Australia's new Consumer Data Right

What's not to like?

LexisNexis®

Introduction

Australia has introduced a new Consumer Data Right (**CDR**) framework that will take effect in July 2020. The new CDR framework comes hot on the heels of the Independent Review into Open Banking in Australia. Open Banking is the application of the CDR in the banking sector.

Implementation is already very much under way and in July 2020 we will start to see the exchange of consumer data from within this sector (*the proposed February 2020 commencement of Open Banking was pushed out by the ACCC in December 2019*). The telecommunications and energy sectors are next in line and over time the CDR will be rolled out more broadly across the economy.

The introduction of the CDR framework comes at a busy time from a regulatory perspective. Just before Christmas in December 2019, the Federal Government publicly released its much-anticipated response, to the recommendations made under the Australian Competition and Consumer Commission's (**ACCC**) final report into the Digital Platforms Inquiry, which was published on 26 July 2019. In its response, the Government flags its intention to undertake a review of the Privacy Act 1988 (Cth) (**Privacy Act**) commencing in 2020 and concluding in 2021.

And on 22 January 2020, the Treasury released the Government's proposed model for expansion of the Banking Executive Accountability Regime (BEAR) to all banks, insurance and superannuation entities.

It is against this regulatory backdrop that the CDR makes its way into Australia's regulatory landscape.

What is the CDR?

Recognising the increasing importance of consumer data and perhaps in an unintended nod to the extensive rights bestowed on individuals in the EU under the General Data Protection Regulation (GDPR) in relation to the access, control and use of their personal data, the new CDR framework seeks to give individuals (and others) greater control over their own data.

The Government wishes to implement the CDR framework according to four key principles, as follows:

1. The CDR framework should be consumer focussed. It should be for the CDR Consumer, be about the CDR Consumer, and be seen from the CDR Consumer's perspective.
2. The CDR framework should encourage competition. It should seek to increase competition for products and services available to CDR Consumers so that CDR Consumers can make better choices.
3. The CDR framework should create opportunities. It should provide a framework from which new ideas and business can emerge and grow, establishing a vibrant and creative data sector that supports better services enhanced by personalised data.
4. The CDR framework should be efficient and fair. It should be implemented with security and privacy in mind, so that it is sustainable and fair, without being more complex or costly than needed.

The CDR framework is very much the culmination of various recommendations and reports, from the Murray, Harper, Coleman and Finkel inquiries to the May 2017 Productivity Commission report on Data Availability and Use. The Open Banking Review in 2017-2018 paved the way for the CDR framework's introduction.

While such lofty aims and objectives are to be commended, the main challenge for the new CDR framework will be around practical implementation.

So what's the catch?

The CDR framework will be administered by two separate regulators, the Australian Competition and Consumer Commission (ACCC) and the Office of the Australian Information Commissioner (OAIC). Both regulators have been fairly proactive on the topic. February 6th 2020 has seen the introduction of the Competition and Consumer (Consumer Data Right) Rules 2020 (Cth) (CDR rules), which is a key development in progressing the Consumer Data Right in banking. The CDR Rules give legislative force to consumer data sharing obligations in banking that become mandatory from 1 July 2020.

The introduction of the CDR rules is welcome but there is still long way to go, considering that much of the detail of the CDR framework is to be determined at a later date.

Of particular interest is how the Australian Privacy Principles (APPs) detailed in the Privacy Act will sit alongside the new Privacy Safeguards introduced by the CDR framework.

Further, the concept of CDR data is an expansive one and is likely to present technical and commercial challenges once its scope is fully explored.

In addition, the effective implementation of the requirements by each industry may lead to some unintended consequences as the market applies its commercial lens to the new compliance obligations.

Background

Before examining some of these challenges it is important to set the scene and provide a little more detail about some of the key concepts involved.

Who is a consumer?

Perhaps surprisingly the concept of a CDR consumer is somewhat broader than you would expect. Yes, it covers individuals but it will also extend to business customers. This is quite different to many legislative regimes which draw a very firm distinction between individuals as consumers and businesses/organisations which do not fall within this consumer category.

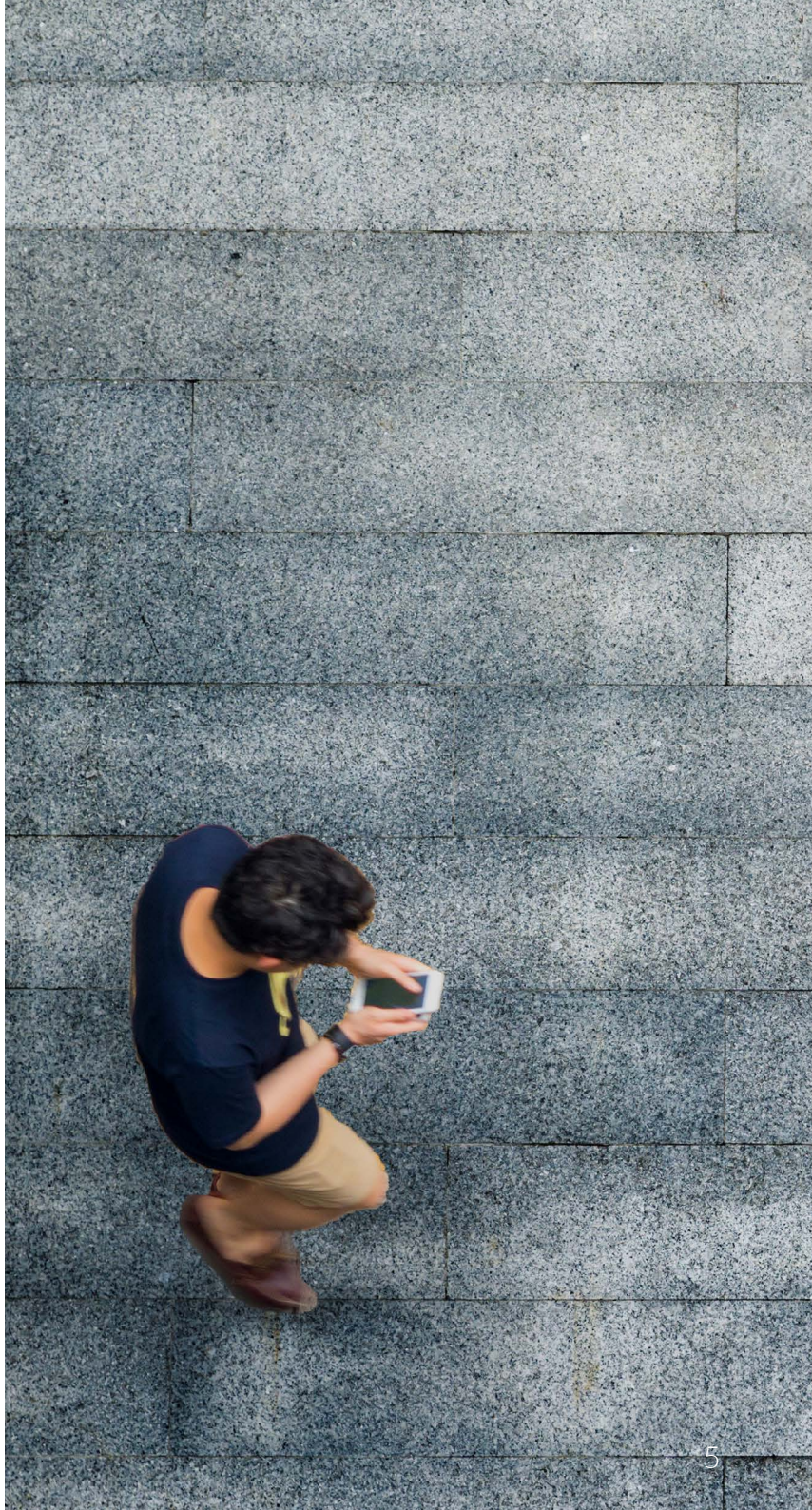
What is CDR data?

CDR data will be determined on a sector-by-sector basis. It will necessarily include the primary data sets specified by the Treasurer but importantly will also extend to include information derived from these data sets. For example, the initial data set for the banking sector will include data on credit/debit cards, deposit and transaction accounts (July 2020), followed by mortgage and personal loan data (November 2020).

So what could have been a fairly narrowly defined category of information is now likely to be somewhat broader. We discuss the commercial ramifications of this extended scope later on.

Data transfers and accreditations

Consumers will only be able to use the right to direct the transfer of their data to trusted third parties who must be accredited.



The following terms must be defined in order to fully understand the scope of the data transfer right:

- an accredited person is a person who has received accreditation from the ACCC that they comply with the requirements of the applicable CDR rules to participate in the CDR framework[1]
- an accredited data recipient is an accredited person who collects, receives or holds CDR data under the CDR rules, but does not hold it as a data holder or designated gateway[2]
- a data holder is a person that holds CDR data for or on behalf of a consumer[3]
- a designated gateway is an entity that facilitates the transfer of CDR data according to the applicable CDR rules[4]

A business may fall within the definitions of an accredited person, an accredited data recipient or a data holder for different consumers or depending on the role the business is fulfilling at any given time. For example, in an open banking context, a bank can:

- Be an accredited person in order to participate in the CDR framework
- Become an accredited data recipient once it has collected CDR data as authorised by a consumer, such as on receipt of account information from another bank to create a new account for a customer
- Become a data holder when holding CDR data for and on behalf of a consumer

The ACCC and OAIC will together set the accreditation criteria, including privacy and security requirements. The Commonwealth Scientific and Industrial Research Organisation (CSIRO)'s Data61 has been appointed as the CDR framework's Data Standards Body, and is developing technical standards for the transfer of CDR data.

1. *Competition and Consumer Act 2010 (Cth) section 56CA*
2. *Competition and Consumer Act 2010 (Cth) section 56AK*
3. *Competition and Consumer Act 2010 (Cth) section 56AJ*
4. *Competition and Consumer Act 2010 (Cth) section 56FA*

A look at some of the practicalities

With so much attention focussed on privacy in the current regulatory environment, the CDR privacy requirements are a good place to start.

Increased privacy obligations

The OAIC has now released its draft Privacy Safeguard Guidelines (Guidelines) for the CDR framework.

The OAIC will regulate the privacy aspects of the CDR framework and provide the primary complaints handling process for the scheme.

The Guidelines aim to provide assistance to entities who will be participating in the CDR framework to understand their privacy obligations, which will be given effect by Part IVD of the Competition and Consumer Act 2010 (Cth) (Privacy Safeguards). There are 13 Privacy Safeguards in total. The Privacy Safeguards are legally binding, but the Guidelines are not.

The OAIC anticipates that for small businesses that are currently not subject to the Privacy Act, compliance with the Privacy Safeguards may be a new experience, if they become participants in the CDR framework. The OAIC is seeking submissions from small businesses to, in particular, identify knowledge gaps and provide further guidance where necessary.

Applicability of the Privacy Safeguards

The Privacy Safeguards will apply differently depending on the roles of the participants in the CDR framework. The table below identifies the Privacy Safeguards that apply to specific roles.

Role	Privacy Safeguards that apply
Accredited person	Privacy Safeguards 1, 3, 4, and 5
Accredited data recipient	Privacy Safeguards 1 to 13 inclusive
Data holder	Privacy Safeguards 1, 10, 11, and 13
Designated getaway	Privacy Safeguards 1, 6, 7 and 12

As such, it is important for businesses to understand how each of the Privacy Safeguards apply in the different roles and functions they may perform in the course of their operations, and how they can integrate the requirements for the Privacy Safeguards into their broader privacy compliance framework.

Interaction with the Privacy Act

While the application of the new Privacy Safeguards is important, how they effectively interact with the Privacy Act and APPs is far from straightforward.

The OAIC has attempted to address this issue in the draft Guidelines by setting out summaries of how each of the Privacy Safeguards applies to each type of CDR entity. In some instances, depending on the status of the CDR entity (for example an accredited person or an accredited data recipient), the relevant APP will apply in parallel with the specific Privacy Safeguard. In other instances, the Privacy Safeguard will apply instead of the corresponding APP or vice versa. Refer to the Appendix for an overview of this interaction between the Privacy Safeguards and the APPs.

A stark difference between the two frameworks is the lack of 'reasonableness' which is a constant theme throughout the APPs and allows a level of flexibility for business in terms of compliance. The concept of reasonableness is missing from the Privacy Safeguards, effectively raising the bar and making privacy compliance in respect of CDR data a stricter requirement.

Of particular note is that an accredited person may only collect and use CDR data with the consent of the consumer. There are stricter consent requirements under the Privacy Safeguards in respect of CDR data than under the Privacy Act. For example, under the Privacy Act, consent must be express or implied. However, the Privacy Safeguards require accredited persons to procure 'voluntary, express, informed, specific as to purpose, time limited, and easily withdrawn' consent from consumers for the collection and use of their CDR data.

The draft Guidelines state that, to comply with this higher standard, accredited persons will be required to provide

consumers with a 'consumer dashboard,' which must contain certain details relating to each consent to collect and use their CDR data.

It is the bolstering of this consent requirement which is likely to cause the most consternation.

Depending on the practical and commercial implications of implementing the 'consumer dashboard' requirement, businesses may consider either:

1. Isolating CDR data from other personal information and records to ensure that they comply with the higher standard of consent in respect of CDR data

2. Altering their existing practices to apply the higher standard of consent in respect of all information collected from consumers. We note that the ACCC has recently recommended to the Government that generally (for privacy law purposes), a higher standard of consent should be required. The Government is currently considering that recommendation amongst others

Implementing effective processes to comply with the express consent requirement is going to be a challenge. Having to consider separating data in this way or applying a higher standard to meet the new Privacy Safeguards across all data management activities is not something that can be achieved overnight.

Either option is likely to be an expensive and time-consuming exercise which should not be underestimated. Notwithstanding this in some ways the broader move to a higher consent standard is likely to arise again as the Government explores changes to the Privacy Act this year. Our expectation is that at some point in the not so distant future, seeking express consent will be the norm. Many organisations grappling with the CDR may well decide to go that next step further and apply the higher standard across their broader data collection activities – only time will tell!

The broad scope of CDR

As noted above, the concept of CDR data is expansive and includes not only the specified primary data set for the nominated sector but also information which is derived from this data set (or further information sourced from the derived information). The intent behind such an expansive definition is to ensure that data holders do not seek to avoid their obligations by making minor alterations to the primary data and thus take it out of scope as a category of CDR data.

While such an approach perhaps deals with this potential risk in part, it creates other issues. The expansive scope makes it a challenge to understand 'what's in' and 'what's out' for data holders. Yes, the right will only apply in respect of specified data sets and specified classes of data holders but these defined categories are somewhat fluid and in some cases open to broad interpretation. Short of published regulatory guidance (which will hopefully be provided at the relevant time by the appropriate regulator for the data holder's industry sector), at

what point can they draw the line?

We all know the value that attaches to data, and in particular, when it is combined with other data sets. Time, effort and money is expended enriching data so it is meaningful to an organisation and can assist it to deliver better product and services to its customers. Clearly, there is a commercial value attached to such data. So can the data holder charge a fee to provide such enriched data? Arguably yes, but not so under Open Banking, with the Treasury indicating fees will be very much the exception rather than the rule. Further, fee amounts are likely to be set by the ACCC, so may not bear any resemblance to the actual investment made by the data holder in the CDR data to be released.

In some circumstances, value added data may comprise confidential information of the data holder. The legislation does not consider this in any way. Can a data holder refuse to release CDR data? If so under what circumstances? All relevant questions which will need to be properly addressed in due course.

While there is an expansive definition of CDR data which preserves and supports the underlying consumer right to access such information, little thought appears to have been given to the practicalities faced by the data holder themselves. In some ways, this is appropriate given the focus of the CDR framework is consumer oriented. However, practical limitations should also be accounted for. While all data holders will no doubt be keen to ensure their customers have appropriate access to their own data, the broad scope of 'consumer' under the legislation may well see circumstances in which competitors of the data holder make access and transfer requests. Such a scenario is fraught with risk and will give little confidence to data holders keen to add value to data sets which may be at such risk.

Preparing for the CDR

For those in the banking sector, we would already expect you to be well advanced as you begin to incorporate the new compliance requirements and update and add new policies and processes to your organisation in advance of July 2020. The CDR rules, introduced by the ACCC on February 6th, will assist to give

some clarity around some of the requirements and practicalities. The CDR will next be introduced to the energy sector (with consultation on data access models already underway), followed by the telecommunications sector. Participants in other sectors will have the opportunity to influence and shape policy by being actively involved during the relevant consultation periods.

From an organisational perspective, it is clear there are some challenges around data management and the interaction between the APPs and Privacy Safeguards. Make the most of the pre-implementation period to assess your key data sets and consider which are likely to fall within scope of a future framework for your sector.

Once your industry sector is designated under formal instrument from the Treasurer, this pre-work will be invaluable as you take more practical steps to review and update processes and infrastructure so you can effectively comply with the new framework.

Once the framework commences in full, there will be a raft of governance and reporting obligations. Your processes and procedures will need to be clearly established so you can properly respond to consumer requests, manage enforcement risk and ensure the smooth running of your technical infrastructure allowing for the transfer and receipt of consumer data to, and from, your organisation. Adequate staff education, resourcing and new policy development will become important. You will need to develop a specific CDR policy which will likely sit alongside your existing privacy policy or be incorporated directly.

Final thoughts and wrap-up

The introduction of the CDR comes at a time of increased regulation across many sectors in the economy – none more so than in banking and financial services. The energy and telecommunications sectors with their close connection to consumers will be watching regulatory developments closely, as they are next in line.

The CDR framework is a bold attempt to promote consumer choice, competition and innovation. It is a complex legislative framework and relies on several regulators, third parties and government agencies for its administration, operation and ongoing implementation.

The CDR has been met with a mixed response to date, with much of the detail yet to be determined. It is this detail that presents a challenge to effective implementation. Time will tell in the coming months as initial commencement for the banking sector in July 2020 approaches. We expect there to be robust discussion from industry, as well as a ramp up by government to explain in a meaningful way to consumers how such an important right is intended to work and how they as the beneficiaries will be able to take advantage of it.

Lead Author Dudley Kneller
Partner | Gadens

Dudley Kneller is a technology lawyer with a specialty in privacy, cyber risk and strategic sourcing and supply projects. He has more than 20 years' experience practising across Australia, Europe and the UK, and has worked on projects based in a range of countries, including the Philippines, India, Russia and throughout South America.

Dudley is listed in Best Lawyers in Australia for Information Technology Law 2020. He is also listed as one of a group of recommended Technology, Media, Telecommunications Lawyers for Melbourne in Doyle's Guide from 2015-2019.

Dudley.Kneller@gadens.com

Contributor Raisa Bianco
Associate | Gadens

Raisa Bianco is an Associate in the Intellectual Property & Technology team.

She has particular focus on information technology, outsourcing and procurement, privacy, and intellectual property. Her commercial experience includes mergers and acquisitions, divestments, start-ups, licensing and operational documentation, and general corporate and contractual advice.

Raisa.Bianco@gadens.com

About LexisNexis®

LexisNexis is part of RELX Group, a world-leading provider of information and analytics for professional and business customers across industries. LexisNexis helps customers to achieve their goals in more than 175 countries, across six continents, with over 10,000 employees.

Appendix

Summary of application of Safeguards and APPs by CDR entity

	ACCREDITED PERSON	ACCREDITED DATA RECIPIENT	DESIGNATED GATEWAY	DATA HOLDER
Safeguard/APP 1	Both	Safeguard 1	Both	Both
Safeguard/APP 2	APP 2*	Safeguard 2	APP 2	APP 2
Safeguard/APP 3	Both	Safeguard 3	APP 3	APP 3
Safeguard/APP 4	Safeguard 4*	Safeguard 4	APP 4	APP 4
Safeguard/APP 5	Safeguard 5	Safeguard 5	APP 5	APP 5
Safeguard/APP 6	APP 6	Safeguard 6	Safeguard 6	APP 6
Safeguard/APP 7	APP 7	Safeguard 7	Safeguard 7	APP 7
Safeguard/APP 8	APP 8	Safeguard 8	APP 8	APP 8
Safeguard/APP 9	APP 9	Safeguard 9	APP 9	APP 9
Safeguard 10/APPs	APPs	Both	APPs	Both
Safeguard 11/APP 10	APP 10	Safeguard 11	Safeguard 11***	APP 10
Safeguard 12/APP 11	APP 11	Safeguard 12	Safeguard 12	APP 11
Safeguard 13/APP 11	APP 12	Safeguard 13	Both	APP 12

* Privacy Safeguard 2 applies in practice to an accredited person, and therefore should still be complied with. This is because an accredited person will become an accredited recipient for a consumer's CDR data once they collect such data.

** Although APP 4 applies in parallel with Safeguard 4, an accredited person will be an accredited data recipient for CDR data collected under the relevant CDR rules, to which APP 4 will not apply.

*** APP 10 continues to apply to all personal information collected, used or disclosed where the entity is not required/authorised to disclose the data under the applicable CDR rules.