Australian Government

Consumer Data Right

CDR Rules Consultation

Draft rules that allow for accredited collecting third parties ('intermediaries')

22 June 2020

Table of Contents

CDR Rules Consultation 0
1. Background to this consultation 2
2. Overview of the consultation process: submissions and a workshop 2
3. Publication of submissions 2
4. The Combined accredited person (**CAP**) arrangement 3
    Who is a principal? 3
    Who is a provider? 3
    What can a provider do with CDR data? 3
    Where will consumers be able to find additional detail about providers? 4
    What new records will need to be kept? 4
    What liability structure applies? 4
    Does a provider have to collect CDR data? 5
5. Minimum information security controls 5

1. Background to this consultation

In December 2019, the ACCC consulted on how best to facilitate the participation of third party providers that collect CDR data on behalf of accredited persons (often referred to as 'intermediaries') in the Consumer Data Right (**CDR**) regime. Submissions in response to the consultation supported both an outsourcing and accreditation model for these collecting parties.

In light of that consultation process, these proposed rules authorise third parties who are accredited at the "unrestricted" level to collect CDR data on behalf of another person accredited to that level. This will allow accredited persons to rely on other accredited persons in the CDR ecosystem to collect CDR data, and to provide other services, that facilitate the provision of goods and services to consumers.

In considering the expansion of the outsourcing rules, some legal uncertainty has been identified about the scope of the ACCC's rule-making powers. We are engaging with Treasury to resolve this, and will explore this further once these issues have been resolved.

2. Overview of the consultation process: submissions and a workshop

The ACCC is seeking views from stakeholders on whether the proposed draft rules operate optimally and as intended, and interested parties have until **Monday, 20 July 2020** to provide submissions in response to this consultation. Submissions will inform amendments to the *Competition and Consumer (Consumer Data Right) Rules 2020* (Rules).

Submissions received will also inform an update to the Privacy Impact Assessment for the CDR regime, and a draft update to the Privacy Impact Assessment is being consulted on concurrently with these draft rules.

Submissions and comments to this consultation and the draft Privacy Impact Assessment should be provided by email to: ACCC-CDR@accc.gov.au, attention: **CDR Rules Team**.

The ACCC is conscious of the high level of interest in this topic and that stakeholders may have queries and views that they wish to share with us directly. Given the range of issues that may be of interest, from a policy and technical perspective, the ACCC, together with the Data Standards Body, intends to host a workshop style discussion with interested stakeholders during the consultation period. Once details are finalised, further information on the attendance and timing of this discussion will be provided in an upcoming newsletter.

3. Publication of submissions

To foster an informed and consultative process, all submissions will be considered as public submissions and will be posted on the ACCC's website.

If interested parties wish to submit commercial-in-confidence material, they should submit both a public version and a commercial-in-confidence version of their submission. Any commercial-in-confidence material should be clearly identified, and the public version of the submissions should identify where commercial-in-confidence material has been removed. Parties will be required to provide reasons in support of any claims of

confidentiality. Further information on the process parties should follow when submitting confidential information to the ACCC can be found in the ACCC/AER Information Policy which sets out our general policy on the collection, use and disclosure of information. A copy of the policy is available on the ACCC's website.

4. The Combined accredited person (**CAP**) arrangement

The draft rules allow a customer-facing accredited data recipient (the **principal**) to engage the services of another accredited person (the **provider**) under a "combined accredited person" (**CAP**) arrangement. This arrangement enables a provider to collect and/or use and disclose CDR data to provide services to the principal in order for the principal to provide the requested goods or services to a consumer.

Who is a principal?

A principal is a consumer-facing person accredited to the "unrestricted" level who a CDR consumer requests goods or services from and, as such, will be the person with whom the CDR consumer has contracted with for those services. The principal will engage the services of a provider for the purpose of providing the goods or services to the CDR consumer.

A principal may use multiple providers, and may have both CAP and outsourcing arrangments in place, in order to provide its goods or services to consumers.

Who is a provider?

A provider is a person accredited to the "unrestricted" level that assists a principal to provide goods or services to consumers. This may include collecting CDR data from data holders on behalf of the principal. A provider may also use and disclose CDR data to provide other services to the principal in the same way that services may be provided under an outsourcing arrangement

Under a CAP arrangement, a provider may engage directly with the consumer. For example, under a CAP arrangement, the provider may be the party responsible for delivering the dashboard to the consumer or it may be providing the app. However, the principal and its branded goods and services will always be the consumer-facing entity with whom the CDR consumer has a contractual relationship. A provider can only provide services to the CDR consumer on behalf of the principal.

An accredited person may have both CDR outsourcing arrangments and CAP arrangments with other accredited persons. This provides parties with flexibility regarding how to structure their arrangements and apportion their liablity contractually, see: 'What liability structure applies?' for further information.

What can a provider do with CDR data?

A provider is only permitted to collect, use and/or disclose CDR data where a principal would otherwise be authorised to perform these actions. The authority to do these actions is governed both by Privacy Safeguard 6 and the consent given by a consumer.

The approach to redundant data and a consumer's right to elect how it is treated remains consistent with the current rules. Where a consumer elects for their redundant data to be deleted, that election will apply as under the current Rules. A provider must treat the data in accordance with the principal's general policy. If the circumstances exist where a decision needs to be made by the accredited data recipient about the treatment of redundant data upon redundancy, that decision will be made by the principal.

What transparency mechanisms are in place about the use of providers for consumers?

Consumers are informed during the consent process if a provider may collect or be disclosed their CDR data, and must be shown the provider's name and accreditation number.

Consumers will also see on their consumer dashboard with the accredited person that collection has been facilitated by a provider (Privacy Safeguard 5).

Similarly, a data holder's dashboard will ultimately display whether CDR data was disclosed to a provider on behalf of a principal (Privacy Safeguard 10). To the extent the proposed additions to the data holder dashboard require technical changes, commencement will be deferred to a date to be fixed but no earlier than February 2021.

Where will consumers be able to find additional detail about providers?

Providers, as accredited persons, will also be required to have their own policy about the management of CDR data (Privacy Safeguard 1 policy).

Principals will also need to include information about their use of providers in their own Privacy Safeguard 1 policies, including information about the nature of the services a provider provides to the principal.

What new records will need to be kept?

Accredited data recipients that engage providers will need to keep and maintain records that record and explain their CAP arrangements, including a copy of all relevant CAP arrangements, for a period of 6 years.

What liability structure applies?

The principal who is providing the services and goods to the CDR consumer remains liable at all times. The principal also remains liable for the acts and omissions of the provider whether or not the provider is acting within or outside of the scope of the CAP arrangement. This mirrors how liability applies under outsourcing arrangements.

However, differently to outsourcing arrangements, and recognising that both the provider and principal are accredited persons, by entering into a CAP arrangement both the provider and the principal accept responsibility for the obligations imposed on accredited persons under the rules in relation to CDR data. Under their contractual arrangements they may decide which of them will discharge those obligations.

For example, rule 4.18(1)(a) imposes an obligation on an accredited person to give the CDR consumer a CDR receipt after the consumer consents to the accredited person collecting and using CDR data in accordance with Division 4.4. The consent is in relation to particular CDR data. If that CDR data is subject to a CAP arrangement, both the principal and the provider are separately responsible for providing a CDR receipt. However, if one of them provides the CDR receipt, the other one is not also required to do so. If under the CAP arrangement the provider is responsible for providing the receipt and does so, it will have met the obligation as will have the principal; however, if the provider fails to provide the receipt, as an accredited person it will be liable under the rules for a breach of the obligation, and any breach by the provider will be taken to be a breach by the principal.

Both the provider and the principal remain separately responsible for meeting their general obligations as accredited persons, for example to meet the requirements of an accredited person at the "unrestricted" level.

Does a provider have to collect CDR data?

No. A CAP arrangement can be used so that another accredited person collects CDR data on an accredited person's behalf, however, the rules are not confined to collection, and the CAP arrangement may cover other services. For example, the provider could deliver the consumer dashboard, or analysis of the data on behalf of the principal.

5. Minimum information security controls

What changes are being proposed?

Aside from the CAP arrangement, we are also seeking views on the proposed additions to the information security controls in Schedule 2 of the rules.

The proposed minimum controls cover encryption in transit and data segregation, and will apply to accredited persons as well as outsourced service providers. The controls are intended to align with industry best practice.