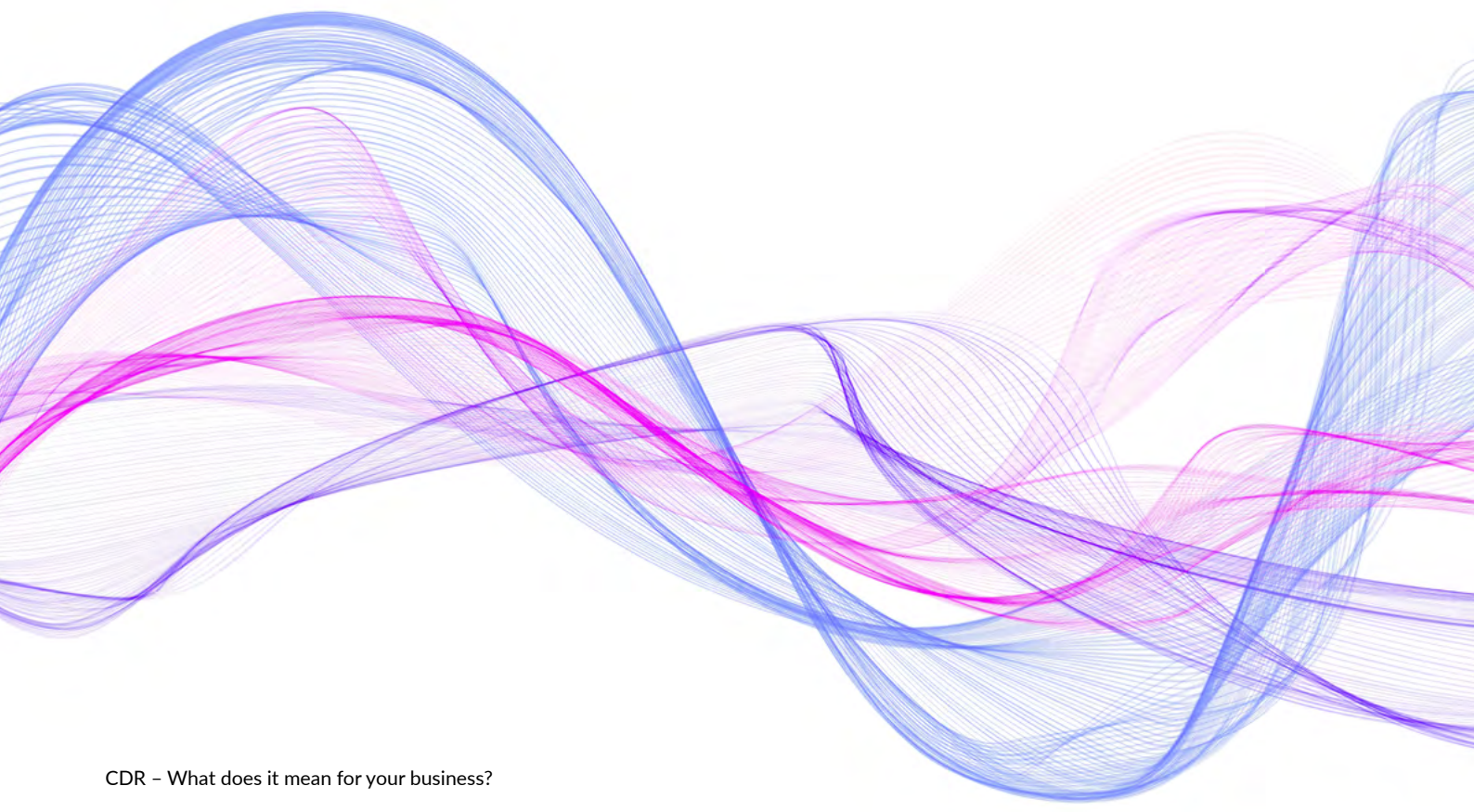
LexisNexis®

# Consumer Data Rights

## What does it mean for your business?

# Contents





## Introduction

In October 2022, LexisNexis Legal Writer Alison Cripps spoke with Melissa Fai and Joy Kim from Gilbert + Tobin. The discussion focused on the progress of Consumer Data Rights since its introduction to Australia in 2017 and what it means for businesses now and in the future. This paper highlights the most salient and practical aspects of that discussion and summarises some of the most important issues you need to be aware of in this complex and changing environment.

## What is CDR?

The Consumer Data Right (CDR) was introduced in response to the Productivity Commission Report on Data Availability and Use. The Report noted that data in the Australian economy was not being fully utilised and expressed concerns about outdated legal and policy frameworks under which data is handled in Australia.

The Government accepted the Report's recommendation to create a right for consumers to request data transfers between entities. They also recognised the need to balance individual privacy and data control and allow businesses to realise the value of data for commercial gain.

The core function of the CDR is to increase competition and improve consumer outcomes. The CDR currently does this by providing a mechanism for data portability for consumers. Under the regime, a consumer can request an incumbent data holder, such as a bank or energy provider, to pass their data on to another entity – an Accredited Data Recipient within the regime. In the future, the CDR regime will also allow consumers to direct third parties (accredited Action Initiators) to initiate actions on their behalf.

> *"CDR is essentially aimed at promoting productivity and competition in the economy, as well as giving consumers the ability to freely transfer their data."*
>
> Melissa Fai, Partner, Gilbert + Tobin

There are currently three main participants in the CDR regime:

1. **Consumers** – individuals & businesses – the people to whom data relates or is identifiable via the data
2. **Accredited Data Recipients** – entities that request and receive data in the CDR regime and hold CDR accreditation
3. **Data Holders** - entities that hold data either on or after the earliest holding date.

In some sectors, there are additional participants such as the energy regulator in the energy sector which plays the role of a designated gateway. In the energy sector, both Data Holders and designated gateways are givers of data.

The CDR is currently "live" in the Banking and Energy sectors, but it is still being rolled out sector by sector across the economy. For each new sector, Treasury will carry out a sectoral assessment. The assessment will analyse what impact the CDR would have on competition, privacy and confidentiality of consumer information, and the likely regulatory impact of a designation.

Treasury will designate a sector based on the recommendation of the sectoral analysis. The designation instrument will set out the data holders and the earliest day for the sector to begin holding CDR data.

*If you are a subscriber to Practical Guidance Cybersecurity, Data Protection & Privacy click here for a detailed overview of the Consumer Data Rights regime in Australia and a timeline of the economy wide roll out of CDR.*

## Accreditation of Data Recipients

Data Recipients must be accredited with the ACCC through the CDR Participant Portal. Once applicants pass the onboarding requirements, they will be accredited as Accredited Data Recipients and will be able to request data on behalf of consumers.

It is important to note, however, that the CDR regime is not exhaustive or all-inclusive; it is an opt-in regime for Data Recipients and does not prohibit other methods of obtaining data, including screen scraping, data arrangements or agreements.

A significant compliance burden comes with being an Accredited Data Recipient. Obligations include:

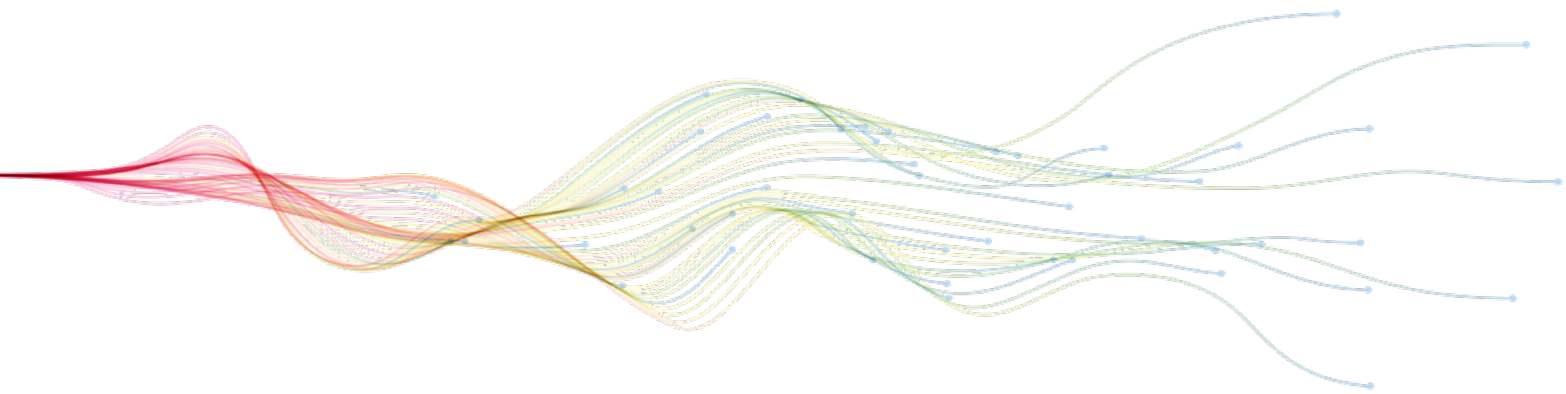
- Complying with consent requirements
- Complying with privacy safeguards
- Maintaining records of transactions & data sharing arrangements
- Providing attestation reports and assurance reports to the ACCC
- Maintaining appropriate insurance and membership with a listed external dispute resolution body
- Compliance with prescriptive data standards set by Data61
- Maintaining appropriate information security controls
- If you have reciprocal Data Holder obligations, you must register as a Data Holder where you will be obliged to share CDR data at the consumer's request.

## Data Holders

The designation instrument determines what entities are Data Holders in any particular sector. However, Data Holders must be registered and must comply any applicable Data Holder obligations. Data Holder obligations include:

- Onboarding systems to the CDR regime
- Transferring consumer CDR data in a standardised machine-readable format
- Publishing general product data about products and services
- Ensuring systems meet relevant service availability and response time metrics (availability 99.5% with response times below one second)
- Some data holders also have legal and IT requirements similar to the obligations of Accredited Data Recipients.

*Practical Guidance Cybersecurity, Data Protection & Privacy has content on the accreditation of data recipients and data holders. If you are a subscriber click **here** to access content on the accreditation of data recipients and **here** to access content on Data Holders.*



## Consumer Consent

The concept of meaningful consumer consent is central to the CDR regime. This is much more prescriptive than the consent requirements for sensitive personal information under the Privacy Act.

Under the CDR, Accredited Data Recipients are required to collect informed consent for the use of CDR data, types of data, and the period over which the data can be collected and used.

The CDR Rules and Consumer Data Standards set out specific categories of consent that accredited persons may seek. There are strict parameters for accredited persons seeking consent and the language used to obtain it. In addition, there is a data minimisation principle in place to ensure that only the data required is collected and only for the time it is needed.

Consent under the CDR must be opt-in and needs to provide consumers with an active choice. This means Accredited Data Recipients cannot use default settings or pre-selected options for consent. In addition, consumers should be able to easily withdraw their consent. Accredited Data Recipients must provide consumers with a clear process to withdraw their consent and this process must be at least as simple as giving consent.

*Subscribers to Practical Guidance  Cybersecurity, Data Protection & Privacy can access more content on consumer consent* ***here****.*



page 6 of 12

## The Privacy Act & Privacy Safeguards

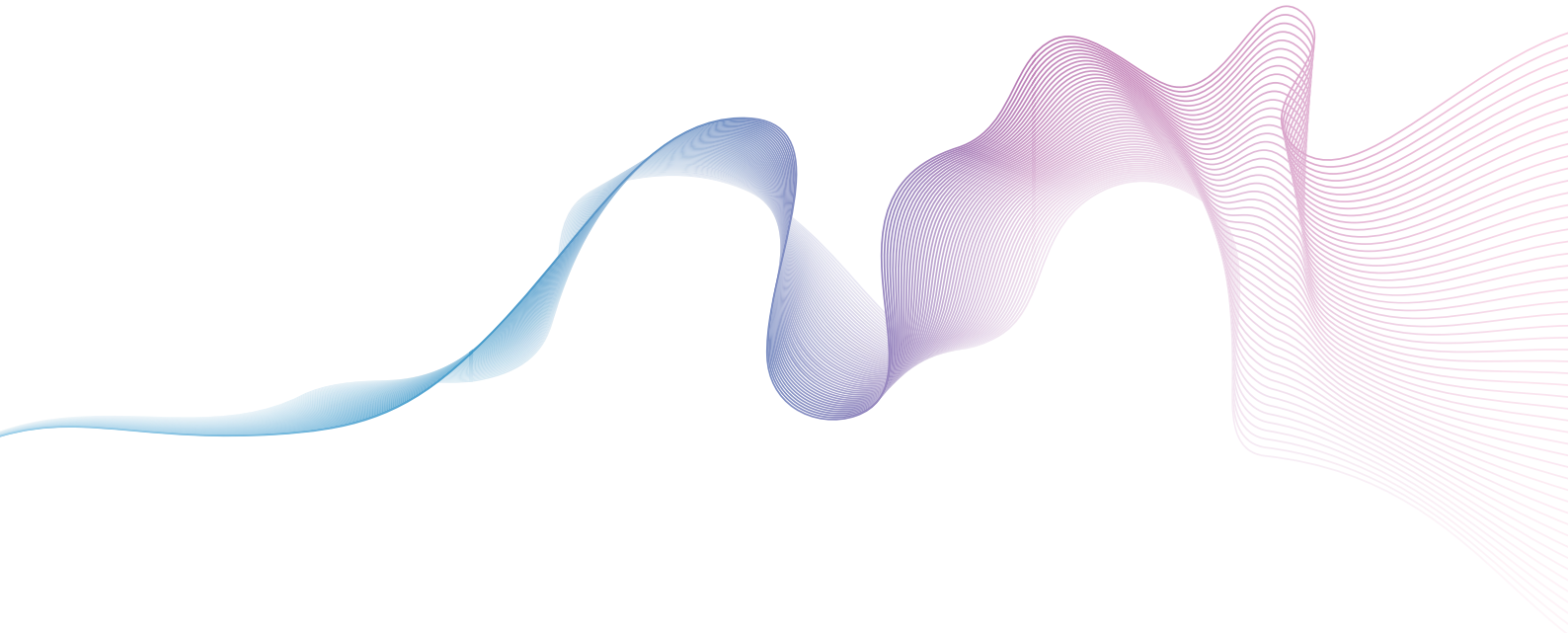
CDR participants must comply with the 13 principles of Privacy Safeguards under the regime. The principles set out the privacy obligations of participants and the rights of consumers when dealing with CDR data.

The principles mirror the Australian Privacy Principles under the Privacy Act but are more prescriptive and cover a broader range of data than just individuals' personal information captured by the Privacy Act.

Privacy Safeguards apply to all CDR data of all CDR consumers, including businesses and individuals who are identifiable or reasonably identifiable from the data. Consumer consent determines what data an entity can collect, use and disclose. Unlike the Privacy Act, consumers must always provide express consent, and if data is disclosed to an accredited person, the consumer must be informed through the consumer dashboards in the CDR Regime.

The CDR regime sits under the Competition and Consumer Act 2010 (CCA) and is subject to the penalties regime under that Act. This means that unlike the Privacy Act, these penalties will apply to any breach, rather than only series or repeated offences. The compliance regime around privacy can be difficult where businesses are subject to both regimes, so careful consideration must be given to how businesses hold their data.

*Subscribers to Practical Guidance Cybersecurity, Data Protection & Privacy can access more content on privacy safeguards* ***here****.*



## Regulations & Penalties

The ACCC and the Office of the Australian Information Commissioner (OAIC) jointly regulate the CDR regime. The ACCC is primarily responsible for consumer and competition outcomes, and the OAIC is primarily responsible for the enforcement of the Privacy Safeguards.

The CDR regime operates on a risk-based approach to compliance, meaning that the regulators focus on breaches with the potential to cause significant harm to the CDR. The regulatory bodies will prioritise matters that provide the most important benefits to consumers.

Both regulators have the power to negotiate administrative resolutions and court-enforceable undertakings, and issue civil penalty orders under the CCA. Because the ACCC is the accrediting body, it can issue infringement notices and suspend or revoke accreditation. The OAIC has additional powers to make determinations and declarations, such as substantiating or dismissing customer breach complaints.

The ACCC can enforce civil and criminal penalties for breaches of CDR obligations. The maximum civil penalty is $2.5 million for individuals and $50 million for corporations, or three times the value of the benefit derived from the breach, or 30% of annual domestic turnover, depending on which is the greater amount. Penalties apply to each violation.

Criminal behaviours such as misleading CDR participants into thinking you are an Accredited Data Recipient when you are not can lead to up to five years imprisonment and a $500,000 fine for individuals.

The ACCC has imposed two fines since the beginning of the CDR regime. The Bank of Queensland paid penalties of $133,200 for failure to provide a data-sharing service by the July 1 cut-off date and ING paid penalties of $53,280 for missing three legislated deadlines and making misleading statements on its website about the reliability and security of its CDR service.

## Breaches & Misconduct

The ACCC and OAIC have listed certain forms of conduct that they consider will result in significant detriment to the consumer and the integrity of the CDR regime.

They include:

- Data holders repeatedly refusing to disclose CDR data and frustrating the CDR process
- Misleading or deceptive conduct
- Intentional misuse or improper disclosure of CDR data
- Not complying with data minimisation principles
- Having insufficient security controls.

"The ACCC is an active regulator, and they are a known litigator. They're very well-practised in enforcement, and they actively seek out cases and actively investigate complaints and behaviours that they consider problematic…" Joy Kim

*If you are a subscriber to Practical Guidance Cybersecurity, Data Protection & Privacy click here to access more on the enforcement of CDR*

## The Future of CDR

The Government has confirmed its economy wide approach for the CDR in its Future Directions report.

The Treasury has finished consultation of the draft CDR rules for the telecommunications sector. The Government envisions that once telecommunications join the banking and energy sectors, it will begin to generate cross-sectoral use to develop new products and services.

The government has announced that the next sector following the Telecommunications sector will be Open Finance. This includes non-bank lending, merchant acquiring services and key data sets in general insurance and superannuation.

There has also been discussion about designating Government held datasets in the near future. Government held data sets are not uniform and the Government agencies holding data cover a range of sectors, which will make the designation of Government held datasets  very different to the frameworks already in place. However,  the Data Availability and Transparency Act (Data Act) which came into force early in 2022 seems to achieve a similar effect as the CDR regime. It authorises and regulates controlled access to Australian Government Data to promote better availability and use of Government data.

In November 2022, the Government introduced a bill to Parliament which would implement Action Initiation. Action Initiation will allow consumers to authorise third parties to act on their behalf and with their consent. For example, consumers may be able to direct Accredited Action Initiators to to make payments and switch accounts on their behalf. There will be a new accrediting body, and Accredited Data Recipients must apply to become accredited Action Initiators.

> “Action initiation is really powerful for empowering customers and helping them get the maximum value out of their data. An example is: An Action Initiator could collect data from your banking, energy and telco accounts and, every six to 12 months, automatically switch your accounts to the best product on the market for you.”

Joy Kim, Lawyer, Gilbert + Tobin

**Melissa Fai**
Partner, Gilbert + Tobin

**Joy Kim**
Lawyer, Gilbert + Tobin

**Alison Cripps**
Legal Writer,
LexisNexis Practical Guidance

## About our expert panellists

**Melissa Fai** is a Partner in the Tech + IP group of Gilbert + Tobin. Melissa is a data and privacy specialist who dedicates a significant part of her practice to regularly advising clients on privacy and data protection compliance obligations and to considering how clients' use of technology and data, and the commercialisation of data, may be structure to meet their legislative requirements and also the best contractual outcome.

**Joy Kim** is a Lawyer in the Tech + IP group of Gilbert + Tobin. She previously worked at the Australian Competition and Consumer Commission (ACCC) on the CDR Compliance and Enforcement Team and was involved in developing the CDR Participant Portal and and Enforcement Policy.

**Alison Cripps** is a Legal Writer for Practical Guidance Cybersecurity, Data Protection & Privacy. She has worked at leading international and national firms including Allens, Henry Davis York, and Maddocks. Alison has developed a passion for cybersecurity, data protection and privacy law. She has particular interest in cybersecurity strategy as well in the organisational management of privacy and data security breaches.

Practical Guidance Cybersecurity, Data Protection & Privacy is an invaluable guide for practitioners preparing to advise on data privacy and cybersecurity matters as well as the digital economy in today's rapidly changing legal landscape.

This module will help you follow best practice in relation to data security, mandatory data breach notification, transfer of data, cybersecurity strategy, privacy, emerging technology, EU General Data Protection Regulation (GDPR), China's Personal Information Protection Law (PIPL), Consumer Data Rights, Freedom of Information, digital currency and blockchain and international content.

*Stay ahead of the market with Practical Guidance Cybersecurity, Data Protection & Privacy. To find out more and trial the module for free click here.*

LexisNexis®



**Legal Advice disclaimer** All information provided in this document is general in nature and is provided for educational purposes only. It should not be construed as legal advice. For legal advice applicable to the facts of your situation, you should obtain the services of a qualified solicitor licensed to practice in your state/territory. Information contained in this report is current as at 15 February 2023

NF112022MS