

# The way consumers share their data is changing. Is your business prepared?



NOVEMBER 2023

The previous New Zealand Government was seeking to introduce legislation (called the Customer and Product Data Bill) that would establish a Consumer Data Right (CDR) in this country. In the run-up to the 2023 General Election, the National Party indicated that it would continue the passage of the CDR legislation if they were elected and make the Bill fit for purpose.

Given this, it's timely to consider how businesses can prepare for the introduction of CDR and consider the likely next steps.

CDR means consumers will be able to request that their personal data, as well as product data, is securely shared with trusted third parties. With greater control over their data, consumers can more easily make decisions about how and where they spend, save and invest.

Organisations impacted by CDR will have to make a wide range of changes. So, even though the new Government is still being formed, businesses should start planning now.

## What is a Consumer Data Right? A summary

When businesses such as banks, insurers, energy and telecommunications companies provide services to consumers, data is created. This consumer data holds significant value but it is not easily unlocked. At the moment, people can ask for a copy of their personal information and pass it on to third parties, but the process can be inefficient, time heavy, insecure and is not digitally-enabled.

Consumer Data Right (CDR) seeks to address this. It gives consumers a mechanism to request that businesses securely share their personal data, as well as product data, in a standard format with trusted third parties. It also authorises third parties to make decisions on behalf of consumers, for instance initiating payments. Essentially, CDR involves setting up a system of rules and technology used to share consumer data in line with a consumer request.

By using a CDR, a consumer could, for example:

- Ask their bank to share their transaction data and product data with a third party budgeting app, so that they can get targeted advice based on their specific circumstances.
- Ask their energy provider to share their data to another energy provider to see if they can get a quote for a cheaper plan.
- Ask their bank to action a decision, such as switching to another provider.



## How can your business get prepared?

CDR will change the way businesses function and consumers behave. For impacted businesses, there are likely to be significant compliance costs for setting up mechanisms to share data, implement updated data security and consent handling measures, and train staff.

However, there are benefits for businesses too. The Government anticipates that CDR will encourage innovation and help facilitate competition, particularly within the financial services sector, by supporting innovators to create new or improved products and services.

Businesses must get ready to face the changes but what do they need to do? The answer lies in some key factors.

### **CDR will make it easy to move providers. Is your customer experience and value proposition strong enough to retain and attract customers?**

CDR will make it easier for customers to switch from one provider to another. This will encourage innovators to create new products and services as the competition for customers increases.

At the same time, customers will likely benefit from reduced prices and improved product offerings. For example, in financial services, CDR will further facilitate open banking, enabling FinTech companies to develop innovative, cost-effective products and services.

This means that customer experience will become even more crucial. In an environment where switching providers will be easier, organisations should know their levers for customer retention and satisfaction, be able to measure and improve it.

CDR also leads to opportunities to support by-Māori, for-Māori data initiatives, and improved accessibility and inclusion. The Government's position is that by enabling data portability with the customer's agreement, the draft law creates an opportunity to access data, not only for the customer's direct benefit, but also potentially the collective benefit. For example, individuals could request that specific data about them could be shared with collectives, such as hapū or iwi for governance purposes or initiatives. Māori organisations could consider becoming accredited data requesters, to offer specialist data capability and functionality for Māori groups.

### **Is your current technology customer-centred? Does it enable agile onboarding and offboarding of customers?**

To ensure open data sharing, a technology stack (a set of tools and components used to create a computer application or programme) that supports both business demands and consumer expectations will be needed. Systems will be required to package up and send data to third parties but also receive new client information. Consumer data should be exchanged in a standard format that can be easily processed by a computer so that it is accessible for any business that receives it.

It is also likely that rules will be developed governing how data can be exchanged. New technology may be required to meet these demands.

#### **The problem of legacy technology**

Many organisations, including banks, are operating legacy technology systems. These pose a variety of challenges in relation to CDR. The three main areas for organisations to consider when they are looking to enhance their technology stack are:

- **Security and compliance risk.** Legacy platforms will not be as mature as newer versions when it comes to managing risk and data protection. In the worst cases, it creates a high risk for data breaches and cyber crime.
- **Customer experience.** Older technology stacks can slow down customer interactions and may not be compatible with other operating systems. A technology and systems audit is a great first step towards building the right infrastructure to align with CDR and innovation opportunities.
- **Ongoing compliance cost.** Using manual workarounds and intermediate systems (i.e. equipment that forwards data to a recipient) to help with compliance could increase system costs, reduce employee productivity and lead to higher overall costs to service consumers.

## With more data flowing between organisations, are your security and privacy measures fit for purpose?

How a business navigates data security and privacy is a crucial consideration. Companies must ensure there are controls in place to protect any personal information and how that data is used. This is vital for consumers to maintain confidence in the overall CDR system.

Customer consent is an important factor. Data will only be shared when the customer has provided express and informed consent. Because of this, organisations need to think about types of consent and approaches when they are designing new products. Whether it's customer or product-generated data such as transactional information, there should be a focus on what details are made available and how they will be extracted for a customer.

In addition, organisations must have processes in place to verify that it is the genuine customer who is providing that consent. Businesses must ensure that the consent is informed, valid and comes from the right person.

Cyber security is another priority. Organisations must consider how risks can be mitigated and what extra measures should be applied to safeguard data. The CDR legislation is likely to emphasise the importance of security by introducing rules and safeguard measures which will need to be in place so customer data can be shared.

## All of this is underpinned by good data governance

Data can quickly turn from an asset to a liability if it is not handled appropriately or by the right people. The CDR will give individuals the right to ask for their data. How you handle it, how you share it and what you do with it will be a critical piece of the puzzle. Data governance will help you make sure you are looking after and correctly treating it.

## What sectors will be impacted?

The banking sector is likely to be the first affected by the CDR legislation. Other sectors, such as energy, insurance and health could be the next in line. This follows the Australian approach, where CDR applied to the banking sector first, before being rolled out to the energy sector, followed by telecommunications.

## What can we learn from other countries?

Australia introduced a CDR in 2019. In the United Kingdom, open banking has been in place since late 2017 (open banking is effectively a CDR, however it applies only to the financial services sector).

We can learn from these international experiences to make sure that CDR is fit for purpose in New Zealand. In particular, we can gain insights into consumer behaviour in relation to CDR.

An [independent statutory review](#) of the Australian CDR framework in late 2022 noted that for the majority of consumers, whether or not they use CDR, it will drive new products and services that can make their lives more convenient. The product and services offered in Australia and the United Kingdom include:

- Account aggregation (bringing together account details and savings rates from multiple sources into one app).
- Financial management tools.
- CDR powered lending applications or services. These can assess transaction data in a person's accounts and automate decisions about the affordability of different products.

Examples of tools from the United Kingdom (where open banking has been in place for slightly longer) include:

- A charity donation tool which a customer can authorise to have visibility over their bank account transactions. It can then round up their spending and donate the extra to their chosen charity e.g. for a £18.50 spend at the supermarket, £1.50 could be donated to charity (there are similar tools in place for savings accounts).
- A 'Pay By Link' tool powered by open banking technology and used by small to medium sized businesses. It provides the business with an email and SMS payment link to collect and send payments online and in person. This removes the need for sharing and storing card or account details.



## How PwC can help

We're confident that with our experienced team and our global perspective from countries where CDR has already been implemented, we will be able to support you in your preparations for CDR.

In particular, we can support you with a CDR 'course setter'; a diagnostic tool to review your readiness for CDR, help you scope and prioritise CDR-required activities. Our 'course setter' brings together our specialists from legal, cyber, data, equity, customer experience, technology and compliance to ensure that you are well-positioned to respond to this transformational change.

## Contact us



**Kylie Reiri**  
Partner  
kylie.a.reiri@nz.pwc.com  
+64 210 243 3589



**Robyn Campbell**  
Partner  
robyn.k.campbell@pwc.com  
+64 27 592 1352



**Polly Ralph**  
Director  
polly.k.ralph@pwc.com  
+64 27 374 2031



**Swathi Parikh**  
Director  
swathi.k.parikh@pwc.com  
+64 20 439 9990

