Australian Government

Consumer Data Right

ACCC CDR Compliance Review of CDR Representative Principals

ACCC Observations

May 2024

1. Introduction and overview

The Australian Competition and Consumer Commission (**ACCC**) is an independent Commonwealth statutory agency that administers and enforces the *Competition and Consumer Act 2010* (**Act**) and other legislation, promoting competition, fair trading, protection of consumers' rights and product safety for the benefit of consumers, businesses, and the Australian community.

The Consumer Data Right (**CDR**) allows consumers to safely share the data that businesses hold about them, helps consumers compare products and services to find offers that best match their needs, and encourages competition between providers, leading to more innovative products and services.

The ACCC's CDR roles include monitoring compliance with Part IVD of the Act, the *Competition and Consumer (Consumer Data Right) Rules 2020* (**CDR Rules**), the Consumer Data Standards (**Standards**), and taking enforcement action where appropriate. The ACCC's other CDR roles include accrediting potential data recipients, establishing and maintaining a Register of accredited persons and data holders, assessing applications for exemption from CDR obligations, and providing guidance to stakeholders about their obligations under the CDR.

This report contains observations from a targeted compliance review of selected CDR representative principals' approach to CDR obligations. The report provides information about compliance with obligations, and transparency about the ACCC's compliance activities.

The ACCC recognises that the introduction of the CDR representative model has encouraged new participants to enter the CDR, and has been a significant driver of the uptake of the CDR. However, ongoing compliance with the CDR Rules is fundamental to maintaining high levels of trust and confidence in the CDR.

The information in this document is of a general nature only and does not constitute legal or other professional advice. We recommend that parties obtain their own independent advice in relation to their compliance.

2. Background to the review

In May 2023, the ACCC commenced a targeted compliance review of a selection of CDR representative principals.

As part of this review, we analysed records provided by the selected CDR representative principals. For each CDR representative principal, we requested 5 specific types of records that CDR representative principals must keep and maintain under rule 9.3(2A).

Objective and scope

The CDR representative model has grown substantially since being introduced in October 2021.

As part of our targeted compliance review, we requested documents to help us understand how CDR representative principals are, in practice, fulfilling their oversight obligations. We also sought to gain further insight into how the CDR representative model is functioning more generally, identify any present or emerging risks, and address any potential compliance concerns.

The outcomes of our targeted compliance review informed guidance published in December 2023 on the CDR representative model, and will help determine whether further guidance or amendments to the CDR Rules would support the CDR in achieving its objectives.

Methodology

In June 2023, we requested that each of the CDR representative principals selected for our review provide records in relation to their arrangements with one of their CDR representatives. These records pertained to the:

1. CDR representative arrangement,
2. management of CDR data by the CDR representative,
3. steps taken by each CDR representative principal to ensure their CDR representative complies with the arrangement's requirements,
4. use of CDR data by the CDR representative, and
5. process used by the CDR representative to ask for consumers' consent.

We examined the records against the provisions of the CDR Rules in force at the time of our request. Unless otherwise stated, all references to the CDR Rules in these observations refer to these rules, being Compilation 7 of the *Competition and Consumer (Consumer Data Right) Rules 2020*, that were in force from 1 February 2022 to 21 July 2023.

Our review commenced before the *Competition and Consumer (Consumer Data Right) Amendment Rules (No. 1) 2023* came into effect on 22 July 2023. CDR representative principals should consider these amendments in assessing their obligations.

3. Outcomes from the review

Our observations in relation to each category of the records we reviewed are outlined are set out below.

3.1. CDR representative arrangement

Rule 1.10AA of the CDR Rules sets out the terms a written contract must contain in order to be a CDR representative arrangement. This includes terms which require the CDR representative to comply with various privacy safeguards as if it were the CDR representative principal in holding, using, or disclosing service data, and to adopt and comply with the CDR representative principal's CDR policy in relation to the service data.

As part of the review, we observed the written contracts examined generally applied rule 1.10AA. However, we observed some instances of drafting that could have been more precise. For example, as noted in our guidance, the CDR Rules require a CDR representative arrangement to impose obligations on the CDR representative to comply with certain components of the CDR framework as if it were the CDR representative principal or accredited data recipient. The CDR Rules also require that the arrangement specify that certain provisions do not operate unless the details of the representative have been entered on the Register of Accredited persons.

3.2. Management of CDR data

Schedule 2 of the CDR Rules specifies the steps a CDR representative must take to protect CDR data as if it were a CDR representative principal. For example, it provides that CDR

representatives must define and implement security governance in relation to CDR data, define the boundaries of the CDR environment, and maintain appropriate information security capability.

As part of the review, we observed that the contracts between the selected CDR representative principals and their CDR representatives generally specified how parties should demonstrate they meet the requirements of Schedule 2. Measures we observed in the contracts included requirements that were imposed requiring the engagement of independent third parties to test security controls.

However, we also observed some variation in approach across the records, including some principals taking a 'risk-based' approach. We acknowledge that CDR representative use cases may pose differing risks of consumer harm. For example, a CDR representative arrangement made for the purpose of allowing a data holder to test their own systems may carry a lower risk than a use case that is specifically directed at consumers. However, we note that CDR representative principals must ensure that their representatives meet all Schedule 2 requirements regardless of their use case.

3.3. Steps taken to ensure compliance with the requirements of the CDR representative arrangement

A CDR representative principal must ensure its CDR representative complies with the requirements of the CDR representative arrangement. A CDR representative principal should implement procedures and practices that are appropriate to the scale, complexity and nature of the relevant obligation to decrease the risk of non-compliance with the arrangement. Our guidance provides detailed examples.

As part of the review, we observed that, in most cases, there were measures in place to address this obligation. In some cases however, we observed a reliance on measures such as:

- self-assessments and attestations. For example, a CDR representative providing a declaration that it is compliant, without additional evidence or oversight by the CDR representative principal as to whether that is the case.
- initial compliance checks or ad hoc checks, rather than proactive and ongoing monitoring throughout the term of an arrangement that would promptly identify whether a CDR representative may be non-compliant with the arrangement.

Such measures may not be sufficient for a CDR representative principal to ensure a CDR representative complies with the terms of a CDR representative arrangement.

3.4. Use of CDR data

As of 22 July 2023, a CDR representative must abide by the data minimisation principle specified in rule 1.8 of the CDR Rules. For example, it must not collect more CDR data than is required to deliver its goods or services. A CDR representative principal is also required to state how it will use data during its consent process, and outline this in its CDR policy.

Given the version of the CDR Rules assessed, the data minimisation principle was not specifically considered as part of our review. However, as noted in our guidance, a CDR representative principal should screen, test and monitor its CDR representatives' compliance with the data minimisation principle on an ongoing basis, and ensure that it has adequate records of their compliance with consent processes.

3.5. Consent processes

The CDR Rules and Standards impose requirements on CDR consent processes. These requirements allow consumers to provide fully informed consent, while having a consistent consumer experience. Strong consent processes are central to the design and success of the CDR.

CDR Rules

As part of the review, we considered representative consent processes, noting that all CDR representatives should ensure their consent processes:

- expressly state that the person seeking consent is a CDR representative, and that the CDR data will be collected by the CDR representative principal,
- allow the CDR consumer to actively select or otherwise clearly indicate the type of data subject to the consent and the duration of the consent, and
- provide sufficient information about withdrawing a consent, including:
  - explicitly stating the consumer may withdraw consent at any time,
  - indicating where a consumer may withdraw consent, and
  - stating the consequences (if any) of withdrawing consent.

Consumer Experience Guidelines

As part of the review, we provided feedback and recommendations to CDR representative principals on how they could improve their CDR representatives' consent processes by implementing more items specified in the Standards' Consumer Experience (CX) Guidelines. These recommendations included that consent processes should:

- include a link to Office of the Australian Information Commissioner's (**OAIC**) guidance on Privacy Safeguard 12, which outlines information on data security and redundant data handling,
- include a link to their specific page on https://www.cdr.gov.au/find-a-provider for accreditation verification purposes,
- provide information about the data deletion process:
  - when data will be deleted,
  - why data may need to be retained (e.g., business or legal reasons), and
  - how the data will be deleted (this may include timeframes),
- provide information on how often data is expected to be collected over that period, and
- provide information in relation to complaint handling at appropriate points throughout the consent process.

4. Next steps

We will continue to closely monitor the compliance of CDR representative principals and their CDR representatives with relevant CDR obligations.

When considering appropriate compliance or enforcement action, the ACCC acts in line with the joint ACCC/OAIC CDR Compliance and Enforcement Policy. Oversight of third parties by accredited persons is one of our compliance and enforcement priority areas.

We also continue to review our guidance to ensure it is fit for purpose, and consult with Treasury and OAIC on how to improve representative arrangement governance as necessary.