COLIN BIGGERS & PAISLEY LAWYERS

THE NEW CONSUMER DATA RIGHT AND THE OPEN BANKING REGIME

September 2019

THE NEW CONSUMER DATA RIGHT AND THE OPEN BANKING REGIME

By Toby Blyth and Jessica Yazbek

In brief - Following the 2017/18 Budget, the Federal Government introduced what has become the CDR (Consumer Data Right).

Toby Blyth
Partner
+61 2 8281 4440
toby.blyth@cbp.com.au

Jessica Yazbek
Paralegal
+61 2 8281 4927
jessica.yazbek@cbp.com.au

The New Consumer Data Right

The CDR aims to provide consumers with rights to direct a business to transfer data on the consumer to a third party in a useable, machine readable form as well as to provide product data to facilitate an economy wide consumer directed data transfer system and reduce barriers to change of suppliers, thereby increasing consumer rights and competition.

The main aim is to allow consumers to switch service providers and services (for example bank accounts or energy providers) in an easy way without any of the friction cost involved to date. For example, automatic bill paying and direct debiting arrangements make it cumbersome for the average consumer to switch bank accounts. That has led to a sticky customer relationship and reduced competition and innovation.

The CDR will require new thinking from those in designated services and likely lead to innovative disaggregated intermediaries, especially on app-based architecture in an ever deepening IoT environment.

The government has determined that the CDR will be immediately targeted at the banking sector, with the energy and telecommunications sectors to follow. Ultimately, the law will be introduced sector by sector broadly across the economy.

The CDR mirrors the data portability right in GDPR Article 20, which suggests that Australia is moving closer to the EU conception of privacy in certain areas.

With opportunity comes risk - the right will increase the move to tech-heavy solutions and inevitably engage information and privacy risks. Understanding the regulatory framework is crucial for business with new regulatory roles for current regulators and a new regulatory body.

In this outline we extract useful guidance from the legislation to set out a high level overview of how the CDR system works.

Treasury has provided a useful summary of the scheme.

CONSUMER DATA RIGHT SUMMARY

- The Government will introduce a Consumer Data Right as part of its commitment to giving Australians greater control over their data.
- Australians will have greatly improved access to their own data in a usable form and be able to direct its secure transfer to trusted third parties.
- Australians will also have better access to data on key goods and services on offer to them.
- Both individual and business customers will be able to exercise the right in respect of data relating to them.
- The Consumer Data Right will commence in the banking sector (where it is called 'Open Banking' followed by the energy and telecommunication sectors. The right will then be rolled out economy-wide on a sector-by-sector basis.
- Data initially made available under Open Banking will be provided without charge.
- Improved consumer control over their own data will support the development of better and more convenient products and services, customised to individuals' needs.
- Better price comparison services, which consider consumers' actual usage, will help consumers to save money by securing better banking, electricity and internet service deals.
- Improved competition and data-driven innovation will support economic growth and create new high value jobs in Australia.
- High levels of privacy protection and robust information security will be a core feature of the system.
- Only accredited trusted service providers will be allowed access to data.
- The Government has provided funding of $90 million over five years to ensure that the Consumer Data Right will be backed by well-funded regulators with strong enforcement powers.
- Implementation of the Consumer Data Right has been informed by the findings of the Report of the independent Review into Open Banking in Australia.
- Open Banking will begin with a phased implementation from July 2019.

What about the Australian Privacy Principles?

There are obvious similarities and overlaps with the APP and, in particular, APP12, which deals with the right of access to personal information held in respect of a person.

Treasury has provided an overview of the relevant regulatory oversight regime delineating areas of responsibility:

Australian Competition and Consumer Commission (ACCC)	Office of the Australian Information Commissioner (OAIC)	Data Standards Body
The ACCC will advise the Treasurer which sectors should be designated. The ACCC will have rule-making responsibilities setting out the required functionality of the right in each sector. In setting rules, the ACCC will consult with the OAIC, the public, and sector specific regulators. The ACCC will set accreditation criteria and processes for data recipients, and manage the accreditation register. The ACCC will certify technical Data Standards as meeting the requirements for the right. The ACCC will take enforcement action in relation to serious or systematic breaches of the Consumer Data Right in line with its enforcement policy.	The OAIC will advise the Treasurer on the privacy impacts of designating a sector. The OAIC will advise the ACCC on privacy impacts on proposed rules. The OAIC will be involved in standards setting to ensure standards meet privacy protections. The OAIC will have primary responsibility for complaint handling. The OAIC will be the first port of call for consumer complaints. They will handle complaints from individuals and small to medium sized enterprises or direct them as applicable to the relevant external dispute resolution body, ACCC or other regulator.	The Data Standards Body will set technical standards relating to transmission of data, data format and security of data. These standards may be tailored to the designated sector. The standards will be formed in consultation with working groups. This function will be performed by Data61 for three years, during which there will be a review of the arrangement.

The statutory framework

The main legislative framework is brought about by amendments to the *Competition and Consumer Act 2010.*

The flowcharts and summaries in the legislation and the rules demonstrate how the scheme works.

The Rules will:

a. enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed to themselves or to accredited persons; and

b. enable any person to be disclosed information in those sectors that is about goods (such as products) or services, and does not relate to any identifiable, or reasonably identifiable, consumers; and

c. may require these kinds of disclosures, and other things, to be done in accordance with data standards.

A register is to be kept of accredited persons.

Privacy safeguards apply. These mainly apply to accredited persons who, under those rules, are disclosed information relating to identifiable, or reasonably identifiable, consumers.

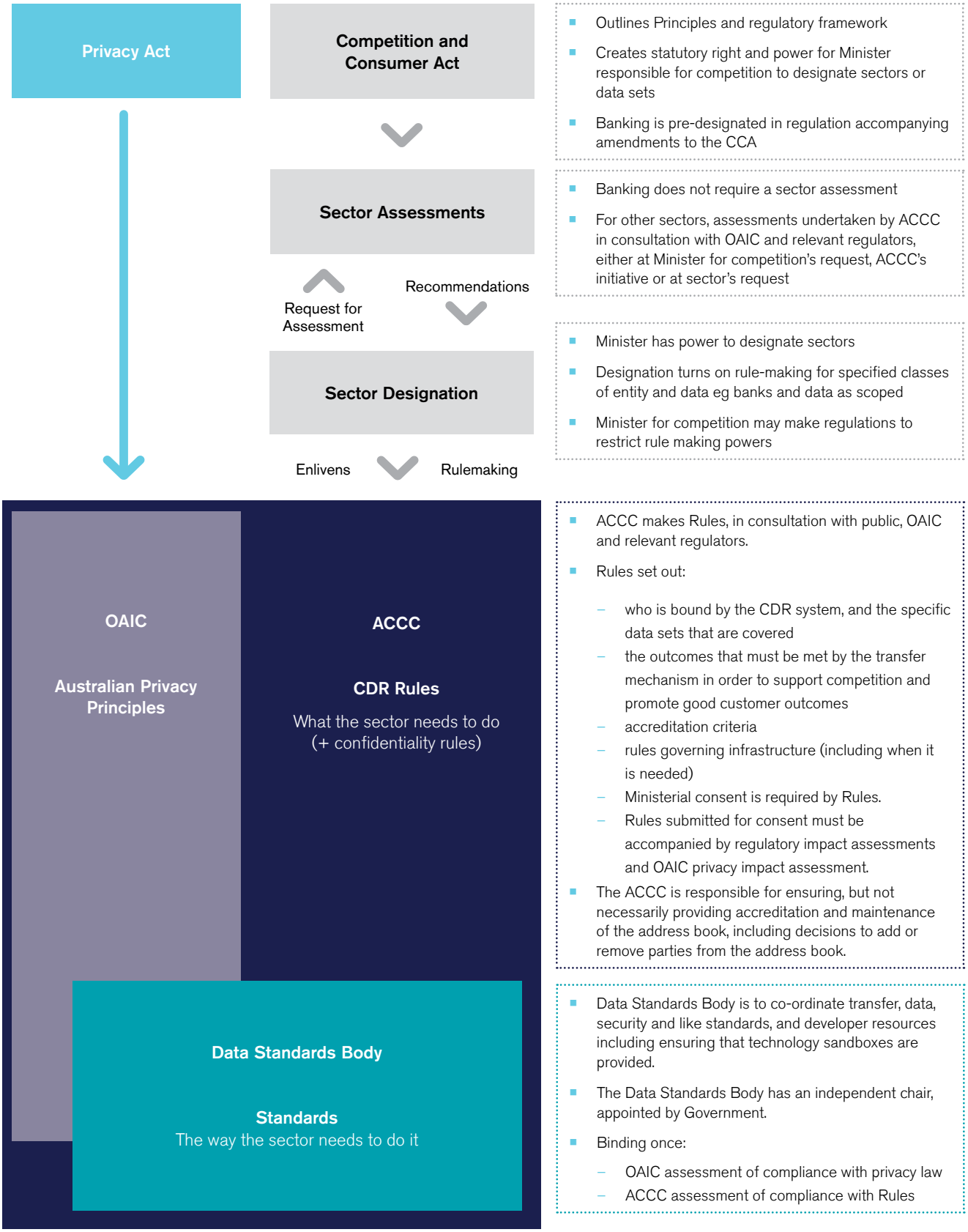
Other penalties and civil and class actions

The Act also enables civil penalties and permits actions for damages by consumers.

It is too early to assess the effect of any "deterrent" effect from the penalties and possible actions, although we expect to see an increase in privacy and data related class actions generally.

How does a sector get designated?

Treasury sets out how the legislation will provide for the review and designation of sectors as follows:



Open Banking Regime

Consumer finance was chosen as the first industry to bring in the CDR in the form of Open Banking, but the relevant reviews and legislation have been designed to keep interoperability between sectors in mind.

The CDR will also be able to work in other different sectors of the economy, for example, energy and telecommunications and those sectors will be introduced over time (once the Open Banking Regime has been established).

What banking data must be provided?

The banking sector designation instrument specifies the following information:

1. Information about the user of the product. The first type of information is 'customer' information. This is information about the person to whom the product has been, or is being supplied, or the person's associate where the product has also been, or is also being supplied to the associate. The information must have been either:
    a. supplied directly by the person or their associate when acquiring or using a product, for example, the person's name and address; or
    b. otherwise obtained by the ADI (or the entity that holds data on the ADI's behalf). For example, this may include information that an ADI has received from another ADI with the consent of the relevant customer.
2. Information about the use of the product by the person or an associate of the person. This includes the type of information that a customer would typically see on a statement, such as the balance of their account, debits and credits on the account and when these occurred, and to whom payments were made. Information on the use of a product also includes information on the authorisations attached to a product. For example, persons who are authorised to use, access or view information about the account, or an authorisation to make a payment to a third party. However, the Designation limits the information about the use of the product where this information has been materially enhanced as a result of analysis or insight by the provider.
3. Information about a product. This includes information that identity's or describes a product, the price of a product such as fees and charges or interest rates, terms and conditions and eligibility criteria that a customer needs to meet to be provided with the product. The product information can be about a certain type of product for a particular customer or group of customers, such as savings accounts for students or retirees.
4. Information that is not information about the user of a product. The Bill amends the *Privacy Act 1988* to exclude the CDR and associated subordinate legislation as an Australian law that would permit the use or disclosure of credit reporting information or credit eligibility information. Designation excludes the following information from the CDR:
    a. a statement that an information request has been made for the individual by a credit provider, mortgage insurer or trade insurer (consistent with paragraph 6N(6) of the *Privacy Act 1988*);
    b. new arrangement information about serious credit infringements (consistent with subsection 6S(2) of the *Privacy Act 1988*);
    c. court proceedings information about the individual (consistent with paragraph 6N(i) of the *Privacy Act 1988*);
    d. personal insolvency information about the individual (consistent with paragraph 6N(j) of the *Privacy Act 1988*); and
    e. the opinion of a credit provider that the individual has committed a serious credit infringement (consistent with paragraph 6N(l) of the *Privacy Act 1988*).
5. Information that materially enhances which is not subject to CDR. Section 10 carves out information about the use of a product which might otherwise be designated by section 7 where that data has been materially enhanced.

The Rules

Each sector that is designated will be designated via rules.

The first set of draft rules have been issued in respect of ADIs by virtue of the banking sector designation dated 4 September 2019.

How to request CDR data?

Consumer data requests made by CDR consumers

A CDR consumer who, in accordance with a Schedule to these rules, is eligible to do so may directly request a data holder to disclose CDR data that relates to them. Such a request is called a consumer data request.

A consumer data request that is made directly to a data holder is made using a specialised online service provided by the data holder. The data is disclosed, in human-readable form, to the CDR consumer who made the request.

Consumer data requests made on behalf of CDR consumers

A CDR consumer who, in accordance with a Schedule to these rules, is eligible to do so may request an accredited person to request a data holder to disclose CDR data that relates to the consumer. The request made by the accredited person is called a consumer data request.

A consumer data request that is made on behalf of a CDR consumer by an accredited person must be made in accordance with relevant data standards, using a specialised service provided by the data holder. The data is disclosed, in machine-readable form, to the accredited person.

Under the data minimisation principle, the accredited person may only collect and use CDR data in order to provide goods or services in accordance with a request from a CDR consumer.

These rules only apply in relation to certain classes of product and consumer CDR data that are set out in Schedules to these rules which relate to different designated sectors. Schedule 3 relates to the banking sector. Initially, these rules will apply only in relation to certain products that are offered by certain data holders within the banking sector. These rules will then apply to a progressively broader range of data holders and products.

Product data requests

Any person may request a data holder to disclose CDR data that relates to products offered by the data holder. Such a request is called a product data request.

A product data request is made in accordance with relevant data standards, using a specialised service provided by the data holder. Such a request cannot be made for CDR data that relates to a particular identifiable CDR consumer. The data is disclosed, in machine-readable form, to the person who made the request. The data holder cannot impose conditions, restrictions or limitations of any kind on the use of the disclosed data.

Consumer Data Requests

Consumer data requests that are made to data holders by accredited persons on behalf of CDR consumers by using the data holder's accredited person request service.

In order for such a request to be made, the CDR consumer must have first asked the accredited person to provide goods or services to the CDR consumer or to another person, where provision of those goods or services requires the use of the CDR consumer's CDR data.

Before making a consumer data request on behalf of a CDR consumer, the consumer must first have consented to the accredited person collecting and using specified CDR data to provide the requested goods or services.

Subject to certain limitations, the requested data can be any CDR data that relates to the CDR consumer.

Collection and use of CDR data under this Part is limited by the data minimisation principle.

A request may be for the CDR consumer's required consumer data, their voluntary consumer data, or both. The rules:

- provide for what is required consumer data and voluntary consumer data for the banking sector; and
- set out the circumstances in which CDR consumers are eligible in relation to a request for their banking sector CDR data.

Subject to exceptions, the data holder:

- must, subject to an exception outlined in this Part, seek the CDR consumer's authorisation to disclose required consumer data; and
- may, but is not required to, seek the CDR consumer's authorisation to disclose voluntary consumer data.

The data holder then must disclose, to the accredited person, the required consumer data it is authorised to disclose, and may (but is not required to) disclose the voluntary consumer data it is authorised to disclose. The data is disclosed in machine-readable form and in accordance with the data standards.

A fee cannot be charged for the disclosure of required consumer data, but could be charged for the disclosure of voluntary consumer data.

Requirement to Create Dashboards and Consumer Data Request Services

Data holders must make available online services that can be used for:

a. product data requests by consumers;

b. the provision of requested data to be disclosed in machine readable form.

Accreditedpersons (ie those who are authorised to receive consumer data) must also have a dashboard that allows CDR consumers to manage their requests and associated consents to collection and dealing with new CDR data.

Importantly, the requirement only seems to be available online. How this will affect less technologically literate, or lower socio-economic status Australians appears not yet to have been considered.

Where a CDR consumer makes a data request

A CDR consumer who is eligible to do so makes a consumer data request to a data holder via the data holder's direct request service.

For any required consumer data, the data holder must (unless covered by an exception) disclose the requested data to the CDR consumer.

For any voluntary consumer data, the data holder may (but is not required to) disclose the requested data to the CDR consumer.

In either case, the data is disclosed through the data holder's direct request service.

Where an Accredited Person makes a data request

The following is a flowchart for how an accredited person makes a consumer data request under this Part:

A CDR consumer has requested an accredited person to provide goods or services, which require the use of the CDR consumer's CDR data.

The CDR consumer consents to the accredited person collecting and using certain specified CDR data.

The accredited person makes a consumer data request, on the CDR consumer's behalf, to the data holder using the data holder's accredited person request service.

For any required consumer data, the data holder must (unless covered by an exception) ask the CDR consumer to authorise disclosure of the requested data.

For any voluntary consumer data, the data holder may (but is not required to) ask the CDR consumer to authorise disclosure of the requested data.

The data holder then must disclose, to the accredited person, the required consumer data it is authorised to disclose, and may disclose the voluntary consumer data it is authorised to disclose.

In either case, the data is disclosed through the data holder's direct request service.

The accredited person may use and disclose the CDR data it collects, in accordance with the Act and these rules, to provide the requested goods and services to the CDR consumer.

What is the difference between required and voluntary consumer data?

Required consumer data is a certain kind of CDR data for which:

1. there are one or more CDR consumers;
2. within the class of information specified in the banking sector designation instrument;
3. customer data in relation to a CDR consumer;
4. held by the data holder in a digital form.

Voluntary consumer data is CDR data for which there is a CDR consumer for CDR data and is not required consumer data.

In effect, voluntary consumer data will be standard non-personal product and services information based on consumer behaviour that will allow customers to compare the products and services offered by different businesses.

The data minimisation principle

Data holders must comply with the data minimisation principle.

The accredited person may only collect and use CDR data in order to provide goods or services in accordance with a request from a CDR consumer.

An accredited person:

a. must not collect more data than is reasonably needed in order to provide the requested goods or services; and
b. may use the collected data only as consented to by the consumer, and only as reasonably needed in order to provide the requested goods or services.

Product data requests

Product data is standard non-personal product and services information that will allow customers to compare the products and services offered by different businesses.

The rules relating to product data requests

Consumer data requests that are made directly by eligible CDR consumers to data holders are made using the data holder's direct request service.

A request may be for the CDR consumer's required consumer data, their voluntary consumer data, or both.

The rules:

- provide for what is required consumer data and voluntary consumer data for the banking sector; and
- sets out the circumstances in which CDR consumers are eligible to request their banking sector CDR data.

When validly requested, a data holder:

- must, subject to an exception outlined in this Part, disclose required consumer data; and
- may, but is not required to, disclose voluntary consumer data.

In either case, the data is disclosed to the CDR consumer who made the request, in human-readable form and in accordance with the data standards.

A fee cannot be charged for the disclosure of required consumer data, but could be charged for the disclosure of voluntary consumer data.

The following is a flowchart for how product data requests are made:

Person makes a request for product data using a data holder's product data request service.

For any required product data, the data holder must (unless covered by an exception) disclose the data to the requester.

For any voluntary product data, the data holder may, but is not required to, disclose the data to the requester.

In either case, the data is disclosed through the data holder's product data request service.

What is the difference between required and voluntary product data?

Required product data is a certain kind of CDR data for which:

1. there are no CDR consumers; and
2. where the CDR data is about the eligibility criteria, terms and conditions, price, availability or performance of a product; and
3. is product specific data about a product; and
4. is held in in digital form.

Voluntary product data is simply information that is not required product data or information that is specified in the banking sector designation instrument. This excludes credit information.

What are the Privacy Safeguards?

The Privacy safeguards are consistent with the APPs (with some renumbering after 9):

	Privacy Safeguard	APP
1	Open and transparent management of CDR data	Open and transparent management of personal information
2	Anonymity and pseudonymity	Anonymity and pseudonymity
3	Soliciting CDR data from CDR participants only with valid requests	Collection of solicited personal information
4	Dealing with unsolicited CDR data from participants - duty to destroy	Dealing with unsolicited personal information
5	Notifying of the collection of CDR data	Notification of the collection of personal information
6	Use or disclosure of CDR data by accredited data recipients or designated gateways	Use or disclosure of personal information
7	Use or disclosure of CDR data for direct marketing by accredited data recipients or designated gateways by request or with valid consent	Direct marketing
8	Overseas disclosure of CDR data by accredited data recipients on condition that there be substantially equivalent privacy safeguards	Cross-border disclosure of personal information
9	Adoption or disclosure of government related identifiers by accredited data recipients not permitted unless authorised	Adoption, use or disclosure of government related identifiers
10	Notifying of the disclosure of CDR data	Quality of personal information
11	Quality of CDR data - date must be accurate, up to date and complete	Security of personal information
12	Security of CDR data and destruction or de identification of redundant CDR data	Access to personal information
13	Correction of CDR data	Correction of personal information

The Privacy Safeguard Rules

The Rules also set out substantive obligations that must be followed.

Privacy Safeguard 1	A CDR policy must be made available in a form of a document that is distinct from any of the CDR entity's privacy policies
	A data holder's CDR policy must indicate whether it accepts requests for voluntary product data or voluntary consumer data, and if so, whether it charges a fee for disclosure of such data and how much the fee is
	The CDR policy must include: (a) a statement indicating the consequences to the CDR consumer if they withdraw a consent to collect and use CDR data (b) include a list of the outsourced service providers (c) disclose whether such service providers are based overseas and is not an accredited person (d) how, if at all, the accredited person uses CDR data that has been de-identified
	CDR policy must include where, how and when CDR consumer compliant can be made; when the CDR consumer compliant will be addressed; and the process for handling a compliant
	The CDR policy must be readily available.
Privacy Safeguard 2	The accredited data recipient is required or authorised by law to deal with an identified CDR consumer in relation to CDR data. It is impractical for a the accredited data recipient to deal with a CDR consumer that has not been identified.
Privacy safeguard 3	Nil
Privacy safeguard 4	Nil
Privacy safeguard 5	An accredited person that collects CDR data must update the person's dashboard as soon as practicable to indicate what CDR data was collected; when the CDR data was collected; and the data holder of the CDR data.
Privacy safeguard 6	An accredited data receipt that has collected CDR data under a consumer data request made on behalf of a CDR consumer must not use or disclose it other than for a permitted use or disclosure (whether or not it relates to direct marketing). The use or disclosure of CDR data for which there is a CDR consumer by an accredited data recipient of the CDR data is authorised under these rules if it is a permitted use or disclosure, other than one that relates to direct marketing.

Privacy safeguard 7	The use oof CDR data for which there is a CDR consumer by an accredited data receipt of the CDR data for direct marketing is authorised under these rules if it is a permitted use or disclosure that relates to direct marketing.
Privacy safeguard 8	Nil
Privacy safeguard 9	Nil
Privacy safeguard 10	An accredited person that collects CDR data must update the person's dashboard as soon as practicable to indicate what CDR data was collected; when the CDR data was collected; and the data holder of the CDR data.
Privacy safeguard 11	The data holder must provide the CDR consumer on whose behalf the disclosure was made and the date of the disclosure via written notice. Notice must be provided as soon as practicable.
Privacy safeguard 12	Where the accredited person has elected to de-identify their redundant data, the step is to apply the CDR data de-identification process to the redundant data. Where data has become redundant, apply the CDR data deletion process to the redundant data.
Privacy safeguard 13	A data holder must not charge a fee for responding to or actioning a request for correction of data. Within 10 business days after receipt of the request, the data must be corrected and provide a statement certifying the data is accurate, up to date, complete and not misleading. Written notice must also be given to the requester indicating how the response was dealt with

BRISBANE

Level 35, Waterfront Place
1 Eagle Street
Brisbane QLD 4000
Australia

+61 7 3002 8700

MELBOURNE

Level 23
181 William Street
Melbourne VIC 3000
Australia

+61 3 8624 2000

SYDNEY

Level 42
2 Park Street
Sydney NSW 2000
Australia

+61 2 8281 4555