Consumer Policy Research Centre

Level 14, 10-16 Queen Street, Melbourne, Victoria 3000

ABN 23 100 188 752 T 03 9639 7600 W cprc.org.au

10th May 2019

ACCC Consultation Hub
Australian Competition and Consumer Commission

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

Dear Secretariat,

Re: ACCC Consumer Data Right Draft Rules (Banking) Consultation

Consumer Policy Research Centre (CPRC) would like to thank you for the opportunity to respond to the ACCC Consumer Data Right Draft Rules (Banking) Consultation (Draft Rules).

CPRC is an independent consumer research organisation which undertakes research to inform policy reform and business practice change. Our goal is to achieve a fair outcome for all consumers. We conduct research across a range of consumer markets, with a focus on consumer decision-making, housing, consumer data and the online marketplace. We work collaboratively with academia, industry, government and the community sector.

CPRC strongly supports reform of the data protection, management and portability framework in Australia to provide consumers greater control of their own data and personal information. We also continue to highlight the benefit and need for the implementation of an economy-wide data protection and management framework in Australia alongside the introduction of the CDR. This economy-wide data protection reform is an approach that many jurisdictions internationally have taken to ensure that consumers are sufficiently protected and provided with agency in the new digital age. Implementing economy-wide protections in Australia would ensure that the reforms to open up data would occur within a protected environment. A modern an integrated data policy framework would provide a better base from which to consider the optimal set of CDR rules for the banking sector.

CPRC strongly supports many elements of the rules, including:

- The use of the data minimisation principle to guide CDR data requests,
- The definition of prohibited use or disclosure of CDR data including selling data and disclosing data to anyone other than an outsourced data provider,
- The requirement for accredited persons to provide the consumer information on the specific use or uses of the CDR data for which the CDR consumer has given their consent,

- The requirement for consent to be voluntary, express, informed, specific as to purpose, time limited and easily withdrawn,
- The requirement for accredited persons to notify CDR consumers every 90 days that the consent is still current, and
- The exclusion of data relating to consumers under the age of 18 from the definition of CDR data.

We have some additional comments and questions around certain elements of the rules including enforcement and reporting, consumer access and control, and definitions.

Data minimisation principle

We note the requirement that the collection of CDR data should reflect the data minimisation principle. CPRC strongly supports the use of this principle as a guide to identifying the which information is required to provide the goods or services in a CDR contract.

However, the enforcement of this provision appears unclear. The audit clauses (Subdivision 9.3.2) and the reporting requirements (Subdivision 9.3.1) do not appear to request information on compliance with the data minimisation principle. Inclusion of a reporting requirement, or another lever to encourage compliance with this principle would be beneficial.

Reporting requirements

CPRC supports the reporting requirements outlined in the rules (Subdivision 9.3.1). Information on complaint data and the volume of requests will be key to assessing the development of the data portability market in the banking sector. We note that reporting requirements do not include the types of complaints or the type of use cases.

Monitoring not only the volume and source of complaints, but also the type or subject would allow the regulator a greater understanding of market operations and development. For example, if 90 percent of complaints were about the same topic, then a problem in the marketplace or regulatory framework would be more easily and quickly identified. This can be achieved with minimal additional burden for the organisations reporting.

In addition, reporting types of use cases reflected in the requests would also provide valuable additional market information. Efficient and relevant regulatory processes require up-to-date market information. Monitoring the types of use cases supported by the CDR would assist regulators in evaluating the functionality and ongoing relevance of the CDR regulatory framework.

Withdrawal of consent

The rules outline the processes for consumer to withdraw consent for access to their data. CPRC supports the rules' requirement that withdrawal functionality must be simple and straightforward to use, no more complicated a process that authorisation, and be clearly visibly displayed (cl. 1.14 (4)).

As this stage of the report drafting, the responsibilities of the accredited person after the withdrawal of consent are unclear. The treatment of the data after withdrawal of consent is a key concern for CPRC, particularly around the deletion or de-identification of data not legally required to be stored. We await further drafts of the rules to address this issue.

Joint accounts

CPRC supports the inclusion of draft rules to define the treatment of joint accounts in the CDR banking regime. We would propose that Part 3, Division 3.1 of the Draft Rules, could be edited to clarify that both parties to the joint account would need to elect to allow each joint account holder to individually make consumer data requests, authorise to disclose CDR data, and revoke those authorisations. The current drafting may lead to confusion as to whether both joint parties need to consent, or only one of the account holders. We strongly recommend against the rules enabling either joint account party to unilaterally enable data to be transferred to an accredited entity.

Consumer Dashboard

We continue to recommend policymakers and regulators consider the development of a central dashboard or portal to enable consumers to access information about their consumer data. While this may not be practical in the first stage, if the CDR is to as planned, be rolled out to other sectors it is impractical to think that consumers will be likely to go into each and every data holder entity to actively manage these activities.

Consent

It is unclear why the consent rules at Division 4.2 for the consent to collect (4.3.1(a)) and use (4.3.1(b)) of CDR data uses the terminology that an accredited entity that enters into a CDR contract with a consumer 'may' ask the consumer to give their consent to the accredited person. This seems an unnecessarily vague introduction to the rules given it is an intended requirement, we suggest strengthening this to 'must'.

We also note that there is no requirement to notify the consumer of any risks associated with the transfer of their CDR data, nor their rights to require deletion of that information. This we believe, will likely undermine consumer trust in the CDR system if this only becomes apparent to consumers at a later point once difficulties are encountered and may well be misleading.

We continue to recommend that consumers gain a right to delete their data if they are no longer comfortable with an accredited person holding it. In the absence of policy & regulation to provide such a protection, at a minimum, consumers should explicitly be informed that they no longer have a right to request that the data be deleted at a later stage, only a right to withdraw any ongoing use.

De-identification

We continue to recommend that data be destroyed upon a use case being spent, or a consumer withdrawing consent. Data experts have consistently highlighted the risks and ineffectual nature of de-identification processes as more data and personal information is exchanged across the economy. Banking data is extremely sensitive and detailed information about an individual. De-identified data can easily be reidentified by matching this with other datasets, which we know is a common practice around the world and particularly opaque within the Australian economy due to ongoing incredibly weak privacy and data protection regulation. This is also consistent with consumer expectations identified in Tobias research conducted by Data61 which found that 54% of consumer expected that their data would be deleted if their consent was revoked. Without such a capacity, we believe consumers may end up distrusting the CDR system and this may undermine the reform.

Accreditation

To ensure the rules enable transparency, we strongly recommend that the ACCC require the application to become an accredited person include specification of what uses the data will be used for. We do not believe that the general description in 5.2(d) is sufficient to ensure that regulators can adequately monitor what data use cases are being put to consumers by accredited entities as part of the consent standard, when compared with what their accreditation enables.

This would also better align the terminology and language used in both the rules and the standards when it comes to what use cases consumers are being asked to consent to by accredited entities. Furthermore, if use cases are required to be specified through the accreditation process this can then be tied to the use case definitions within the consent standards.

Not only will this enable a more transparent process for monitoring and enforcement, it will also enable policymakers to ascertain what the major use cases have been for consumers accessing and using the Consumer Data Right. This is critical in terms of being able to estimate the benefits of this reform. If regulators and policymakers are not clear about what the majority of use cases are.

Outsourced service provider

An 'outsourced service provider' is defined in cl.4.8(3) as an entity that has entered into a contract with the accredited data recipient for the provision of goods and services, and that contract includes a requirement for the outsourced service provider to give the data the security protections outlined in Schedule 1.

It is unclear as to whether the outsourced service provider is subject to the other data protections outlined in the Draft Rules. Division 7.2 would suggest that outsourced service providers are not subject to the same obligations in terms of data privacy. The specific obligations of outsourced service providers, and related exemptions, could be made more explicit in the Draft Rules. It is unclear why an outsourced service provider would have different obligations in the treatment of the CDR data compared to the accredited entity.

We would welcome any opportunities for further discussions during the consultation process.

If you have any questions or would like further information regarding this submission, please don't hesitate to contact Senior Research & Policy Officer, Brigid Richmond on 03 9639 7600 or brigid.richmond@cprc.org.au.

Yours sincerely,

Lauren Solomon
Chief Executive Officer
Consumer Policy Research Centre