Robyn Chatwood, Dentons

Robyn Chatwood is a partner and leader of the technology practice group at Dentons, specialising in fintech and privacy. Her practice covers franchising and distribution, commercial contracts and concession agreements, information technology and communications law, e-commerce law, data protection/privacy, and new technology and IP such as artificial intelligence, payment platforms and crypto currencies, augmented reality and virtual reality.

CONSUMER DATA RIGHTS

An introduction to open banking

Robyn Chatwood

Overview

The consumer data right (CDR) regime aims to give more control to customers over data held about them. It will start a new era of 'open banking' and reflects that Australia values a data economy and sees that as a way to enhance competition and innovation in banking, energy and telecommunications, as it will make it easier for consumers to change suppliers.

Consumers will be able to direct their current supplier to provide their data to other suppliers or comparison services. However, there will also be more privacy and data sharing obligations and additional penalties for breaches of the new laws.

Open banking

The Australian government passed legislation on 1 August 2019 to provide new rights for consumers and small businesses in relation to their data from July 2019. The *Treasury Laws Amendment (Consumer Data Right) Act 2019* (CDR Act) provides a new 'consumer data right' (CDR) that will have a major impact on the banking sector. The CDR relating to banking data is usually referred to as 'open banking'.

The legislation will have a major impact on the banking sector immediately, and the energy and telecommunications sectors will also soon be within the scope of the new laws. And it will have broad extra territorial reach as it will apply to CDR data generated or collected both in and outside Australia.

The text of the actual legislation passed differs from the draft legislation released in 2018 and also differs from the text of the enacting Bill, which had been first introduced into Parliament in early 2019; that draft legislation lapsed due to the Federal election in May 2019.

The regime will give customers more control and choice over data held about them. The government considers that this will promote competition and innovation in the affected sectors as customers will be able to change their suppliers more easily if they can direct their current supplier to provide their data to other suppliers or comparison services.

The CDR regime will impose significant additional privacy and data sharing obligations and penalties for breach. The geographic scope of the proposed law is broad as it will apply to CDR data generated or collected both in Australia and outside Australia.

In this paper, Robyn Chatwood and Ben Allen, who lead the Dentons Australian privacy law practice, explain.

What is a 'consumer data right'?

Consumer data rights are rights of consumers to direct their supplier (such as their bank) to share with others the supplier's information held about the consumer.

Once a sector is designated under the CDR regime, product data and consumer data must be disclosed on request of the customer.

- **Product data** is CDR data that does not relate to any specific consumers—so this is generic product information of the supplier

such as terms and conditions or the availability of a product.
- **Consumer data** is CDR data that is specific to the consumer, such as name and contact details, account details and transaction details.

As noted below, certain classes of information or data will initially be excluded from the open banking regime, being certain credit information and 'materially enhanced information'.

Who has consumer data rights?

The definition of 'CDR consumer' is broad—a consumer can be individuals, businesses and trusts. Small and medium-sized businesses (SMEs) will have CDR rights. The Act extends coverage to those business customers and individuals who are 'reasonably identifiable' from CDR data.

Sectors that will be regulated and reach outside Australia

The CDR Act provides that the Australian Treasurer can designate industry sectors to which the CDR will apply ('designated sectors'). The government has committed to applying the CDR regime to the banking, energy and telecommunications sectors, and eventually across the economy.

Currently, all authorised deposit-taking institutions (ADIs), other than foreign bank branches, will be regulated data holders and so banks, credit unions and building societies will need to comply with the new laws.

The government has released for consultation a draft designation instrument (the *Consumer Data Right (Authorised Deposit-Taking Institutions) Designation 2019*) designating the CDR regime applying to the banking sector once the final instrument is registered.

Of interest is that the draft designation instrument provides that two categories of data are to be initially excluded from the open banking regime:
- **Certain credit information:** certain credit information (as described in the *Privacy Act 1988*) such as credit infringements, court proceedings and information about personal insolvency etc., is to be excluded.
- **Materially enhanced information:** data holders will also not be required to disclose 'materially enhanced information' which is defined as information where "… the information was wholly or partly derived through the application of insight or analysis to… [the] source material; and … that insight or analysis … was applied by, or on behalf of, the entity that holds the information or on whose behalf the information is held; and rendered … significantly more valuable than the source material".

The Explanatory Material to the draft designation instrument provides examples of information that is considered to be and to not be materially enhanced.

Examples of material enhanced information include:
- the outcome of an income, expense or asset verification assessment
- categorisation of transactions as being related to groceries or rent
- significantly improved descriptions of transactions utilising geolocation or business name data from external sources.

Examples of information which is not material enhanced information include:
- a calculated balance
- an amount of interest earned or charged
- a fee charged
- a reference number, including a routing number, a clearing house number or a swift code
- information identifying a person, body, product, transaction or account
- data on authorisations
- the categorisation of source material based on a feature of the product to which it relates, including categorisation by the fees or interest rates applicable to the product
- information that results from filtering or sorting source material by reference to a date, period, amount or classification.

Legislative framework

The CDR Act sets out the overarching regulatory framework and contains the power of the Minister to designate the sectors to which it will apply. It also sets out the framework for there to be rules and standards governing how data is to be shared and the technical standards for sharing of the CDR data.

Rules and privacy safeguards—ACCC and OAIC

The Act is supplemented by further rules which are being developed by Australia's consumer regulator, the Australian Competition and Consumer Commission (ACCC). The ACCC will have an enforcement role and its consumer data rules provide more detail about how the regime will work.

Draft CDR Rules released by the ACCC provided that product reference data (PRD) were due to be made available by the four largest banks (being the Commonwealth Bank, National Australia Bank, Australia and New Zealand Bank and Westpac) from 1 July 2019. These banks have commenced voluntarily publishing PRD.

The ACCC, as lead regulator, will be supported by the federal privacy regulator in Australia, the Office of the Australian Information Commissioner (OAIC) and certain privacy safeguards.

The CDR Act provides for new enhanced 'privacy safeguards' and an accreditation process for data sharers. The privacy safeguards will be incorporated under the *Australian Competition and Consumer Act 2010* and they will apply irrespective of whether data belongs to an individual or a business—a departure from the current approach of the Australian Privacy Principles which are established under the *Privacy Act 1988* and which regulate 'personal information'.

The quote

The CDR regime will give customers more control and choice over data held about them.

Breaches of the new privacy safeguards will attract civil penalties and the OAIC will have new powers to enforce them through the courts.

[Note: the OAIC released its draft privacy safeguard guidelines for comment in late-October 2019.]

Technical Standards

Technical standards for the CDR are to be designed by a new Data Standards Body established to create data standards for how data is to be shared.

Data61 (ie. the data arm of CSIRO, which is the Australian Government's research organisation) has been appointed as the interim standards body and has published a working draft of the standards that will underpin the new regime.

Data61 has been working with the ACCC and the OAIC to develop draft technical standards to design application program interfaces (APIs) to allow consumers to access and share data with accredited parties under a CDR regime. Data61 has posted a set of draft banking and common application program interface (API) standards on GitHub, guided by four 'outcome principles' [refer to https://consumerdatastandardsaustralia.github.io/]. APIs must also comply with eight 'technical principles'.

When will open banking commence?

Timing for commencement of the regime will differ among the various players in the banking sector. The four largest Australian banks will start first, with the other ADIs to follow. The Treasurer has announced the following timetable [as at August 2019]:

From July 2019:

- The four largest Australian banks will be required to publicly share the product data (being the PRD) about credit and debit cards, deposit accounts and transaction accounts.
- The ACCC and Data61 will launch a pilot program with these banks to test the performance, reliability and security of the open banking system, with consumers and fintechs being invited to participate in these pilots.

From February 2020:

- Product and consumer data for mortgage accounts is to be made available.
- Banks will be required to publicly share consumer data about credit and debit cards, deposit accounts and transaction accounts.

From July 2020:

By the four largest Australian banks:

- access to product data for personal loan and other accounts.
- access to consumer, account and transaction data for personal loan and other accounts.

By all other ADIs:

- access to product, account and transaction data for credit and debit cards, deposit accounts and transaction accounts.

From February 2021:

By all other ADIs:

- access to product, account and transaction data for mortgage products.

From July 2021:

By all other ADIs:

- Access to product, account and transaction data for personal loan and other accounts.

Now that the law has been passed, the designation instrument will be finalised and issued together with the rules, technical standards and privacy safeguards. Participants in the new regime, such as the various entities who are to be accredited to receive data and the ADIs who are data holders, will then undergo testing to ensure the data exchanges are accurate and compliant.

Concurrently, the ACCC has commenced consultation on the CDR regime applying to energy sector. The telecommunications sector will be next.

What penalties will apply?

Penalties of up to AU$420,000 (or AU$2.1 million for businesses) may be imposed for misleading conduct relating to the transfer of CDR data and to breaches of the new privacy safeguards.

What to do now?

Now that the CDR laws have been passed, those in the banking, energy and telecommunications sectors should prepare for the new rules by doing the following:

- Consider if and when you are caught by the new laws and what data (and where it is held around the world) will be within scope.
- Plan how to comply by reviewing operations and considering what systems or processes would need changing or implementing.
- Consider how to leverage CDR data to take advantage of opportunities provided by the new laws and consider if you hold valuable data sets that might be required to transfer or that may be excluded from requirements to transfer.
- Implement your new functional capability, compliance systems and processes (eg. by developing APIs that meet the technical standards). Consider how to make product data available via an API in accordance with standards made by the Data Standards Body.
- Establish procedures for dealing with consumer requests for CDR data transfers and a CDR policy to govern them.
- Train staff on the new laws and how to comply with them.
- If not already, become a member of the external dispute resolution scheme for the resolution of disputes involving the CDR—for open banking that will be the Australian Financial Complaints Authority (AFCA). **FS**