AUSTRALIA'S REGULATORS REVEAL THEIR STANCE ON POLICING CONSUMER DATA RIGHTS

15 May 2020 | Insight
Legal Briefings – By **Julian Lincoln, David J Ryan, Danielle Briers and Siobhan Lane**

Covid-19 disruption adds to the challenge facing the banking sector as Australia's new data rights regime looms.

The Consumer Data Right (**CDR**) is currently proceeding through a staged implementation in the financial sector. On 8 May 2020 the Australian Competition and Consumer Commission (**ACCC**) and the Office of the Australian Information Commissioner (**OAIC**) released their Compliance and Enforcement Policy for the CDR (**Policy**). This guidance is an important development as the large banks prepare to make initial consumer data sets available imminently – from 1 July 2020.

Acknowledging that engagement with the CDR may be challenging given disruptions caused by the COVID-19 pandemic, CDR participants in the financial and energy sectors should continue to proactively assess and develop their existing compliance, data governance, technology and customer engagement functions to meet CDR regulatory requirements. In that context, this article explores the regulators' proposed approach to compliance and enforcement, and outlines how this approach interacts with the CDR exemptions framework on which the ACCC has also recently provided guidance.

POLICY OVERVIEW

COMPLIANCE MONITORING

Commentary from the ACCC indicates that the regulators recognise that while the CDR will give consumers greater access to and control over their data, there is a resultant need for significant safeguards to protect consumer data in the context of the CDR's more 'open' data access model. To assess compliance with and identify breaches of the CDR regime (including the Privacy Safeguards, Consumer Data Right Rules and Data Standards), the regulators plan to deploy a wide range of monitoring tools and gain access to broad information sources (including stakeholder intelligence, consumer complaints, mandatory periodic reports, periodic audits and compulsory notices to produce information). The Policy identifies an approach to compliance and enforcement informed by the objective of ensuring that consumers can trust the security and integrity of the CDR regime.

ENFORCEMENT

While the Policy suggests that the regulators' priority is to prevent breaches of CDR obligations through compliance management, enforcement action will also be taken where necessary. Consumer detriment and harm to the CDR regime will inform the regulators' decisions whether to take enforcement action, and while the regulators acknowledge that not all breaches can be pursued, those breaches resulting in a serious level of harm are more likely to result in proportionate enforcement action. CDR participants should take particular care to ensure that their internal systems, processes and compliance functions are directed at preventing the types of conduct identified below, as the regulators have indicated that these types of conduct will be a focus for enforcement:

- repeated refusal to disclose consumer data that is legally required to be disclosed
- misleading or deceptive conduct – for example, an organisation holding itself out as an accredited data recipient when it is not one
- collecting CDR data without valid consent
- intentional use or disclosure of consumer data that is inconsistent with the consumer's consent (including where consent was initially given but has been withdrawn)
- insufficient security controls to protect CDR data.

The enforcement approach and actions taken will depend on a range of factors, including the nature and extent of the breach, the impact of conduct on consumers, subsequent actions of the business and the specific and general deterrent effect of the proposed enforcement action. Types of enforcement actions available to the regulators include:

- ‘administrative resolutions’, such as a voluntary written commitment from a business to improve its internal practices and procedures
- court-enforceable undertakings to the same effect
- infringement notices
- suspension or revocation of accreditation as a data recipient (which may have a significant impact on business operations)
- determinations and declarations by the OAIC following an investigation into a breach of the regime’s privacy provisions
- initiation of court proceedings (especially if the conduct is widespread, causes competitive harm or substantial consumer detriment, or involves a CDR participant that has a history of previous breaches of competition, consumer or privacy laws).

ESTABLISHING COMPLIANCE

The ACCC and OAIC recognise that CDR participants may require a transition period to ensure their systems and processes fully meet their CDR obligations. The Policy provides useful guidance and should help to inform the development of compliance measures (including systems, policies and processes) for businesses preparing to participate in the CDR regime. Fundamentally, it is important for businesses to manifest a culture of compliance to achieve the objectives of the CDR and not be waylaid by time-consuming and expensive compliance and enforcement action from the regulators. Accordingly businesses should consider:

- thoroughly reviewing their relevant policies and processes, including those for privacy and data handling, having regard to the regime and other laws that interact or overlap with the regime (e.g. the Privacy Act)
- implementing robust training programs so that all staff understand CDR obligations and how to manage the risks involved with handling consumer data
- establishing breach notification procedures
- developing a well-structured response plan to rectify breaches in an appropriate and timely manner.

CDR EXEMPTIONS

Where businesses assess that they may not be ready or able to wholly comply with the CDR regime, it may be prudent to consider eligibility to apply for an ACCC exemption in relation to particular data, classes of data or obligations.[1] Importantly the ACCC will not retrospectively grant exemptions, so businesses should engage with the exemptions process as promptly as possible if they think an exemption might be needed.

In response to the impacts of COVID-19 (and submissions from the banking industry), the ACCC granted a three-month exemption to financial services providers including non-major banks, building societies and credit unions regarding their obligation to share product reference data (these obligations will now commence on 1 October 2020). This temporary exemption also applies to product reference data in respect of non-primary brand products offered by the major banks.

When preparing an exemption application, businesses should be mindful that there is "no restriction on the internal use, including future use, that the ACCC may make of the confidential information [disclosed in an exemption application] consistent with the ACCC's statutory functions."

FUTURE CONSIDERATIONS

There has been a high degree of consultation and cooperation with industry throughout the development of the CDR framework, and the Policy continues this theme, stating that the regulators will continue to "work with stakeholders…including through coordinated approaches" to facilitate a compliance culture within the CDR regime. The Policy also notes that the regulators will regularly review and update the Policy to ensure it aligns to their actual approach, and confirms that finalised enforcement actions will be made public. CDR participants are accordingly encouraged to continue engaging with the regulators and the CDR implementation process to support appropriately tailored regulator approaches to CDR compliance and enforcement.

Despite the competing challenges of COVID-19, the timeline for implementation of the CDR in the financial services industry remains in place at the time of writing (subject to the 3 month extension noted above). We acknowledge that this is a challenging time for businesses as they balance competing priorities due to the COVID-19 pandemic. Please reach out to any of the team members listed below for further support in ensuring your business is CDR-ready.

For further information on the CDR regime, please refer to our CDR showcase page.

ENDNOTES

1. The ACCC has recently published its guidelines on applications for exemption under

section 56GD of the *Competition and Consumer Act 2010* (Cth).

Please click here to return to our CDR showcase page

RELATED TOPICS

Data and privacy

FEATURED INSIGHTS

FEATURED INSIGHTS

HELPING YOU STAY AHEAD OF THE BIG ISSUES

BROWSE BY:

- TECH, DIGITAL & DATA

- GEOPOLITICS AND BUSINESS

- NEW BUSINESS LANDSCAPE

RELATED ARTICLES

UPDATED: UK NATIONAL SECURITY ACT 2021 - WHAT INVESTORS NEED TO KNOW

Foreign investment: Rising tides of politics in regulation

Comply or Explain to climate-related reporting – A cross-industry roadmap

KEY CONTACTS

If you have any questions, or would like to know how this might affect your business, phone, or email these key contacts.

JULIAN LINCOLN
PARTNER, HEAD OF TMT & DIGITAL AUSTRALIA, MELBOURNE
+61 3 9288 1694
Julian.Lincoln@hsf.com

TONY COBURN
CONSULTANT, SYDNEY
+61 2 9322 4976
Tony.Coburn@hsf.com

DAVID J RYAN
SENIOR ASSOCIATE, MELBOURNE
+61 3 9288 1831
david.j.ryan@hsf.com

DANIELLE BRIERS
SENIOR ASSOCIATE, SYDNEY
+61 2 9322 4177
danielle.briers@hsf.com