates they are an appropriate person to collect, handle and use CDR data, and are able to adequately protect it in accordance with the requirements outlined in Schedule 2 of the CDR Rules.

OVIC also supports the provider and principal under a CAP arrangement both being accredited to the unrestricted level (as outlined under Rule 5.5). Again, this provides assurance to consumers that both parties have met the same criteria required at this level, and are equally fit and capable of handling and protecting CDR data. Should different levels of accreditation be introduced in the future, OVIC would

[1] See OVIC submission dated 7 February 2020, available at https://ovic.vic.gov.au/privacy/submissions-and-reports/submissions/.

support requiring both parties to a CAP arrangement being accredited to the same level, to ensure that CDR data is offered the same level of protection whether handled by a provider or principal.

Another welcome amendment in relation to CAP arrangements are the notification requirements and transparency measures in relation to the use of providers under such arrangements – for example, providing information to CDR consumers, where applicable, about the use or potential use of providers at the time of seeking their consent (as per Rule 4.11(3)(i)); and requiring an accredited person to include a list in their CDR policy of other accredited persons with whom it has a CAP arrangement, along with certain information about those other accredited persons and the arrangement (per Rule 7.2(4)). Such transparency around the use of providers under a CAP arrangement is essential to enable the CDR consumer to make an informed decision about their CDR data, and may help enhance consumer trust.

Further privacy protections for consumers and CDR data subject to CAP arrangements

While the current draft Rules provide a good starting point for facilitating the use of third party providers in the CDR regime, OVIC considers that further privacy protections in relation to the use of such providers can and should be included in the Rules.

Mandatory provisions in CAP arrangements

The draft Rules outline what a CAP arrangement involves, and its general effect, but does not prescribe the form or content of a CAP arrangement. While both parties are accredited in their own right and therefore subject to a range of obligations, OVIC agrees that as noted in the PIA Update, including mandatory provisions in CAP arrangements that clarify the role of each party in discharging certain obligations would benefit both parties to the arrangement, as well as provide greater protections to consumers.

For instance, the PIA Update gives the example of including a requirement for CAP arrangements to contain a mutual obligation for the principal and provider to notify each other if a CDR consumer withdraws their consent or authorisation, so that the other party does not continue to use or disclose that consumer's CDR data without an appropriate consent or authorisation.[2] OVIC would support such a requirement, as well as another obligation under the Rules for a previously-accredited party to a CAP arrangement to notify the other party in the event that it is no longer accredited, and for either party to notify the consumer of the fact (and other measures per Recommendation 26 in the PIA Update).[3]

In addition to the CDR Rules containing mandatory provisions in CAP arrangements, OVIC would welcome additional detailed guidance around what should be included in such arrangements.

Transparency and notification obligations

The draft Rules add another requirement to Rule 7.4 for accredited persons to update the relevant consumer dashboard to indicate, where applicable and amongst other information, the fact that a consumer's CDR data was collected by an accredited person (i.e. provider) on behalf of the accredited person (i.e. principal) under a CAP arrangement. OVIC considers that Rule 7.4 could be further bolstered, to the benefit of the consumer, by requiring the principal to specify in the consumer dashboard which provider collected the consumer's CDR data.

Similarly, Rule 7.9 requires data holders to update each relevant consumer dashboard to indicate, where applicable and amongst other information, the fact that CDR data was disclosed to an accredited person (i.e. provider) on behalf of an accredited data recipient under a CAP arrangement. Again, more granular information such as the name of the provider to whom CDR data was disclosed would be beneficial for consumers, allowing them to know exactly who is collecting their CDR data.

[2] Page 14 of the PIA Update.
[3] Page 34 of the PIA Update.

Information security controls under Schedule 2

The PIA Update identifies a potential privacy risk where information about a CDR consumer that is not considered CDR data – for example, details about the consumer's consent, or their contact information – may not be secure as the protections of the CDR Rules do not apply to such data. OVIC understands that non-CDR data communicated between parties to a CAP arrangement would be offered some protection under the Australian Privacy Principles.[4] However, OVIC is of the view that applying the additional control of encryption in transit (as proposed under Schedule 2 of the draft Rules) to non-CDR data communicated between parties to a CAP arrangement, would be beneficial to appropriately ensure the privacy and security of such data. OVIC also considers that all data should ideally also be encrypted when at rest. Encrypting non-CDR data may mitigate the potential risk of it being harvested by intermediaries or malicious actors within the system, or being used to infer relationships between parties. OVIC would therefore support all data within the CDR system – be it CDR data or non-CDR data – being encrypted, both when at rest and in transit, by default.

OVIC also supports the proposed data segregation control similarly applying to non-CDR data. This would further enhance the privacy protection provided to non-CDR data – for example, by limiting the dissemination of that information, and by limiting the exposure of non-CDR data in the event of a breach.

Data holders

When seeking authorisation from a CDR consumer for the disclosure of their CDR data, Rule 4.23 requires data holders to provide certain information to the consumer, such as the name of the accredited person that made the consumer data request. Where an accredited person is acting in the role of a provider and has made a request to a data holder in that capacity, OVIC suggests that the data holder should be required to give to the CDR consumer the names of both the provider, and the principal on whose behalf the provider has made the request. This will necessarily require the data holder to know, where relevant, whether an accredited person is acting as a principal or provider.

OVIC also welcomes the suggestion on page 11 of the PIA Update (Recommendation 11) that data holders be required to check the accreditation of both the provider and principal, to ensure that CDR data is not disclosed to an entity whose accreditation has been surrendered, suspended, or revoked – particularly given a collection of CDR data by a provider is taken to be a collection by the principal, per the draft Rules.

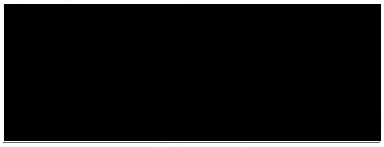
Further to this point, there would be value in clarifying in the Rules and CDR guidance how Rule 5.23(4) applies in the context of a CAP arrangement, where one party to the arrangement has their accreditation surrendered or revoked. For example, the obligations of the principal or provider to delete or de-identify CDR data subject to a CAP arrangement, where the other party's accreditation has been suspended or revoked. Where it is the principal whose accreditation has been surrendered or revoked, OVIC would support a default requirement for a provider who has collected and held CDR data on behalf of that principal, to also delete or de-identify that CDR data.

Thank you for the opportunity to consult and provide comment on the draft CDR Rules. I have no objection to this submission being published by the ACCC without further reference to me. I also propose to publish a copy of this 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.

[4] As accredited data recipients that are APP entities would need to comply with the APPs in relation to such non-CDR data, and given section 79 in the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth) applies the Privacy Act to small business operators, upon accreditation, as if they were an organisation under the Privacy Act and therefore also obliged to comply with the APPs in relation to personal information that is not CDR data – per page 17 of the PIA Update.

If you would like to discuss this submission, please do not hesitate to contact me directly or my colleague [redacted]

Yours sincerely



Sven Bluemmel
Information Commissioner