ORGANISATION

The consumer data right framework

Consumer data rights aim to shift the balance of power between Australian companies and their customers. The consumer data right (CDR) framework creates rules in relation to account service and product-related information, associated with individual and corporate customers (CDR data). These rules allow customers greater transparency and control over their data.

This director tool aims to outline the CDR framework and highlight some core risks and opportunities boards should consider when assessing its impact to their organisation. The CDR framework can be used to access a great deal of valuable information about customer behaviour and opportunities for product bundling, cross-selling, and the delivery of new information-based services. CDR may not only impact an organisation directly, but also indirectly if other organisations with which it is associated make use of CDR data.

What is the scope of the CDR framework?

Under the CDR framework, customers have the power to access their CDR data to better understand the service or product they are receiving, the price they are paying for that service or product, and for ease of comparison with the services and products of competitor. Customers may also give permission for third parties to access and use their CDR data. The third parties may be competitors of their current service provider, supplementary or related service providers, (perhaps including intermediaries that offer to analyse the value being received or assist customers to get a better outcome).

The CDR framework also includes mandated standard product information. Regulated industries (see 'designated sectors' below in *How is the scheme administered?*) are required to provide product information statements so that customers have an accessible way to understand the terms of supply and to compare their product or service with alternatives available from competing providers.

The CDR framework has been created so that it can apply across the Australian economy. The stated intention of the government is to have it apply widely. It has been implemented for the financial services industry and application to the energy sector is underway. The government has indicated that telecommunications service providers is expected to be the next.

An important feature of the framework is that participants are not limited to their industry sectors. An accredited participant might, for example, offer a general service that aims to optimise customer choices over multiple products and services from different industry sectors.

What information must be shared?

The information that must be shared by a sector is determined in the first instance by the ministerial designation issued in relation to that sector. For financial institutions, for example, the information to be shared is described as information provided directly by the person using the service (including in relation to other persons using the service), information about the service, information otherwise obtained buyer on behalf of the financial institution and information about the use of the product including access information. Within these limitations, the Australian Competition and Consumer Commission (ACCC) has made rules that specify the information to be shared.

For the financial sector, the listed information specified includes:

- Customer data: information about the customer, personal contact details if a natural person (but not the date of birth), or company details if a business;
- Account data: account identification and operation information including name, number, transactions, authorisations, scheduled payments, and authorised payees;
- Transaction data: date of transaction, identification of counter party, merchant information, amount, and description; and
- Product specific data: type, name, price including fees, charges and interest rates, benefits including discounts and bundles, terms, and conditions an eligibility.

For the energy supply sector, the specified information proposed by the ACCC includes:

- Information about the customer and customers associates;
- National metering data information relating to the arrangement with the customer;
- Metering data that relates to the supply to the customer;
- Distributed energy resources register information relating to the supply arrangements with the customer;
- Billing information;
- Details of an electricity or dual fuel arrangement tailored to the customer or as provided to the customer; and
- Information about a natural gas retail arrangement as available to new customers.

Who can participate in the scheme?

The parties required and/or able to participate in the scheme are:

- CDR consumers: these are not 'consumers' as protected by Australian Consumer Law. Rather a CDR consumer is any entity that can access the CDR data held by a data holder and can direct that the information be disclosed.
- Data holder: this is an entity that holds CDR data. A data holder can be designated, reciprocal or receiving (but is not a designated gateway):
  - A designated data holder is a party subject to the rules, such as the financial institutions currently regulated, the energy supply companies whose scheme is under development and those further industry sector participants to be designated by the Minister.
  - A reciprocal data holder holds CDR data that was not transferred to it under the consumer data rules (or derived from such data). This could occur where the accredited data recipient provides similar services to a designated data holder
  - A receiving data holder is a person who holds an accreditation, holds data included in the designation instrument as a result of a transfer under the consumer data rules, and meets conditions included in the consumer data rules.
- CDR participant: this can be an accredited person, data recipient or a designated gateway:
  - An accredited person is a person accredited by the ACCC;
  - A designated gateway is an entity that helps organise, manage, and provide access to CDR customers on behalf of a designated industry. For example, the Australian Energy Market Operator is acting as a designated gateway for the energy regulator.

The criteria for approval by the ACCC of a CDR participant includes that the applicant:

- be a fit and proper person per fit and proper person criteria;
- have adequate insurance or comparable guarantee to compensate for reasonably foreseeable loss arising from a breach of obligations;
- be able to comply with Schedule 2 of the CDR Rules[1], setting out data security obligations;
- have internal dispute resolution and be a member of an external dispute resolutions scheme;
- have an address for service and, if a foreign entity, have a local office; and
- has not:
  - committed an offence punishable by five years or more within last 10 years;
  - committed an offence of dishonesty;
  - committed a contravention of CDR law or similar overseas law;
  - suffered an adverse determination under the *Privacy Act 1988* (Privacy Act) or similar overseas law;
  - been disqualified from managing a corporation or subject to a banning order;
  - suffered insolvency or bankruptcy;
  - been subject (or an associate subject) to a determination under an external dispute resolution scheme recognised by the Privacy Act or otherwise that requires monetary compensation.

The ACCC can also consider any other matter, including the objects of the CDR scheme.

How is the scheme administered?

Treasury has oversight of the scheme. The Treasurer has power to make legislative instruments designating sectors.

The ACCC has power to make CDR rules, operate as the data recipient accreditor (to accredit participants) and engage in enforcement. The ACCC currently also maintains the Accreditation Registrar of accredited participants.

The OAIC has power to make Privacy Safeguard Guidelines and enforce the privacy of CDR data.

There is also a data standards body called Consumer Data Standards (the program is part of CSIRO's Data61)[2].

Examples of how it will work in practice

CDR consumers obtain CDR data

CDR consumers can obtain and review information about a product or service that they have been receiving. Under the Privacy Act, natural persons can review personal information held by regulated businesses and government departments. The CDR right extends to corporate business customers and the information that can be accessed relates to the customer, the services and the services being supplied, rather than only personal information.

CDR consumers authorise an accredited data recipient to obtain CDR data

CDR consumers can authorise an accredited data recipient to obtain CDR data. This may be to provide an additional service. For example, an investment adviser might review the fees and charges made by a financial institution against a customer's account and recommend an alternative supplier or review the customer spending habits and recommend a savings plan.

In this scenario the accredited data recipient must only use the CDR data for the authorised purpose. There must be express consent for that purpose from the customer and that consent must be renewed annually.

There is no requirement that the accredited data recipient be limited to a particular designated industry. The accredited data recipient might seek consent from a CDR consumer to review CDR data from financial providers, energy providers, telecommunications providers and, in future, other designated sectors in order to build a more complete picture of the consumer and provide more holistic advice.

CDR consumers authorise competing businesses to access CDR data

CDR consumers can authorise competing businesses to access CDR data. This this might be done to support a competing service offer, to facilitate the transfer of the account and/or to provide a value-added service.

[1] Australian Government, 2020, Supplementary Accreditation Guidelines, Information Security v2.0, Consumer Data Right, **https://www.accc.gov.au/system/files/CDR%20-%20Accreditation%20-%20Supplementary%20Accreditation%20Guidelines%20Information%20Security.pdf**, (accessed 3 November 2020).

[2] Consumer Data Standards, [website], **https://consumerdatastandards.gov.au/**, (accessed 3 November 2020).

Considerations for Australian boardrooms

The expanding application of the CDR framework presents elements of opportunity and risk for Australian organisations. At its core, this important legislative regime will have the significant impact of increasing competition and enabling many new information-based services.

Directors of organisations in a current or future designated sector should consider the following:

- Your organisation will be managing the costs of understanding and implementing the new requirements and maintaining security of the CDR data.
- Your organisation might consider how to obtain consent from the customers of your competitors, and how you might use the CDR data of your competitors' customers to improve service offerings and/or facilitate the transfer of customers from competitors.
- Conversely, your organisation might consider the possible consequences of your competitors gaining access to CDR data regarding your customers, and how competitors might go about obtaining consent and winning away business.
- You might consider how data from other sectors could be relevant to your organisation and whether or not it might indicate potential new customers, potential cost savings and/or new services offerings and bundling opportunities.
- The CDR framework foreshadows the possible creation of new service intermediaries operating as accredited intermediaries. Consider whether your management is monitoring market entrants, how that market entrant is impacted by accredited participants, and how they might impact business operations.

Related AICD Director Tools:

- *Managing a data breach: Ten oversight questions for directors*
- *National security compliance for directors*
- *Data and privacy governance*

About the Author

Patrick Fair GAICD BEc LLB CIPM FAISA, is the principal of Patrick Fair Associates; an Adjunct Professor at the School of Information Technology, Faculty of Science, Engineering and Built Environmental, Deakin University; the Chairman of the Communications Security Reference Panel at the Communications Alliance; and General Adviser for LexisNexis Practical Guidance Cybersecurity, Data Protection and Privacy.

About us

The Australian Institute of Company Directors is committed to strengthening society through world-class governance. We aim to be the independent and trusted voice of governance, building the capability of a community of leaders for the benefit of society. Our membership includes directors and senior leaders from business, government and the not-for-profit sectors.

For more information **t:** 1300 739 119 **w:** aicd.com.au