TREASURY LAWS AMENDMENT (CONSUMER DATA RIGHT) BILL 2018: PROVISIONS FOR FURTHER CONSULATION

EXPLANATORY MATERIALS

Table of contents

Glossary

The following abbreviations and acronyms are used throughout this explanatory memorandum.

Abbreviation	*Definition*
ACCC	Australian Competition and Consumer Commission
AFCA	Australian Financial Complaints Authority
AIC Act	*Australian Information Commissioner Act 2010*
APPs	Australian Privacy Principles
the CC Act	*Competition and Consumer Act 2010*
Commissioner	Commissioner at the Australian Competition and Consumer Commission
Information Commissioner	Australian Information Commissioner
CDR	Consumer Data Right
OAIC	Office of the Australian Information Commissioner
Privacy Act	*Privacy Act 1988*

Chapter 1
Consumer Data Right

Introduction

1.1 The primary aim of the CDR is to give consumers the ability to access and use more information about themselves and, about their use of goods and services, in a manner that allows them to make informed decisions about both themselves and their participation in the market. By doing so, the CDR aims to increase competition in any market, enable consumers to fairly harvest the value of their data and enhance consumer welfare. This should be done in a manner that fairly considers the incentives for all participants.

1.2 The exposure draft of the *Treasury Laws Amendment (Consumer Data Right) Bill 2018: Provisions for further consultation* builds on the exposure draft of the *Treasury Laws Amendment (Consumer Data Right) Bill 2018* that was released for consultation on 15 August 2018.

1.3 The general context for the amendments establishing the regulatory framework for the CDR is outlined in Chapter 1 of the Explanatory Materials for the exposure draft of the *Treasury Laws Amendment (Consumer Data Right) Bill 2018* (that was released on 15 August 2018).

1.4 This chapter of the explanatory materials explains the revised provisions that are released for consultation.

Summary of key changes since the earlier exposure draft

Designating a sector – scope of the instrument and the factors the Minister must consider

1.5 The Minister's powers to designate a sector of the economy as subject to the CDR have been more clearly set out.

1.6 The Minister designates a sector by specifying classes of information, and persons who hold such information and the earliest day applicable to the sector for beginning to hold the information.

1.7 In addition to the previously set out factors the Minister must consider prior to designating a sector, the Minister must consider the likely effect on any intellectual property in the information to be covered by the instrument (see sections 56AC and 56AD and paragraphs 1.20 to 1.33).

Derived data - limiting the application of the CDR

1.8 During the first consultation a number of stakeholders were concerned about the scope of the definition of CDR data and the requirement to share derived or value added data.

1.9 While the definition of CDR data remains unchanged, a limitation on the ACCC's rules making powers has been included in the Bill.

1.10 Where the information relates to a consumer, the ACCC can only make consumer data rules which require access and transfer of information that is in the designation instrument (See section 56BC and paragraph 1.53).

1.11 Similarly, for information not relating to a consumer the ACCC rules making powers requiring access and transfer are limited to information about the eligibility criteria, terms and conditions, or price of a product, other kind of good, or a service (See section 56BD and paragraph 1.53).

Definition of CDR consumer

1.12 During the first consultation a number of stakeholders noted that the definition of 'CDR consumer' could apply more broadly than intended.

1.13 The definition has been revised so that a CDR consumer is an identifiable or reasonably identifiable person, including a small, medium or large business enterprise, to which the CDR data relates because of the supply of a good or service either to the person or an associate of the person (See section 56AF and paragraphs 1.55 to 1.65).

Data reciprocity

1.14 During consultation stakeholders requested further information about how reciprocity would operate within the CDR regime. Reciprocity will operates to allow the ACCC to write rules requiring data recipients to provide customers access to data, or the ability to request disclosure of data to accredited parties.

1.15 Reciprocity will apply to:

- **Equivalent data** which is data included within a class in the designation instrument which has not been transferred within the CDR system and which is held by an accredited data recipient; and/or
- **Received data:** Data that recipients have received through the CDR.

1.16 While the concept of reciprocity will be given effect through rules made by the ACCC, the definition of data holder has been amended to clarify the treatment of data in the hands of certain accredited entities (See subsection 56AG(3) and paragraphs 1.38 to 1.41 and 1.66 to 1.71).

Interaction of Privacy Safeguards with the Privacy Act

1.17 The first consultation identified the need to further clarify the interaction of the Privacy Safeguards implemented under the CDR with the existing privacy protections in the Privacy Act. It was not clear whether an entity would need to meet obligations under both the Privacy Safeguards and Privacy Act for the same data.

1.18 The Bill has been amended to reduce this complexity and better clarify the obligations which fall on a data holder and accredited data recipient.

Table 1.1 Application of Privacy Safeguards by CDR participant

CDR Participant	*Privacy Safeguard that applies*
Data holder	PS 1 – applies concurrently to APP 1 PS 10 - Applies to the disclosure of CDR data. The Privacy Act does not apply. PS 11, PS 13 – Apply to the disclosure of CDR data and substitutes for APPs 11 and 12 for disclosed CDR data
Accredited person	PS 1, PS 3, PS 4, PS 5 - the APPs apply concurrently, but with the Safeguards prevailing.
Accredited data recipient	PS 2, PS 6, PS 7, PS 8 , PS 9, PS 10, PS 11 - the Privacy Safeguards apply and substitute the APPs. The APPs do not apply to an accredited data recipient of CDR data for CDR data that has been received or data derived from that data.

1.19 For a more detailed explanation see sections 56EA to 56EO and paragraphs 1.72 to 1.134).

Designated Sectors

1.20 The Minister is given the power to designate a sector of the Australian economy as a sector to which the CDR applies. ***[Schedule 1, item 1, section 56AC]***

1.21 The instrument designating the sector is a legislative instrument which is subject to the scrutiny of Parliament and is disallowable.

1.22 The CDR is intended to eventually apply widely across the economy. The designation process is therefore a process to aid in the prioritisation of sectors, and to identify data sets where the potential

benefits for consumers to access and transfer their information exceed the potential costs.

1.23 Prior to making a designation, the Minister must consider a range of factors in order to inform his or her decision and ensure that the designation of the sector is appropriate. The ACCC will be responsible for advising the Minister on these matters. ***[Schedule 1, item 1, section 56AD]***

1.24 These factors include consideration of the effect of designating a sector on the consumers within that sector. This will ensure that as the CDR is rolled out across the economy, the beneficial impact of designation and impact on consumers are considered. ***[Schedule 1, item 1, subparagraph 56AD(1)(a)(i)]***

1.25 Other factors which must be considered by the Minister include the impact designation will have on the privacy of individuals and confidentiality of business consumers. The Minister must consult the OAIC about the likely effect of making the instrument on the privacy or confidentiality of a consumer's information. ***[Schedule 1, item 1, subparagraph 56AD(1)(a)(iii) and subsection 56AD(3)]***

1.26 The ability of the CDR to promote market efficiency, competition and innovation and the ways designation will enhance these matters must be considered prior to the designation of a sector. The Minister must also consider the impact on the intellectual property rights of CDR participants of designating a data set. ***[Schedule 1, item 1, subparagraph 56AD(1)(a)(vi)]***

1.27 The Minister may also consider any other relevant factors. This could include considering a consumer's existing access to a particular data set. ***[Schedule 1, item 1, paragraph 56AD(1)(c)]***

1.28 The regulatory impact of designating a sector must be determined. In practice, this means that a Regulatory Impact Statement must be prepared reflecting the net benefits of designation, before a sector is designated. ***[Schedule 1, item 1, paragraph 56AD(1)(b)]***

1.29 The Government's policy on Regulatory Impact Statements requires that both the costs and benefits are considered. This includes consideration of costs to business, including to small business, methods to minimise drivers of costs, concepts of fairness and equality. It also includes consideration of benefits including improved competition, lower prices, availability of better products, improved productivity, the creation of new jobs and reduction in risk or improvement in safety.

1.30 While the CDR is intended to enhance competition this should not occur at the expense of significant regulatory burden or disruption unless the broadly defined benefits of designation outweigh the regulatory impact.

1.31 Before designating a sector, the Minister is required to consult with the ACCC as well as any other person or body prescribed by regulations. ***[Schedule 1, item 1, subsection 56AD(2)]***

1.32 The Bill places obligations on the ACCC and OAIC as to the process for consulting and advising the Minister when the Minister seeks advice prior to designating a sector. These provisions are not included in this exposure draft.

1.33 The banking sector will be designated as the first sector of the economy to which the CDR applies. Public consultation was undertaken as a part of the process of preparing the Open Banking Report presented to the Minister in December 2017. Six weeks public consultation on that Report was also undertaken by the Minister from 9 February 2018.

Participants in the Consumer Data Right system

Data holders

1.34 Data holders are a key player in the CDR regime as the entities that have collected, generated or hold data set out in the designation instrument. ***[Schedule 1, item 1, subsection 56AG(1)]***

1.35 Data holders are potentially subject to rules mandating data access at the request of a consumer. No data holder will be required to disclose information at a consumer's request in accordance with the CDR unless there is a rule that requires them to do so.

1.36 The Bill has been amended to more clearly set out who is a data holder. There are three circumstances.

Case 1: Designated data holders

1.37 Generally speaking, a data holder will be the entity that is specified in the designation instrument***. [Schedule 1, item 1, subsection 56AG(2)]***

Example 1.1

BankY is a major Australian bank with many customers. It collects transaction information for each of its customers reflecting the debit and credits on accounts.

The designation instrument lists transaction information generated from providing a service or good related to a banking business as a "class of information".

The designation instrument also lists authorised deposit-taking institutions as a person holding such information.

BankY is a data holder. It generates and collects data that is listed in the designation instrument and is a specified person.

Case 2: Reciprocal data holders

1.38 In some circumstances an accredited data recipient may also be a data holder.

1.39 An accredited data recipient will also be a data holder where the entity holds data specified in the designation instrument and this data was not transferred to it under the consumer data rules (or derived from such data). ***[Schedule 1, item 1, subsection 56AG(3)]***

1.40 This could occur where the accredited data recipient provided similar services to an entity listed in the designation. For example, a non-ADI lender would also hold transaction information about credit provided to its customers but as it is not an ADI it would not be captured under the scenario described in Case 1.

Example 1.2

> LendMeMoney is an accredited data recipient. It holds an Australian credit license and provides credit to its customers. As part of this service it generates and holds lists of the transactions for each consumer.
>
> As an accredited entity it can also be disclosed this type of information from other data holders.
>
> For the data that it holds about its own customers which reflects the credit services it provides its customers LendMeMoney would be a data holder and potentially subject to access rights.

1.41 By treating an accredited entity as a data holder the CDR data that the accredited entity collects or generates outside of the CDR will be subject to the smaller subset of Privacy Safeguards

Case 3: Receiving data holders

1.42 Finally, a person will be a data holder where the person holds an accreditation, holds data included in the designation instrument as a result of a transfer under the consumer data rules and meets conditions included in the consumer data rules. ***[Schedule 1, item 1, subsection 56AG(4)]***

1.43 In these circumstances an accredited data recipient would be able to handle CDR data as a data holder. This has the effect of changing the privacy protections applying to the CDR data so that the APPs, as applicable, apply to a data holder's ongoing use of that CDR data.

1.44 It would be expected that the conditions included in the rules would be that:

- the data is data of a class that the accredited data recipient would generate or collect in the ordinary course of its business outside of the CDR; and

- the accredited data recipient would use the information for the same purpose as their ordinary business.

Example 1.3

BankY became an accredited data recipient so that it is able to receive CDR data.

Martin switches to BankY. He uses the CDR to transfer his historical data from Bank A to BankY. BankY receives this data comprising banking information of the type BankY ordinarily holds. BankY collects that data about Martin as an accredited data recipient.

The consumer data rules provide that if a CDR consumer transfers their banking business, the recipient bank is able to treat banking information transferred under the consumer data rules as if the recipient bank was the data holder of the information.

Because Martin has transferred his banking business to BankY, Bank Y will be considered a recipient data holder for this information.

Example 1.4

BankY became an accredited data recipient so that it is able to receive CDR data.

Martin switches to BankY. BankY offers an energy consumption monitoring and alert service. Martin uses the CDR to monitor his energy usage data from Energy A.

BankY receives this data comprising energy information of the type BankY does not ordinarily hold. BankY collects that data about Martin as an accredited data recipient.

Accredited data recipients

1.45 For completeness, this exposure draft includes the definition of 'accredited entity'. This definition is largely unchanged from the earlier exposure draft except to allow for the changes to the definition of data holder.

1.46 Accredited data recipients are entities holding CDR data as a result of that CDR data being disclosed to them at the direction of a CDR consumer under the consumer data rules. The person is not a data holder. ***[Schedule 1, item 1, subsection 56AGA]***

1.47 The consumer data rules will provide that a CDR consumer's right to access their data and direct a data holder to transfer the data to another entity under the CDR, exists where the entity holds an accreditation. There is a limitation on the rule-making power that data holders can only be required to disclose CDR data to accredited persons. Accreditation will initially be managed by the ACCC who will be the Data Recipient Accreditor. ***[Schedule 1, item 1, subsection 56BC(3)]***

1.48 Data holders within the CDR system will only be treated as accredited data recipients if they seek to participate in CDR as recipients of CDR data.

1.49 If a data holder wishes to access CDR data as a recipient, the data holder must be an accredited data recipient and its use, disclosure, collection, storage and deletion of received CDR data will be subject to the Privacy Safeguards and the consumer data rules.

1.50 Other data that could be transferred to a non-accredited entity is CDR data that does not relate to the CDR consumer, such as general product information. ***[Schedule 1, item 1, sections 56BB and 56BD)]***

CDR data

1.51 The new concepts of CDR data and CDR consumer are created to clarify how the CDR system applies to information and consumers. ***[Schedule 1, item 1, section 56AF]***

1.52 CDR data will be data that is outlined in the instrument designating a sector and any information that is subsequently derived from that data. CDR data can include product information, records of usage of a good or service, or any other data specified in the designation; the data can relate to natural and legal persons.

1.53 While the definition of CDR data may appear broad, the data that data holders may be required to give access to is limited to the information specified in the designation instrument. Mandatory access to data that does not relate to an identified consumer is further limited to data about products. ***[Schedule 1, item 1, subsection 56BC(4) and 54BD(2)]***

1.54 The second limb of the definition of CDR data, data that is 'derived' from data in the designation instrument, only has effect for the purpose of the Privacy Safeguards and the scope of the rule-making power outside of disclosures of data.

CDR consumer

1.55 The definition of a CDR consumer limits mandatory access requirements to data relating to an identified consumer and the supply of a good or service to them or their associate.

1.56 CDR data is data that 'relates' to a CDR consumer. The concept of 'relates to' is a broader concept than information 'about' an identifiable or reasonably identifiable person under the Privacy Act. The term 'relates' has a broader meaning than 'about' and is intended to capture, for example meta-data of the type found not to be about an individual in *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFA 4 (19 January 2017).

1.57 Relates can include reference to an identifier such as a name, an identification number, location data of the person or of products that

would reasonably be expected to be co-located with either the person or their address, an online identifier (including cookie identifiers and internet protocol addresses) or to one or more factors specific to the physical, physiological, genetic, mental, behavioural (including predictions of behaviours or preferences), economic, cultural or social identity or characteristics of that person. Where information is primarily about a good or service, but reveals information about a consumer's use of that good or service, it relates to the consumer.

1.58 The CDR consumer is broader than the CC Act definition of a consumer. This is because the CDR system will apply to business consumers.

1.59 The CDR consumer is an identifiable or reasonably identifiable person, including a small, medium or large business enterprise, to whom the CDR data relates because of the supply of a good or service either to the person or an associate of the person. The CDR data will be held by or on behalf of a data holder or accredited data recipient entity under the CDR system. ***[Schedule 1, item 1, subsections 56AF(3) and 56AF(4)]***

1.60 While the government has determined that Open Banking will apply to large customers, the extent of the definition of CDR consumer can be narrowed on a sector by sector basis through the designation process and the rule-making process. For example, in the banking sector, it is proposed that the access and transfer right under the rules will not extend to large customers who have bespoke arrangements.

Example 1.5

TBM is a large corporation specialising in manufacturing bicycle parts. It obtains banking services from one of the medium sized banks operating in Australia, Stately Bank. Following the designation of the banking sector as a CDR sector, TBM is keen to send its designated banking data to a fintech, MoneyMoney, to check whether it is getting the best banking services.

TBM would not be covered by the definition of 'consumer' in section 4 of the CC Act. However, because Stately Bank has data about TBM that is covered by the designated data set applying to the banking sector, TBM is a CDR consumer and is able to participate in the CDR system.

1.61 The term 'associate' is defined with reference to the *Income Tax Assessment Act 1936*. It is a broad definition and includes a person's relatives such as spouse, children or siblings.

1.62 It means that where a person uses a good or service (person 1) but the contract or similar is in the name of someone else (person 2), the ACCC is able to write rules allowing person 1 the right to access or direct the transfer of information about their use of the good or service.

Example 1.6

Mark is an additional card holder of Amanda's credit card. Mark is the primary user of the credit card. Under the ACCC access and transfer rules, Mark is able to request that the credit card information be transferred to a third party. Due to the notification requirements in Privacy Safeguard 10, Amanda is notified of this disclosure prior to the disclosure, as specified in the Consumer Data Rules.

If Amanda requests disclosure of this information, the rules can require that Mark be notified.

1.63 Whether information is about a 'reasonably' identifiable person requires a contextual consideration of the particular circumstances of the case, including the nature and amount of information, other information that may be available to the persons who will have access to the information, and the practicability of using that information to identify a person.

1.64 An important consideration in whether data can be considered to relate to a 'reasonably identifiable' person is what motivations there may be to attempt re-identification. A person will be reasonably identifiable where:

- it is technically possible for re-identification to occur (whether from the information itself, or in combination with other information that may be available), and
- there is a reasonable likelihood of re-identification occurring.

1.65 The ACCC rules and OAIC guidance may provide further requirements for when information can be considered to be de-identified.

Principle of Reciprocity

1.66 The consumer data rules may provide that a consumer can direct that an accredited entity must provide access to certain CDR data to the consumer or other accredited recipients. This is known as the principle of reciprocity.

1.67 The principle of reciprocity imports elements of fairness and allows customers to request access to or to transfer additional data-sets.

1.68 A CDR system in which eligible entities participate fully — both as data holders and data recipients — is likely to be more vibrant and dynamic than one in which data recipients are solely receivers of data, and data holders are largely only transmitters of data.

1.69 Reciprocity operates to allow the ACCC to write rules requiring certain accredited data recipients to provide customers access to, or the ability to request transfer to accredited parties.

1.70 The principle of reciprocity will therefore be implemented through the rules. The same factors for considering whether a rule should be made apply to whether reciprocity should apply.

1.71 As such, if a CDR participant does not hold data that falls within a class designated in a designation instrument, reciprocity cannot apply. Similarly, as reciprocity is a principle that goes towards fairness and the vibrancy of the data economy, it would be expected that rules regarding reciprocity would more often be made about the same or equivalent data, than received data.

CDR Privacy Framework

1.72 Division 5 creates the CDR privacy safeguards (the Privacy Safeguards). It is useful to understand how the Privacy Safeguards work in relation to the Privacy Act and APPs.

1.73 Generally speaking, the Privacy Act and the APPs will continue to apply to data holders (as defined by section 56AG) under the CDR with the exception of accuracy and correction rights and notification obligations once a valid request for CDR data has been received. In this instance the Privacy Safeguards apply and the APPs do not. ***[Schedule 1, item 1, paragraph 56EC(4)(a)]***

1.74 For accredited data recipients (as defined by section 56AGA), the Privacy Safeguards will substitute for the APPs and the APPs will not apply to CDR data that has been received by an accredited data recipient through the CDR regime. ***[Schedule 1, item 1, subsection 56EC(4)]***

1.75 The definitions of CDR Data, CDR Consumer, data holder, accredited person and accredited data recipient operate to determine when each of the Privacy Safeguards apply and the data that the Privacy Safeguard apply to.

Table 1.2 Application of Privacy Safeguards by CDR participant

CDR Participant	*Privacy Safeguard that applies*
Data holder	PS 1 – applies concurrently to APP 1 PS 10 - Applies to the disclosure of CDR data and there is no similar requirement under the Privacy Act PS 11, PS 13 – Apply to the disclosure of CDR data and substitutes for APPs 11 and 12 in respect of disclosed CDR data
Accredited person	PS 1, PS 3, PS 4, PS 5 - the APPs apply concurrently, but with the more specific Privacy Safeguards prevailing

CDR Participant	*Privacy Safeguard that applies*
Accredited data recipient	PS 2, PS 6, PS 7, PS 8 , PS 9, PS 10, PS 11 - the Privacy Safeguards apply and substitute the APPs which do not apply to an accredited data recipient of CDR data in relation to the CDR data that has been received or data derived from that data

Example 1.7

Max is a consumer with AllenBank. All of his transaction information held by AllenBank is treated consistently with the Privacy Act and APPs by AllenBank.

Max has a transaction (savings) account with AllenBank but has been told by friends he can probably get a better interest rate elsewhere. Keen to make the most of the CDR, Max has requested AllenBank to transfer his CDR data relating to the transaction account to HIZAI Banking Services.

At the time of receiving Max's CDR data, HIZAI Banking Services is required to handle the data in accordance with the CDR Privacy Safeguards because HIZAI Banking Services is an accredited data recipient in respect of Max's data.

Max discovers that HIZAI Banking Services will provide him with a better interest rate on his transaction account. Max closes his transaction account with AllenBank and opens an account with HIZAI Banking Services.

All new transaction data created by HIZAI Banking Services in relation to Max's transaction account is subject to the Privacy Act and the APPs.

Consumer data rules may enable HIZAI Banking Services to also treat Max's historical data as a data holder, and subject instead to the APPs.

Example 1.8

Max subsequently hears of a service offered by HIZAI Banking Services. HIZAI Banking Services is an accredited data recipient for the energy sector and it offers to compare customers' energy bills and advise customers if savings could be made by switching providers.

Max consents to the transfer of his energy bills from GasCo and PowerProvider to HIZAI Banking Services. HIZAI Banking Services must handle Max's energy sector information in accordance with the Privacy Safeguards, as it is an accredited data recipient of this CDR data.

1.76 A more prescriptive approach has been taken to the design of the Privacy Safeguards to ensure the proper use, access, disclosure or transfer, storage and deletion of CDR data. The Privacy Safeguards will also apply to CDR data where the CDR consumer is a business.

1.77 The Privacy Act principally applies to 'personal information' which is defined at section 6 of that Act to include information or an opinion about an individual from which the individual may be capable of being identified.

1.78 Similarly, the Privacy Safeguards only apply to information that relates to identifiable or reasonably identifiable CDR consumers, including business consumers who wish to participate in the system. As such, the Privacy Safeguards have been created to ensure that business information is also protected.

1.79 The use of the term 'relates' creates a lower threshold for information to be protected by the Privacy Safeguards than applies to information protected by the APPs. The APPs apply to information 'about' a person. This means that CDR data held by an accredited data recipient will continue to be protected by the Privacy Safeguards until that data ceases to 'relate' to an identifiable or reasonably identifiable consumer. In particular, it is intended that the term 'de-identification' be interpreted by reference to this threshold.

1.80 The Bill clarifies the types of data the Privacy Safeguards apply to and how the Privacy Safeguards interact with the consumer data rules. The consumer data rules may impose additional privacy protections provided they are consistent with the Privacy Safeguards. ***[Schedule 1, item 1, subsections 56EC(1) and 56EC(2)]***

1.81 The Bill provides coverage for CDR consumers irrespective of whether they are an individual or a business consumer. ***[Schedule 1, item 1, section 56EB]***

1.82 CDR data must be handled by accredited recipients consistently with the Privacy Safeguards. The collection of CDR data may also be authorised or required under another Australian law. In that case, a person will be authorised to make the collection of the CDR data by that law.

Consideration of CDR data privacy

CDR Privacy Safeguard 1 - Open and transparent management of CDR data

1.83 It is important that CDR consumers have the ability to inquire or complain about the manner in which their CDR data is being handled by a CDR participant. The CDR system is consumer driven. If a consumer is not satisfied that their data is being treated in compliance with the consumer data rules, the consumer should have a clear avenue to raise this with the data holder or accredited entity in possession of the consumer's CDR data.

1.84 To assist in this, all CDR participants must have policy, procedures and systems in place that ensure compliance with the CDR regime and management of CDR data.

1.85 For data holders, the policy must contain the following information:

- How a CDR consumer may access the CDR data and seek corrections if there are errors; and
- How a CDR consumer may complain about a failure of a data holder or accredited data participant to comply with the CDR regime.

1.86 For accredited data recipients, the policy about the management of CDR data must contain the following information:

- The kinds of CDR data held by the accredited data recipient and how that data is held;
- The purposes for collecting, holding, using and disclosing the CDR data;
- How a CDR consumer is able to access their CDR information and seek a correction of the CDR data if there are errors;
- How a CDR consumer can complain about the failure of a CDR participant to comply with the CDR regime;
- How the accredited data recipient will address such a complaint;
- If the accredited data recipient is likely to disclose CDR data to an overseas accredited data entity, information about the country in which that entity is based;
- The circumstances when the accredited data recipient will disclose the data to a person that does not hold an accreditation;
- The events that the CDR consumer will be notified about; and
- The circumstances when the accredited data recipient must delete CDR information.

[Schedule 1, item 1, section 56ED]

1.87 CDR participants' policies must detail each of the above factors in order for the policy to be compliant with Privacy Safeguard 1. It is essential that CDR consumers clearly understand how to make a complaint about the use, disclosure or storage of their CDR data. Equally, it is important that information be accurate and corrections be made, if required.

1.88 For ease of access, the CDR privacy policy must be made available free of charge and in an appropriate form. An appropriate form might, for example, include online or in a booklet which is capable of being sent to a CDR consumer or other participant. ***[Schedule 1, item 1, paragraph 56ED(6)(a)]***

1.89 The policy must be made available consistent with the consumer data rules. If the consumer data rules specify for the policy to be made available in a certain format, the CDR consumer may require the policy be provided to them in that format. ***[Schedule 1, item 1, subsection 5ED(7)]***

CDR Privacy Safeguard 2 – Anonymity and pseudonymity

1.90 Generally, whether a CDR consumer will be able to utilise a pseudonym in relation to their CDR data will be a matter prescribed by the consumer data rules. ***[Schedule 1, item 1, subsection 56EE(2)]***

1.91 As a general rule, a CDR consumer may be provided with the option of utilising a pseudonym if that is considered appropriate for the sector. However, as the first sector to be designated as a CDR sector is likely to be the banking sector, it is expected that the ACCC will make consumer data rules which prohibit the use of a pseudonym for this sector. Consumers are not able to deal with their bank via a pseudonym and it would not be appropriate to enable them to do so within the CDR system.

1.92 There may be other sectors designated in the future where it is acceptable for individuals to use a pseudonym, such as social media. As such, scope is provided for the use of pseudonyms in the future.

1.93 Unless the consumer data rules specify instances where an accredited data recipient is unable to provide a CDR consumer with the ability to use a pseudonym, a pseudonym may be permitted. ***[Schedule 1, item 1, subsection 56EE(1)]***

1.94 Privacy Safeguard 2 does not apply to data holders. As applicable, the Privacy Act and APPs will apply to data holders.

Collecting CDR data

CDR Privacy Safeguard 3 – Collecting solicited CDR data

1.95 An accredited person must only seek to collect CDR data in accordance with the CDR regime if the CDR consumer has given a valid request for the accredited person to collect the data under the consumer data rules. ***[Schedule 1, item 1, section 56EF]***

1.96 An accredited person may collect data for other purposes if it is allowed by another law but the accredited entity should not purport that the collection is being made under the CDR regime.

CDR Privacy Safeguard 4 – Dealing with unsolicited CDR data

1.97 This Privacy Safeguard is included to cover scenarios where an accredited person may not have sought particular CDR data from a data holder, but they find themselves in possession of it.

1.98 In such circumstances, the accredited person is required to destroy the CDR data unless an Australian law requires the person to retain that data. ***[Schedule 1, item 1, section 56EG]***

1.99 This section makes it clear than an accredited person will not be able to retain unsolicited CDR data, except if required to do so under an Australian law or by order of a court or tribunal.

CDR Privacy Safeguard 5 – Notifying the collection of CDR data

1.100 If an accredited person collects data in accordance with Privacy Safeguard 3, then the accredited person must comply with the consumer data rules relating to advising the CDR consumer about the collection of their data. For example, the consumer data rules may require that each holder of a joint account be notified prior to the data being disclosed pursuant to an authorisation to transfer data to that account. The consumer data rules will provide for matters which need to be addressed in such notifications, based upon the relevant sector. ***[Schedule 1, item 1, section 56EH]***

1.101 This notice must also be given to the CDR consumer in accordance with the requirement, if any, specified in the consumer data rules relating to Privacy Safeguard 5 notices. ***[Schedule 1, item 1, subsection 56EH(b)]***

Dealing with CDR data

CDR Privacy Safeguard 6 – Use or disclosure of CDR data

1.102 An accredited data recipient must not use CDR data unless it is consistent with a consent given by a consumer under the consumer data rules. ***[Schedule 1, item 1, paragraph 56EI(1)(b)]***

1.103 Similarly, an accredited data recipient must not disclose CDR data unless the disclosure is authorised or required under the consumer data rules in response to a valid consent by the consumer. ***[Schedule 1, item 1, paragraph 56EI(1)(a)]***

1.104 This is an important acknowledgement of the fact that the CDR system is driven by consumers. Consumer consent for uses of their CDR data, including subsequent disclosure, is at the heart of the CDR system.

1.105 A use or disclosure will be allowed without the consumer's consent under the consumer data rules where it is required or permitted by an Australian law, (except the APPs), is authorised under the consumer data rules, or an order of a court or tribunal. ***[Schedule 1, item 1, paragraph 56EI(1)(c)]***

CDR Privacy Safeguard 7 – Use or disclosure of CDR data for direct marketing by accredited data recipients

1.106 In order to ensure that CDR consumers are not subject to unwanted direct marketing as a result of their engagement with the CDR system, the use of CDR data for direct marketing purposes must be required or authorised by the consumer data rules consistent with the a consumer's request and consent. ***[Schedule 1, item 1, section 56EJ]***

1.107 It is worth noting that this Privacy Safeguard does not apply to the use of CDR data in the hands of the original data holder. These data holders will be required to comply with APP 7 in relation to direct marketing use of individual.

1.108 Unless authorised or required by the consumer data rules and specifically consented to by the CDR consumer, direct marketing is not permitted.

CDR Privacy Safeguard 8 – Cross-border disclosure of CDR data

1.109 As overseas entities may be able to be accredited, it is possible that disclosure of CDR data may be provided to accredited data recipients located outside of Australia.

1.110 The Bill applies to disclosures of CDR data to offshore entities so that disclosure is permitted if the entity is an accredited data recipient. ***[Schedule 1, item 1, section 56EK]***

1.111 Accreditation is considered sufficient protection to ensure that the accredited entities will not breach the Privacy Safeguards.

1.112 The consumer data rules may also provide that a cross-border disclosure is authorised for CDR data where conditions specified in the consumer data rules are met. It is anticipated that these conditions will reflect the conditions in APP8 with the additional requirement that consent to such a disclosure would be required. ***[Schedule 1, item 1, subsection 56EK(d)]***

CDR Privacy Safeguard 9 – Adoption or disclosure of government related identifiers

1.113 As the CDR system develops, it is possible that CDR consumers who are individuals may have CDR data sets that contain government related identifiers, as defined in the Privacy Act. This could include a tax file number.

1.114 In order to protect government related identifiers, they are not permitted to be used by an accredited data recipient as an identifier of a CDR consumer who is an individual. ***[Schedule 1, item 1, subsection 56EL(1)]***

1.115 The exception is where the use is allowed under an Australian law (other than the consumer data rules), or an order of a court or tribunal. ***[Schedule 1, item 1, paragraph 56EL(1)(c)]***

1.116 Similarly, it is not permissible for an accredited data recipient to disclose CDR data about an individual containing a government related identifier. The only exception to this is if the disclosure is permitted by an Australian law (except the consumer data rules), or by an order of a court or tribunal. ***[Schedule 1, item 1, subsection 56EL(2)]***

1.117 The limitation on using or disclosing government identifiers does not apply where the CDR consumer is not an individual. For example, the ABN of a business which is not a sole trader would not be subject to Privacy Safeguard 9.

CDR Privacy Safeguard 10 – Notifying of the disclosure of CDR data

1.118 Unlike the other Privacy Safeguards discussed to this point, Privacy Safeguard 10 applies to a data holder as well as an accredited data recipient.

1.119 Where a data holder has responded to a valid request from a CDR consumer and disclosed CDR data consistent with the consumer data rules the data holder must notify the consumer as required by the consumer data rules. ***[Schedule 1, item 1, subsection 56ELA(1)]***

1.120 The consumer data rules may set out which CDR consumer must receive the notification, where there is more than one consumer, what matters must be included in the notification and the time in which the notification must be given. ***[Schedule 1, item 1, subsection 56ELA(1)]***

1.121 Similarly, where an accredited data recipient has disclosed CDR data, the accredited data recipient must notify the consumer as required by the consumer data rules. ***[Schedule 1, item 1, subsection 56ELA(2)]***

1.122 The consumer data rules may set out which CDR consumer must receive the notification, where there is more than one consumer, what matters must be included in the notification and the time in which the notification must be given. ***[Schedule 1, item 1, subsection 56ELA(2)]***

Integrity of CDR data

CDR Privacy Safeguard 11 – Quality of CDR data

1.123 Privacy Safeguard 11 also applies to data holders. Where a data holder is required to disclose CDR data in response to a valid request from a CDR consumer, the data holder must ensure that the CDR data is accurate, up to date and complete for the purpose for which it is held. ***[Schedule 1, item 1, subsection56EM(1)]***

1.124 The CDR data is not held for the purpose of being required to be disclosed under the CDR rules. For example, a data holder that is an ADI collects transaction data for the purpose of providing a banking service to its customer. It does not hold transaction data for the purpose of being required disclose the data under the CDR regime. ***[Schedule 1, item 1, subsection56EM(6)]***

1.125 Similarly, an accredited data recipient must ensure that the data it discloses consistent with the consumer data rules is accurate, up to date and complete for the purpose for which it is held. It is not held for the

purpose of disclosing the CDR data under the CDR rules. ***[Schedule 1, item 1, subsections 56EM(2) and 56EM(6)]***

1.126 Where either the data holder or accredited data recipient becomes aware that the CDR data that was disclosed was incorrect, the data holder or accredited data recipient must notify the consumer in writing. ***[Schedule 1, item 1, subsection 56EM(3)]***

1.127 If the CDR consumer asks the data holder or accredited data recipient to disclose the corrected CDR data to persons to whom it was previously disclosed, the data holder or accredited data recipient must comply. ***[Schedule 1, item 1, subsection 56EM(4)]***

Example 1.9

Levi requested that his mobile phone information from his current provider be disclosed to a fintech, TeleMarketDeals for the purpose of comparing whether there is a better rate for his international calls. TeleMarketDeals undertakes some analysis of Levi's calling patterns, in particular his overseas calls, and recommends CheepCalls.

Levi's original request allowed TeleMarketDeals to on-disclose Levi's information to CheepCalls which offered the best rates for Levi.

However, TeleMarketDeals accidentally discloses an erroneous copy of Levi's information to CheepCalls. TeleMarketDeals contacts Levi and advises him of their error. Levi then requests that TeleMarketDeals provide the corrected information to CheepCalls.

CDR Privacy Safeguard 12 – Security of CDR data

1.128 An integral element of the CDR system is the protection of consumers' CDR data. As such, Privacy Safeguard 12 places a requirement on accredited data recipients, to ensure that CDR data is protected from misuse, interference and loss as well as from unauthorised access, modification or disclosure. ***[Schedule 1, item 1, subsection 56EN(1)]***

1.129 In addition, if an accredited data recipient no longer needs the CDR data for the purposes permitted by the consumer data rules or for the purposes as allowed under the CDR regime, then the redundant data must be destroyed or de-identified according to the consumer data rules. ***[Schedule 1, item 1, subsection 56EN(2)]***

1.130 Exceptions to this apply if the person is required under an Australian law (aside from the APPs), a foreign law or as a result of an order of a court or tribunal to keep the data. ***[Schedule 1, item 1, subsection 56EN(2)]***

Example 1.10

Nick currently banks with ZAP but is interested to see whether he is able to obtain a better deal on his credit cards with other banks and financial institutions.

Nick requests ZAP to transfer details of his credit card transactions and product information, which is part of the designated data set for the banking sector, to four other banks in order to test the offers they may be able to provide him.

In time, Nick considers the other offers and declines to transfer his banking business. He remains with ZAP.

The four other banks, who received Nick's credit card information are required by the consumer data rules to de-identify or destroy that information.

In this case, there is no applicable Australian law or court or tribunal order which requires them to retain Nick's CDR data.

Example 1.11

Following on from example 1.10 above, Bucks Banking retains Nick's data as they think he will come back to them and seek a credit card from them.

The consumer data rules require that once banking information is no longer required, it must be destroyed, and not de-identified.

Bucks Banking should have destroyed Nick's CDR data. The offers Bucks Banking provided to Nick expired after one month and he has not contacted Bucks Banking.

Bucks Banking complies with the ACCC's direction to destroy all CDR data that it is no longer using.

Correction of CDR data

CDR Privacy Safeguard 13 – Correction of CDR data

1.131 A CDR consumer has correction rights for CDR data that has been disclosed by a data holder in response to a valid request from that consumer. ***[Schedule 1, item 1, subsection 56EO(1)]***

1.132 Where the CDR consumer requests that the data is corrected, the data holder must correct the data, or include a statement with the data to ensure that the purpose for which it is held it is accurate, up to date, complete and not misleading. ***[Schedule 1, item 1, subsection 56EO(3)]***

1.133 The data holder must also give a statement about the correction or why a correction was not necessary. The consumer data rules may also specify actions that the data holder must take for in response to the correction request. ***[Schedule 1, item 1, subsections 56EO(1) and 56EO(3)]***

1.134 The same obligations as described above apply to an accredited data recipient when a CDR consumer request that data is corrected.
[Schedule 1, item 1, subsections 56EO(2) and 56EO(3)]