



## What is the Consumer Data Right?

The Consumer Data Right (CDR) provides 'CDR consumers' (both individuals and businesses) with a right to access, and direct data holders to provide to accredited third parties ('accredited data recipients' or ADRs), information held about that consumer by a data holder. The CDR regime, through the implementation of stringent rules and standards, is intended to ensure that this information is accessed in a safe, effective and efficient manner, and can be transferred, as directed by CDR consumers, to ADRs.

The CDR regime aims to give CDR consumers control

over certain data held about that person, recognising the value and utility of data as an asset which has previously been accessible only by organisations that collect CDR consumers' data.

One of the key policy drivers for the CDR regime is to provide a framework which encourages competition between service providers. The CDR regime promotes the creation of innovative and improved ancillary services and applications developed through the use and exploitation of new or different data sets accessible by ADRs under the CDR regime. Decoupling services

and data will enhance CDR consumer convenience as unbundled data can be more easily shared between companies to facilitate transactions or customer portability. The CDR will also promote the development of niche service offerings and accelerate digitisation on a broader scale.

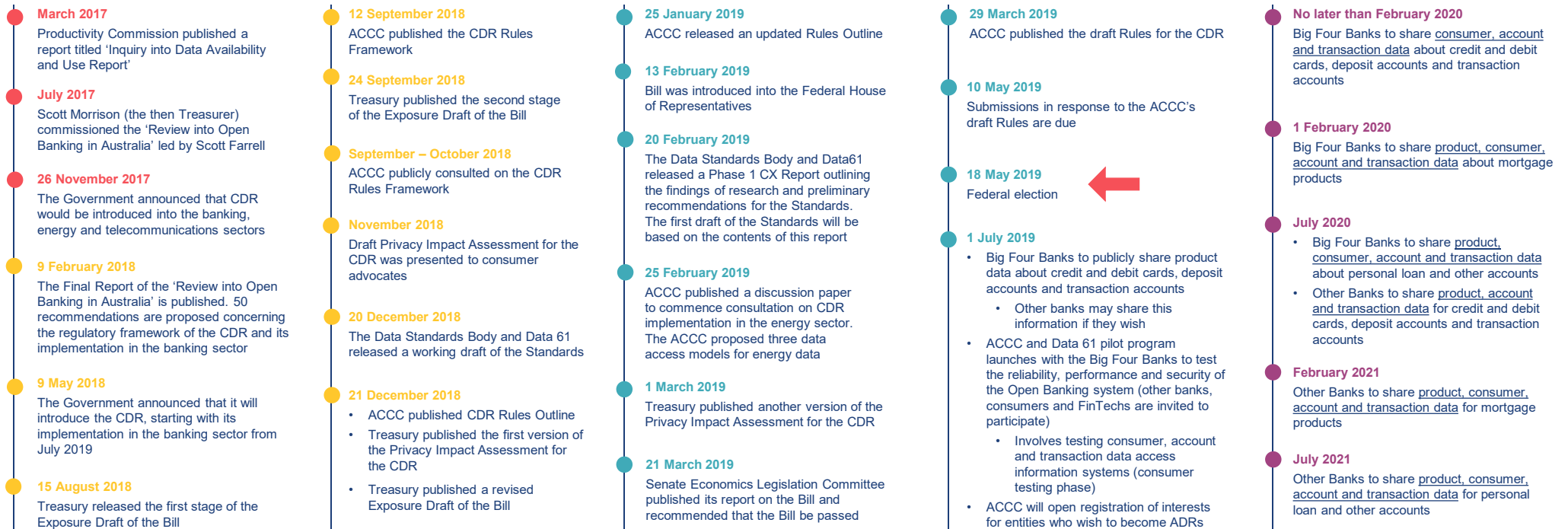
The CDR framework is created through legislation that establishes the basic principles and structures of the regime (through an amendment to the *Competition and Consumer Act 2019* (Cth)), rules developed by the ACCC that can adapt to changes in the digital economy

(Rules), standards developed by the Data Standards Body and Data61 (Standards), and Privacy Safeguards. These four regulatory elements are currently in the process of being implemented in Australia.

'Open Banking' (OB) is the term used to describe the first application of the CDR regime in the banking sector. Under 'Open Banking', 'read access' will be granted to ADRs as directed by CDR consumers. 'Write access' may be included in the future.



## An overview of CDR in Australia





# Consumer Data Right: Briefing and State of Play



## The road so far

- **2016 / early 2017:** Beginning of concrete conversations on creation of a CDR regime in Australia
- **9 May 2018:** Australian Government announced that the CDR will be introduced, initially to the banking sector from July 2019
  - Public consultation run by Treasury, the Data Standards Body and the ACCC on OB regulatory instruments occurred both before this date and throughout 2018
- **21 December 2018:** Go-live date of OB delayed to allow for more consumer and market testing
- **March 2019:** Senate recommends that the Treasury Laws Amendment (Consumer Data Right) Bill 2019 (the Bill) be passed. ACCC published its draft Rules
- **July 2019:** Consumer testing anticipated to commence
- **End of 2019 / early 2020:** Projected that OB will go-live



## Recent updates

The Senate Economics Legislation Committee published its Report on the Bill on 21 March 2019, in which it recommended that the Bill be passed. The ACCC also published its draft Rules on 29 March 2019, for which submissions could be made. These recent developments indicate the Australian Government's general commitment to finalise the CDR framework within the stated timeline. Despite these recent updates, we are still awaiting publication of the draft Standards.

There is still a significant amount of detail and guidance on the regime which needs to be settled. Businesses have begun exploring and understanding how the scheme will operate in practice and how they will navigate the interaction between different components of the framework and the CDR regime's interaction with other existing regulatory requirements (for example, the interplay between the Privacy Safeguards in the Bill and the Australian Privacy Principles (APPs)). It remains to be seen if these interactions will be further clarified as the framework is developed. However, given the timelines for compliance and potential opportunity, businesses should proactively engage with the material currently available to prepare for CDR implementation, adjust their strategy and potentially start developing new product offerings.

The Bill was not passed in the recent April Parliamentary sitting. This was ever-important given the looming 1 July 2019 timeline, by which the Big Four banks are required to make available the first tranche of product data. This timeline may pose difficulties in light of the Federal election on 18 May 2019, as well as the fact that Labor has suggested that the Bill should not be passed in its current form. If Labor win the upcoming election, it is likely that the CDR regime's implementation will be delayed to allow time for further consideration of key issues.

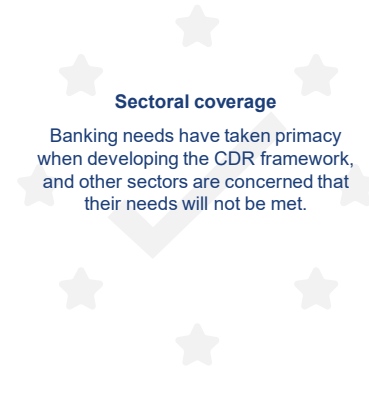
### Key takeaways

- It is unclear if the Bill will be passed in its current form, especially if Labor win the upcoming Federal election.
- Businesses can engage with the draft Rules to determine the appropriateness of the Rules and if their planned product offerings meet the requirements.
- A significant amount of detail is still needed to demonstrate how the scheme will effectively operate in practice.



**Privacy protections**

Understanding the interaction between the APPs and Privacy Safeguards will challenge businesses and require development of strict data management practices and procedures.



**Sectoral coverage**

Banking needs have taken primacy when developing the CDR framework, and other sectors are concerned that their needs will not be met.



**Accreditation requirements**

A single tier of accreditation may pose difficulties for new entrants.

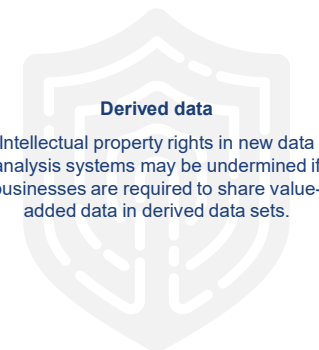


**Informed consent**

An effective mechanism to obtain voluntary, express and informed CDR consumer consent needs to be developed.

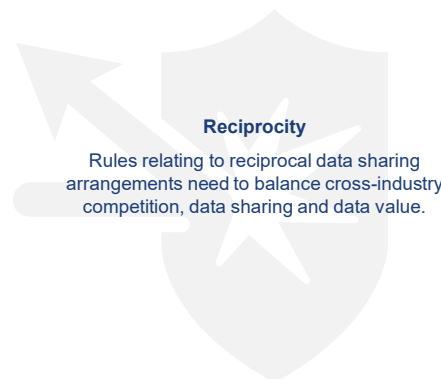


**CDR Issues Toolkit**



**Derived data**

Intellectual property rights in new data analysis systems may be undermined if businesses are required to share value-added data in derived data sets.



**Reciprocity**

Rules relating to reciprocal data sharing arrangements need to balance cross-industry competition, data sharing and data value.



**Data fees**

New market entrants may be disinclined to participate in the CDR regime if they have to pay large fees to access specific data sets.



## CDR background brief

### Privacy protections

The APPs are a set of well-established privacy principles which govern how personal information may be collected, disclosed, used, handled and stored by businesses.

The Bill introduces a new, more stringent set of Privacy Safeguards as part of the CDR regime which is intended to operate as a separate legislative regime applicable to CDR data relating to an identifiable CDR consumer. The Privacy Safeguards expand privacy protections to data that may not currently be protected by the APPs, including by extending its protections to small businesses.

Businesses will need to navigate the complex interaction between the two privacy regimes, with these regimes operating concurrently in certain cases or being substituted in others. The different role that organisations play in the CDR regime will dictate how data must be managed. Additionally, if a business is required to comply with the EU General Data Protection Regulation, businesses may need to ensure they develop data management policies that satisfy the three different regimes as required. Ideally, further guidance from Treasury will be issued to enable businesses to navigate the interaction and ensure the right systems and processes are in place.

### Sectoral coverage

Stakeholders from industries outside of the banking sector have expressed concern that the CDR regime has been developed with a focus on the banking sector, without considering how this regime will be implemented in other sectors. The implemented CDR regime in an OB context is likely to have a precedential impact on the CDR's implementation in other sectors. However, there will be significant differences in the energy and telecommunications sectors because these sectors are already governed by considerable consumer and data regulatory requirements.

In response to these sectoral differences, the ACCC has commenced consultation on CDR implementation in the energy sector. The ACCC has proposed three data access models for energy data, and has sought stakeholder feedback on these models. Until the ACCC provides more guidance, it remains unclear how these requirements will interact with the CDR regime, and whether changes will need to be made to those complementary and coexisting regulatory regimes when the CDR is introduced in the energy sector.

### Accreditation requirements

All businesses that wish to receive data must be accredited by the 'Data Recipient Accreditor'. The draft Rules currently only provide for a person to be an 'unrestricted' ADR, which requires the 'Data Recipient Accreditor' to be satisfied of the following criteria:

- the relevant business or individual is fit and proper to manage CDR data;
- CDR data management and information security policies exist and are adhered to in a manner that appropriately manages associated risks;
- internal dispute resolution procedures compliant with the Rules are in place;
- the relevant business or individual is a member of a recognised external dispute resolution scheme in relation to CDR consumer complaints; and
- evidence of adequate insurance (or comparable guarantee) to recompense for certain losses relating to breach of CDR data management obligations.

The rigorous accreditation process reinforces the requirement that data recipients must be trusted third parties, but there are arguments that different levels should apply depending on the relevant risk profile. These rigorous requirements may operate as prohibitive hurdles for some new market entrants, reflecting the balance that needs to be struck between protection of consumer data and the CDR policy objectives of encouraging competition. It is yet to be seen whether and when different accreditation levels will be introduced into the regime, and how a tiered structure may work in practice.

### Informed consent

The CDR regime is premised on CDR consumers providing voluntary, express, informed, and time limited consent. Consumer consent needs to be specific as to its purpose, and must be able to be withdrawn at any time. A key concern is ensuring that CDR consumers do not just click 'accept', without understanding the consequences. However, stakeholders have grappled with how this consent can effectively be provided.

In its draft Rules, the ACCC has included specific provisions about how consent to collect CDR data will need to be acquired, as well as consent for ADRs to use CDR data. For example, to monitor the consents provided, each CDR consumer will have a dashboard that tracks what consents they have provided and/or withdrawn, and with respect to whom. It is yet to be seen how this will work in practice, and whether this approach will be effective to establish voluntary, express, informed and time-limited consent. Limited consent periods will also be introduced to ensure consumers remain informed of what consent they have provided. ADRs have expressed concern about how they will satisfy this requirement and effectively re-obtain consent from CDR consumers.

### Derived Data

CDR data is defined in the Bill to include data 'directly or indirectly derived'. It is currently unclear whether companies will be required to disclose data that they have created, derived, re-organised or otherwise added value to from 'base' CDR data (e.g. banking transaction history data that has been grouped into different purchase categories or used to create new data that predicts consumer behaviours). The regulatory regime arguably undermines the ADRs' intellectual property and other proprietary rights in such derived data, and could function as a disincentive for businesses investing in innovation and data analysis and AI tools that analyse and create modified data sets.

Data sets, including derived data, will be explicitly stated in the designation instruments – accordingly, until the designation instruments are published, it is unclear what extent value-added data will be captured in the data sets. Whether the designation of derived data operates effectively as a barrier to competition by disincentivising investment in CDR-driven technologies remains to be seen.

### Reciprocity

When defining 'data holder' the Bill introduces the concept of 'reciprocity'. Specifically, the Explanatory Memorandum for the Bill notes that if an entity wishes to become accredited and receive CDR data, the entity must also be willing to share CDR data already received, and 'equivalent' data when requested by a CDR consumer to do so. For ADRs that do not primarily operate in designated CDR sectors (such as technology companies), the ACCC will, as part of the accreditation process, likely have to define which data sets are 'equivalent' to designated CDR data sets. What is considered to be an 'equivalent' data set must be appropriately defined in order to realise the true benefit of reciprocity.

Reciprocal data sharing arrangements have the potential to blur sectoral divides where innovative businesses subject to the CDR regime use reciprocal data sets to expand their product offering in other verticals, ultimately advancing a policy objective of the CDR regime to provide consumers with more choice. Without effective reciprocity principles, there is a risk of 'platform envelopment' that the CDR will strengthen dominant players even more, cutting across the objective that the CDR regime will promote competition. However, if the scope of 'equivalent' data is too broad, engagement with the CDR regime by ADRs may be discouraged if ADRs are required to share broad sets of their valuable data.

Beyond navigating this fine balance, if 'equivalent' data sets are not clearly defined, ADRs may struggle to identify and access, and have appropriate systems and processes in place to identify and access, the data sets that they are obligated to share, particularly if ADRs have modified the data that they originally received.

Unfortunately, much-needed guidance on how reciprocity will operate in practice was not provided in the recent draft Rules. More clarity is needed in this space to fully realise the importance that reciprocity plays in the CDR regime.

### Data fees

The Minister will have discretion to specify which CDR data sets businesses can charge for access to. The ACCC's recent draft Rules indicate that fees cannot be charged for product data and consumer data. However, the framework does not provide concrete guidance on what data sets CDR consumers will have to pay for before they are transmitted to other ADRs, and if so, what fees will or can apply.

Accordingly, this lack of clarity leaves potential new market entrants uncertain about whether the payment requirements will prohibit their anticipated entry.

## Key contacts



**Julian Lincoln**  
Partner  
T +61 3 9288 1694  
M +61 419 685 104  
julian.lincoln@hsf.com



**David J Ryan**  
Senior Associate  
T +61 3 9288 1831  
M +61 479 048 290  
david.j.ryan@hsf.com



**Annalisa Heger**  
Special Consultant  
T +61 3 9288 1523  
M +61 447 635 330  
annalisa.heger@hsf.com



**Kaman Tsoi**  
Special Counsel  
T +61 3 9288 1336  
M +61 412 687 842  
kaman.tsoi@hsf.com



# Key CDR concepts



## ACCC or Australian Competition & Consumer Commission

The ACCC is the lead regulator for the CDR regime with the power to make consumer data rules with general, and sector-specific, application.



## ADR or Accredited Data Recipient

A person that satisfies the accreditation criteria outlined in the Rules, and is subsequently able to receive CDR consumer and product data.



## API or Application Programming Interface

An API is a set of public functions and properties that allows one software application to plug-in to others.



## APPs or Australian Privacy Principles

The APPs are a set of privacy principles in the *Privacy Act 1988* (Cth) that regulate the collection, disclosure, handling, use, storage and management of personal information.



## CDR or Consumer Data Right

The CDR provides CDR consumers with a right to access, and direct data holders to provide to ADRs, information held about that consumer by data holders.



## CDR consumer

Individuals and businesses that disclose information or data that may be subject to the CDR regime.



## Data holder

A business that collects and stores information about CDR consumers.



## Data Standards Body

Advisory committee that provides guidance and advice on the development and implementation of technical standards to support consumer data sharing.



## Data Recipient Accreditor

The body that certifies a person as an ADR if the person satisfies the accreditation criteria.



## Data 61

CSIRO's data innovation research group.



## Designated sector

The economic sectors that the Minister (Treasury) designates will be subject to the CDR regime.



## Designation instrument

The instrument that the Minister publishes to announce a new designated sector.



## GDPR or General Data Protection Regulation

A regulation in EU law on data protection and privacy for all individuals within the European Union and the European Economic Area.



## OB or Open Banking

The term used to describe the application of the CDR regime to the banking sector.



## Privacy Impact Assessment

A methodical assessment of a project, business or strategy that enables organisations to recognise privacy risks for individuals, and identify how to manage, reduce or remove those risks.



## Privacy Safeguards

Privacy principles introduced as part of the CDR regime that protects CDR data relating to an identifiable CDR consumer.



## Read access

The ability to access files and directories to read information, but not the ability to change information.



## Write access

The ability to access and change information in the files and directories.