Information Integrity Solutions Pty Ltd
Building trust and innovative privacy and security solutions

Studio 2, Level 1, 71 Balfour Street, Chippendale
Sydney NSW 2008 Australia

Tel: +61 2 8303 2438
Fax: +61 2 9319 5754

inquiries@iispartners.com

www.iispartners.com

High-level briefing on Consumer Data Right (CDR)

This paper offers a high-level overview of some of the key features of the CDR which is now up and running following amendments to the *Competition and Consumer Act 2010*. A phased introduction to the banking sector begins early next year. The energy and telecommunications sectors are set to follow. There are no plans to target further sectors at this stage but expansion to other sectors is, of course, possible.

At this point, it appears that CDR in the energy sector will look quite different. In banking, ACCC has adopted an 'economy-wide' model, in which consumers and accredited third parties access data directly from data holders. However, for the energy sector, the ACCC prefers a 'gateway model' whereby an industry body (in this case, the Australian Energy Market Operator (AEMO)) plays a gateway function, providing CDR data from data holders (which may include retailers and potentially distributors) to accredited data recipients.[1]

1. The CDR: aims and objectives

The CDR aims to allow Australian consumers to access certain data in a usable form and to direct a business to securely transfer that data to an accredited third party. The ACCC states that 'The CDR will give consumers greater access to and control over their data. It will improve consumers' ability to compare and switch between products and services, and will encourage competition between service providers, leading not only to better prices for customers but also more innovative products and services.'

The Privacy Act already gives individuals rights to access personal information held about them. These rights are not new. What is new under the CDR regime is the attempt to strengthen the 'portability' aspect of data access and create a framework for consent-driven disclosure of consumer data between CDR participants.

2. Regulations to be aware of

The CDR is established by Part IVD of the *Competition and Consumer Act 2010.* The Act also contains CDR privacy safeguards. The Act enables the ACCC to establish binding rules

[1] ACCC, *Consumer data right in energy, Position paper: data access model for energy data,* August 2019, p 3.

that add 'meat' to the Competition and Consumer Act 'bones.' So far, as noted above, the ACCC has established CDR rules for the banking sector. Next it will do the same for the energy sector. Other CDR standards and guidelines include:

- Accreditation guidelines, and supplementary guidelines made by the ACCC
- Consumer Data Standards, under development by the Data Standards Body
- Consumer Experience Standards and Guidelines, also under development by the Data Standards Body
- CDR Privacy Safeguard Guidelines, which are provided for under the Competition and Consumer Act but are not a legislative instrument; under development by the OAIC.

3. The CDR and the Privacy Act

The OAIC advises that: 'Generally, the privacy safeguards [in the Competition and Consumer Act and in CDR rules] apply in respect of an entity's handling of CDR data instead of the *Privacy Act 1988* (Cth) and the Australian Privacy Principles (APPs).'[2] What 'CDR data' means depends on the sector and is designated via a legislative instrument. Adding to the complexity, however, is that not all privacy safeguards apply to all CDR participants all of the time. Where a privacy safeguard does not apply, the APPs will. For example, Privacy Safeguard 12 requires security protections for CDR data. It applies to 'accredited persons' and 'designated gateways' but not 'data holders.' Therefore, data holders must continue to comply with APP 11 (the security principle in the Privacy Act) in relation to CDR data.

4. Key features of the CDR

This section gives an outline of a few of the key features of the CDR, **as it applies to the banking sector**. In it, IIS refers to key CDR participants, including 'accredited persons', 'accredited data recipients' and 'data holders.' For more information about the meaning of these terms, see Chapter B of the OAIC's Draft CDR Privacy Safeguard Guidelines.

4.1 Access requests to CDR data

Providing for access to CDR data is the central aim of the CDR regime. The CDR rules applying to the banking sector require participants to offer online services to facilitate access requests and provision of information. These include:

- **A product data request service**
  Data holders (eg banks) must provide an online service that allows others to make product data requests and receive the data in machine readable form.
- **A direct request service**
  Data holders must provide an online service for consumers that allows them to make

[2] OAIC, *Draft CDR Privacy Safeguard Guidelines*, Consultation draft, October 2019, paragraph A.25.

CDR data requests (for data about themselves) and receive the information in human readable form.

- **An accredited person request service**
  Data holders must provide an online service for accredited persons (persons accredited to make CDR data requests on behalf of consumers) that allows requests that return data in machine readable form.
- **Consumer dashboards**
  Data holders and accredited persons must provide consumers with an online 'consumer dashboard' which sets out the various requests they have made or consented to, along with a range of prescribed information about the nature of the data and its use; the dashboard must allow the consumer to manage the various consents and withdraw consent at any time.

All of these online services must comply with the data standards.

The CDR rules for the banking sector outline a range of other requirements to support this access regime – rules about when an 'accredited person' may make a request on a consumer's behalf, how to make a valid request, what CDR data may be requested, what the accredited person must tell the consumer when they seek consent and how they are able to use and disclosure the data they receive. If a 'data holder' receives a valid request for 'required consumer data', it must give access.

4.2 Consent

The different ways that consent is dealt with under the CDR rules and the Privacy Act gives an apt illustration of how differently the two approach privacy: the former is prescriptive and detailed; the latter principle-based. Under the CDR regime, an accredited person may not collect or use CDR data about a consumer without express consent. The CDR rules require that consent be voluntary, informed, specific as to purpose, time limited and easily withdrawn. While the Privacy Act does not formalise such concepts, the OAIC's APP guidelines set out similar requirements and it is generally accepted that consent would be meaningless or invalid if such foundational concepts were missing.

The CDR rules articulate a wide range of other consent requirements. Their comprehensive and prescriptive nature demonstrate that aligning with CDR consent requirements will be a major change of approach rather than a small adjustment for most participants.

4.3 Data sharing

The CDR regime facilitates data sharing in the sense that it requires data holders to disclose product information and CDR data about consumers on request. Requests for CDR data about a consumer can only be made by the consumer or on their behalf with their express consent. Some CDR data is designated as 'required' and must be disclosed by the data holder when requested by or on behalf of the consumer. Other data is designated as 'voluntary' meaning that it is at the discretion of the data holder whether to disclose it.

There are, however, restrictions on how recipients of the data may then use or disclose that data. Those restrictions apply to data recipients, not to the data holders that disclose the information. Generally, an accredited data recipient may only **use** CDR data to provide goods or services requested by the consumer in compliance with the 'data minimisation principle' and in accordance with a consent from the CDR consumer. And the recipient may only **disclose** CDR data to the consumer in question or to an outsourced service provider to achieve those allowable uses and disclosures.

Accredited data recipients may only disclose CDR data (by sale or otherwise) more broadly if the data has been de-identified in accordance with the CDR data de-identification process. The CDR rules specifically prohibit a data recipient from asking a consumer to consent to the recipient selling their data (unless it is de-identified) or using it for the purpose of identifying, compiling insights in relation to, or building a profile in relation to, any identifiable person who is not the CDR consumer who made the request (other than in limited circumstances set out in the rules).

4.4 Data analytics

Data analytics activity is permitted but may be restricted by CDR rules on use and disclosure and de-identification (see below). That said, restrictions on use and disclosure (including restrictions that limit analytics) apply to data recipients and designated gateways and not to data holders. Therefore, analytics activity of data holders should not be affected by the CDR regime as their use and disclosure of CDR data would be regulated by APP 6 as it is now (though any activity in the role of an accredited data recipient would). IIS understands that a data recipient may use CDR data for analytics (or disclose the data to an outsourced service provider to conduct analytics) if the analytics are to provide goods or services requested by the consumer. The Competition and Consumer Act specifies that derived data (for example, data derived from conducting analytics on a consumer's CDR data) still constitutes 'CDR data' and is therefore still subject to the various restrictions on use and disclosure contained in the CDR rules.

4.5 'Redundant data' and de-identification

The CDR regime introduces the concept of 'redundant data'. An accredited data recipient must destroy or de-identify CDR data that has become redundant. Data is rendered redundant if the consent applying to the data expires or the consumer withdraws their consent. CDR data also becomes redundant if the accredited data recipient no longer needs the data for a purpose allowable under the CDR rules or privacy safeguards and other exceptions do not apply.

In practice, this means that a consumer can effectively ask an accredited data recipient to delete their data at any time by withdrawing their consent and indicating that they wish their redundant data to be deleted rather than de-identified.

In cases where a recipient of CDR data elects to de-identify the data rather than delete it (where it is allowable to do so and the consumer has consented) it must ensure that its de-identification process meets the requirements of the CDR rules. The CDR rules create a high bar for de-identification. Data recipients must de-identify data to the extent that it would be suitable for an open release environment (regardless of whether data is in fact to be released into an open environment, or what controls and safeguards apply to the data access environment).[3]

The OAIC advises, therefore that, 'de-identification will generally only be appropriate where CDR data has been through an extremely robust de-identification process that ensures — with a very high degree of confidence — that no consumers are reasonably identifiable.' The OAIC further observes that, 'as a result, even if some CDR data is able to be sufficiently de-identified to this required extent, the utility of that data for many intended uses would likely be compromised.'[4]

This is a higher bar than equivalent de-identification provisions in the Privacy Act which generally allow that data is de-identified if it is no longer about an identifiable person or a person who is reasonably identifiable. The OAIC has advised in guidance material that context is important and that the same information may be identified in one context and de-identified in another. This means that an organisation can take into account the specific environment in which the data is to be held, as opposed to having to assume open release.

5. Conclusion

IIS has two broad observations with which to sum up.

First, data portability – as a concept, as a consumer offering – has value. It supports consumer rights and control over their information and allows them to move their information between organisations more effortlessly and seamlessly. From a consumer and privacy perspective, it is ethically sound. Therefore, IIS believes there is value in exploring options to enhance data access rights (already available under the Privacy Act) in that direction.

Second, organisations should monitor CDR developments closely and engage with ACCC during consultations affecting their sector. We recommend being ready to act, but not acting too soon, given the potential for variability between the sectors, both in terms of the different CDR models that may apply to a given sector, and the sector-specificity of the data that may be covered.

Natasha Roberts
Senior Consultant

[3] OAIC, *Draft CDR Privacy Safeguard Guidelines*, Consultation draft, October 2019, paragraph 12.90.
[4] OAIC, *Draft CDR Privacy Safeguard Guidelines*, Consultation draft, October 2019, paragraph 12.92-93.