CLARITY FOR CONSUMER DATA RIGHT PARTICIPANTS ON REGULATORY OBLIGATIONS: IS YOUR BUSINESS READY?

Date: 5 June 2020

Australia Antitrust, Competition, and Trade Regulation Alert

By: Ayman Guirguis, Harriet Alexander, David Howarth

IN BRIEF

- The Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commission (OAIC) have issued a joint Compliance and Enforcement Policy for the Consumer Data Right (CDR) (CDR Policy) to assist consumers and CDR participants to understand the approach the regulators will adopt to encourage compliance and prevent breaches of the CDR regulatory framework Compliance and Enforcement Policy for the Consumer Data Right.
- The CDR regulatory framework will give consumers access to control over their data held by a business, and a right to direct that data to a third party.
- The CDR regime is being rolled out progressively across different sectors of the economy beginning with the banking sector and extending to energy and telecommunications.
- The CDR Policy demonstrates that regulators will have a broad range of powers to facilitate compliance with the CDR framework.
- Businesses in the banking sector should be testing and reviewing their current CDR implementation procedures and businesses in the energy and telecommunications sector should be evaluating what the CDR may look like in their particular sector while planning for future implementation procedures.

THE CDR: WHAT IT IS AND WHERE IT'S AT

The CDR was enacted by the Australian Parliament in August 2019 to facilitate greater choice and control for consumers about how their data is used and disclosed by businesses supplying them with goods and services.

Giving customers greater control over their data is intended to promote greater competition for supply of services to consumers.

Open Banking

The CDR is being rolled out sector by sector across the economy, beginning with the banking sector where it is known as Open Banking.

The timeline for implementation of the sharing of product reference data was initially 1 July 2020. However, due to the impact of the COVID-19 pandemic, banks have been granted a three month exemption to the deadline. This

extension was designed to ensure bank's resources were being directed towards supporting customers during the pandemic.

Consumer data relating to mortgages and personal loans must be able to be shared from 1 November 2020.

Energy & Telecommunications

The Federal Government has announced that the CDR regime will then be extended to the energy sector, with the telecommunications sector to follow.

The Treasury is currently seeking stakeholder views on the draft energy sector designation instrument which outlines the categories of data and entities included within its scope and would provide the ACCC with CDR-rule making powers for the energy sector.

Under the draft instrument, the Australian Energy Market Operator (AEMO) will act as the 'gateway' between energy retailers and customers for requests for CDR information. The draft instrument proposes that CDR information will include identification and eligibility information about the customer, and that electricity distributors will not be subject to the CDR.

The ACCC has recently:

- released CDR accreditation guidelines which are designed to assist applicants with lodging a valid application to become an accredited person under the CDR regime by outlining the criteria for accreditation
- released supplementary guidelines on the insurance and information security requirements of accreditation.

The ACCC has also recently launched what it describes as the 'IT backbone' of the CDR - the CDR Register and Accreditation Platform (RAAP) and the CDR Participant Portal which will allow businesses to apply to become accredited data recipients. Click here for further information.

HOW IT WORKS - THE CDR FRAMEWORK

The CDR framework is intended to improve customer choice and convenience by allowing data to be shared with third parties, such as comparison sites, allowing a customer to negotiate better deals with their current provider which will have the effect of facilitating competition between service providers and developing innovative services for customers.

The CDR regulatory framework has four key elements:

- the *Treasury Laws Amendment (Consumer Data Right) Act 2019* (Cth), which amends the *Competition and Consumer Act 2019* (Cth) (CCA)
- the CDR Rules
- the Consumer Data Standards, developed by CSIRO's Data61 as the Technical Advisor to the Data Standards Body
- the Privacy Safeguard Guidelines developed by the OAIC.

Following the designation of specific sectors of the economy by the Treasurer on advice from the ACCC and OAIC, the ACCC develops rules to govern the specific sector's implementation of the CDR. The rules are then approved by the Treasurer and issued as a Ministerial direction.

The ACCC is responsible for overseeing compliance of the regulatory framework, with assistance from the Data Standards Body in regards to technical matters and the OAIC regarding privacy protections.

CDR COMPLIANCE AND ENFORCEMENT POLICY

The ACCC and the OAIC have recently published the joint monitoring and enforcement policy for the CDR which sets out the approach that they will take to encourage compliance and prevent breaches of the CDR regulatory framework: Compliance and Enforcement Policy for the Consumer Data Right.

The regulators will adopt a 'strategic risk-based approach', guided by principles including accountability, efficiency and proportionality. The policy gives the regulators broad and rigorous powers to facilitate compliance with the CDR.

The ACCC and OAIC will use a wide range of information sourcing and monitoring tools including:

- Stakeholder intelligence and complaints from CDR consumers, businesses consumer groups, other government agencies and approved external dispute resolution bodies
- Mandatory business reporting from data holders and accredited data recipients which will be used to track compliance and identify issues or trends
- Audits and Assessments to ensure parties are complying with the framework which may involve further action to resolve identified compliance problems
- Information requests, compulsory notices and statutory information gathering powers to compel the provision of information where conduct may constitute a contravention of the CCA.

In deciding whether to take enforcement action, regulators will consider factors including the nature and extent of the conduct constituting the breach, whether the conduct was deliberate and whether the business has displayed a corporate culture of compliance.

Enforcement options available to respond to and resolve breaches of the CDR regulatory framework are:

- Administrative resolutions which include accepting a voluntary commitment from a business to address a non-compliance issue, monitoring compliance with the commitment, and recommending improvements to businesses internal procedures and monitoring
- Infringement notices (ACCC), which involves issuing data holders or accredited data recipients infringement notices if the regulators consider a breach has occurred
- Court-enforceable undertakings which involve accepting a formal undertaking from a CDR participant that it will take or refrain from certain action
- Suspension or revocation of accreditation (ACCC) for example, where the ACCC reasonably believes that a revocation or suspension is necessary in order to protect customers

- Determinations and declarations power (OAIC) under which the OAIC can make a determination to either dismiss or substantiate a breach of a Privacy Safeguard or Rule following an investigation which may include an order that the CDR participant not repeat or continue the conduct or redress any loss or damage suffered by consumers including compensation
- Court proceedings which may result in a range of orders made by the Federal Court including civil penalties, actions to remedy the breach, injunctions, or orders disqualifying individuals from being directors of corporations.

The regulators will prioritise forms of conduct that are likely to result in significant detriment to consumers and the integrity of the CDR regime including where data holders refuse to disclose consumer data, or where data holders engage in misleading or deceptive conduct in 'holding out' against consumers wishing to access their data. The regulators will also hone in on conduct that might result in the misuse or improper disclosure of CDR consumer data.

WHAT DOES THIS MEAN FOR YOUR BUSINESS?

The broad enforcement powers available to the ACCC and the OAIC under the policy indicate that regulators will take a vigorous approach to ensuring compliance with the CDR regulatory framework.

Businesses in the banking sector should be:

- reviewing and testing their current CDR implementation procedures to ensure they are compliant before the 1 October 2020 implementation deadline.

Other businesses, especially those in the energy and telecommunications sector, should be:

- carefully reviewing the CDR regulatory framework to evaluate what the CDR may look like in their particular sector
- planning for future implementation procedures.

If you have any issues complying with these obligations, or for more information about the content of this Insight or assistance with compliance of your Competition law obligations, please contact a member of the the firm's Australian competition law team - working together with our banking, commercial technology and energy colleagues.

KEY CONTACTS

AYMAN GUIRGUIS
PARTNER

SYDNEY
+61.2.9513.2308
AYMAN.GUIRGUIS@KLGATES.COM

