TREASURY LAWS AMENDMENT (CONSUMER DATA RIGHT) BILL 2018

EXPOSURE DRAFT 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*
CDR	Consumer Data Right
Commissioner	Commissioner at the Australian Competition and Consumer Commission
Information Commissioner	Australian Information Commissioner
OAIC	Office of the Australian Information Commissioner
Privacy Act	*Privacy Act 1988*
Privacy safeguards	Consumer Data Right privacy safeguards

Chapter 1
Consumer Data Right

Outline of chapter

1.1 The Consumer Data Right (CDR) will provide individuals and businesses with a right to efficiently and conveniently access specified data in relation to them held by businesses; and to authorise secure access to this data by trusted and accredited third parties. The CDR will also require businesses to provide public access to information on specified products they have on offer. CDR is designed to give customers more control over their information leading, for example to more choice in where they take their business, or more convenience in managing their money and services. Over time it is expected that these same benefits will be rolled out to other sectors of the economy.

1.2 The Government has committed to applying the CDR to the banking, energy and telecommunications sectors. The CDR relating to banking data is commonly referred to as "Open Banking".

1.3 CDR will reduce the barriers that currently prevent potential customers from shifting between banking and other service and utility providers. Through requiring service providers to give customers open access to data on their product terms and conditions, transactions and usage, coupled with the ability to direct that their data be shared with other service providers, we would expect to see better tailoring of services to customers and greater mobility of customers as they find products more suited to their needs.

1.4 The CDR places the value of consumer derived data in the hands of the consumer and will enable a range of business opportunities to emerge as new ways of using the data are discovered. Consumers will be the decision makers in the CDR system and will be able to direct where their data goes in order to obtain the most value from it.

1.5 Strong privacy and information security provisions are a fundamental design feature of the CDR. These protections include Privacy Safeguards and additional privacy protections through the consumer data rules. The OAIC will advise on and enforce privacy protections. Consumers will have a range of avenues to seek remedies for any breach of their privacy including access to internal and external dispute resolution.

Context of amendments

1.6 On 26 November 2017, the Government announced, as a partial response to the Productivity Commission's Inquiry into Data Availability and Use (the PC Data Report), the introduction of a Consumer Data Right (CDR) with application initially in the banking, energy and telecommunications sectors. The Government confirmed its commitment to the CDR and announced the creation of a new National Data Commissioner, as part of its full response to the PC Data Report on 1 May 2018.

1.7 In its response to the Productivity Commission's Data Report the Government announced that CDR will be introduced to provide individuals and businesses with a right to efficiently and conveniently access specified data about them held by businesses. Under the CDR consumers can also authorise secure access to this data by trusted and accredited third parties The CDR will also require businesses to provide public access to information on specified products they have on offer. A key feature of the right is that access must be provided in a timely manner and in a useful digital format.

1.8 On 20 July 2017, the Treasurer commissioned the *Review into Open Banking in Australia 2017* (Open Banking Review) to recommend the best approach to implementing Open Banking. The report recommended that Open Banking be implemented through a broader CDR framework. The report was then released for public consultation on 9 February 2018 and on 9 May 2018 the Government responded to the Open Banking Review, agreeing to all the recommendations, other than the recommendation about the timing for implementation.

1.9 The CDR implements recommendations from a wide range of reviews. Notably, the *Competition Policy Review 2015* (the Harper Review), was the first to recommend data access and portability rights in an efficient format across the economy. This recommendation was further developed in the Productivity Commission's *Inquiry into Data Availability and Use 2017* and the *Australia 2030: Prosperity through Innovation Review 2017* (ISA 2030).

1.10 A number of reviews have recommended data portability rights in specific sectors including the *Financial System Inquiry 2015* (the Murray Inquiry), the *Northern Australia Insurance Premiums Taskforce Final Report 2016,* the *Review of the Four Major Banks 2016* (the Coleman Review), the *Independent Review into the Future Security of the National Electricity Market – Blueprint for the Future 2017* (the Finkel Review), the draft report on *Competition in the Australian Financial System 2018,* COAG's report *Facilitating Access to Consumer Energy Data,* the Australian Small Business and Family Enterprise Ombudsman's

report *Affordable Capital for SME Growth*, and the ACCC's *Electricity Supply and Prices Inquiry 2018*.

1.11 The CDR provides access to a broader range of information within designated sectors than is provided for by Australian Privacy Principle (APP) 12 in the Privacy Act. While APP 12 allows individuals to access personal information about themselves, the CDR applies to data that relates to individual consumers, as well as business consumers. It also provides access to information that relates to products.

1.12 As the CDR covers both competition and consumer matters, as well as privacy and confidentiality concerning the use, disclosure and storage of data, the system will be regulated by both the ACCC and the OAIC. The ACCC will take the lead on issues concerning the designation of new sectors of the economy to be subject to the CDR and the establishment of the consumer data rules. The OAIC will take the lead on matters relating to the protection of individual and small business consumer participants' privacy and confidentiality, and compliance with the CDR privacy safeguards.

1.13 A Data Standards Body will also be established to assist a Data Standards Chair as he or she makes data standards. These data standards will explain the format and process by which data needs to be provided to consumers and accredited entities within the CDR system. Initially, this function will be undertaken by Data61 of the CSIRO.

Summary of new law

1.14 The CDR creates a new framework to enable consumers to more effectively use data relating to them for their own purposes. While initial application will be to the banking sector, the Government has committed that the telecommunications and energy sectors will soon also be subject to the CDR creating opportunities in these key areas of the economy for consumers to ensure that they are getting the best deal for their circumstances.

1.15 Further sectors of the economy may be designated over time, following sectoral assessments by the ACCC in conjunction with the OAIC.

1.16 The CDR framework gives consumers control over their consumer data. It will enable them to direct the data holder to provide their data, in a CDR compliant format, to accredited entities including other banks, telecommunications providers, energy companies or companies providing comparison services. CDR also allows consumers to access their own data without necessarily directing that the data be provided to a third party. The CDR system may also see the emergence of new data driven service providers.

1.17 The ACCC is provided with the power to make rules, in consultation with the OAIC, that will determine how CDR functions in each sector.

1.18 Entities must be accredited before they are able to receive consumer data. This will ensure that the accredited entities have satisfactory security and privacy safeguards before they receive CDR data.

1.19 Data relating to a consumer will be subject to strong privacy safeguards once a consumer requests its transfer to an accredited recipient. These safeguards are comparable to the protections for individuals contained in the APPs. The safeguards provide consistent protections for consumer data of both individuals and business enterprises. They also contain more restrictive requirements on participants than those applying under the Privacy Act.

1.20 The data must be provided in a format which complies with the standards. While the standards may apply differently across sectors, it is important that the manner and form of the data coming into the CDR system be consistent within and between designated sectors, as far as is practicable. This will promote interoperability, reduce costs of accessing data and lower barriers to entry by data driven service providers – promoting competition and innovation.

1.21 All individual and small business consumers in a designated sector to which the CDR applies will have access to dispute resolution processes to resolve disagreements with participants in the system. It is envisaged that sectors will access existing alternative dispute resolution arrangements, for example AFCA.

1.22 The CDR will provide the OAIC with the function of enforcing the privacy safeguards and providing individual remedies to consumers, while the ACCC will have the function of enforcing the balance of the regime and for taking strategic enforcement actions.

Comparison of key features of new law and current law

New law	*Current law*
The amendments to the CC Act to establish the CDR build upon APP 12 providing consumers with access to information about the transactions they enter into as consumers. Through designating sectors of the economy as participating in the CDR regime, over time consumers will be able to request that their information be provided to trusted recipients who will provide services including the ability to compare products and services to ensure that consumers are getting the best deal they can. The type of information consumers are able to request will be established through the instrument designating the sector, as well as clarification of this through consumer data rules made by the ACCC.	The Privacy Act provides the basis for nationally consistent regulation of privacy and the handling of personal information for a natural person. It balances protection of personal information with the interests of entities in carrying on their business functions or activities. This includes the APPs, which establish principles that require APP entities to consider the privacy of personal information. APP 12 establishes a principle to deal with requests for access to, and the correction of, personal information.
The ACCC is empowered to make consumer data rules, with the consent of the Minister, determining how the CDR applies in each sector. Consumer data rules may be made on all aspects of the CDR regime including accreditation of an entity, use, storage, disclosure and accuracy of CDR data, about the Data Standards Body and the format of CDR data and the data standards.	No equivalent.
The CDR will include privacy safeguards that provide an enhanced level of protection for CDR data relating to a CDR consumer that is, not CDR data about a product. This includes protection of information not covered by the APPs. The privacy safeguards provide minimum standards for the treatment	The APPs apply to the use, disclosure, storage and collection of personal information, as defined in the Privacy Act. The APPs continue to apply to CDR data held by data holders.

of CDR data. They can be supplemented by the consumer data rules to ensure CDR data is adequately protected. This also means that the system is able to respond flexibly to any emerging risks. The APPs will not create circumstances where a prohibited disclosure pursuant to the CDR safeguards will be 'authorised by law'. The APPs have been switched off and substituted by the CDR safeguards in respect of the use, disclosure, storage and collection of CDR data by accredited data recipients.	
Under the CDR, all businesses will similarly be able to access information covered by designated data sets.	The Privacy Act does not protect or facilitate access to businesses' information about themselves.
The Privacy Act will be expanded to protect the non-CDR data held by small businesses, if the small business is an accredited data recipient under the CDR system with an annual turnover of less than $3 million.	The Privacy Act does not bind small businesses, as defined in section 6D of that Act.
The Information Commissioner's functions will include functions conferred on him or her under Part IVD of the CC Act. The Information Commissioner (and the OAIC) will work with the ACCC in administering Part IVD of the CC Act.	The Information Commissioner undertakes his or her functions as established by the Privacy Act and other legislation which confers a power or function on the Information Commissioner.

Detailed explanation of new law

1.24 The Bill amends the CC Act to create the CDR which will apply to sectors of the economy that have been designated by the Minister. Under the CDR individuals and businesses can directly access or direct that their data be shared with certain participants.

1.25 Within a designated sector the types of data the CDR will apply to will be outlined via the designation instrument as well as the consumer data rules and, broadly speaking, the manner of making that data available will be established by the consumer data rules and the data standards.

1.26 The framework relies on three key participants – consumers, data holders and accredited entities. However, the system is flexible and may also provide via the consumer data rules, for interactions between consumers and non-accredited entities. It will be regulated, initially, by the ACCC and the OAIC. The OAIC has primary responsibility for complaint handling under the CDR framework with particular attention to the privacy of individuals and the confidentiality of small businesses. The ACCC will oversee the CDR from a consumer and competition perspective with particular focus on systemic enforcement. The ACCC will also be responsible for establishing the consumer data rules, in consultation with the OAIC. Each of the elements of the CDR system is explained below.

1.27 This Bill establishes a framework to enable the CDR to be applied to various sectors of the economy over time. As such, the Bill enables the ACCC to make consumer data rules covering a broad range of issues within the CDR framework. While it might appear that the ACCC is provided with significant powers to create consumer data rules and the framework is merely that, it is important to consider the broader context. The CDR will be applied across very different sectors of the economy which are already subject to various regulatory regimes. As a result, the Government considers it important to provide direction to the ACCC on the types of consumer data rules that can be made, balanced with the flexibility to make rules that are appropriate and adapted to any industry that might become designated into the future.

1.28 All legislative references are to the CC Act, unless otherwise specified.

Designated Sectors

1.29 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]***

1.30 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]***

1.31 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 potentially beneficial impact of designation and how that might impact consumers are considered. ***[Schedule 1, item 1, subparagraph 56AD(1)(a)(i)]***

1.32 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 OAIC will advise the Minister about the privacy of individuals and confidentiality of business consumers and oversee the privacy-related aspects of the CDR system. ***[Schedule 1, item 1, subparagraph 56AD(1)(a)(iii), subsections 56AD(3) and 56AE(2)]***

1.33 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 CDR is primarily designed to increase competition and enable consumers to harvest the value of their data. ***[Schedule 1, item 1, subparagraphs 56AD(1)(a)(ii), (iv) and (v)]***

1.34 The regulatory impact of designating a sector must be determined. While the CDR is intended to enhance competition, that should not occur at the expense of significant regulatory burden or disruption unless the broadly defined benefits of designation outweigh the regulatory impact. ***[Schedule 1, item 1, paragraph 56AD(1)(b)]***

1.35 The Minister is required to consult with the ACCC and the OAIC as well as any other person or body prescribed by regulations before designating a sector. The ACCC must undertake public consultation in relation to the potential designation of that sector before providing advice to the Minister. This public consultation can be achieved via publication to the ACCC website, but it is expected that the ACCC will engage with the potentially affected sector in order to better understand the benefits, regulatory impact and risk attached to designation. This approach is also consistent with obligations applying under Part 3 of the *Legislative Instruments Act 2003.* Understanding the risks associated with designation places the ACCC in a position to be able to counter those risks via the rule-making process. ***[Schedule 1, item 1, subsections 56AD(2) and 56AE(1)]***

1.36 The ACCC is also given the ability to make a recommendation to the Minister to designate a sector of the economy provided that the ACCC has first undertaken public consultation in relation to the impact and benefits of the CDR to the sector and consumers within the sector. ***[Schedule 1, item 1, subsections 56AE(3) and 56AE(4)]***

1.37 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. The banking sector will be designated by legislative instrument which will also outline the designated CDR data set. Acknowledging consultation undertaken in preparing the Open Banking Report, item 2 to this Bill provides that consultation is not required to be undertaken prior to designating the banking sector. ***[Schedule 1, item 2]***

Participants in the Consumer Data Right system

Data holders

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

1.39 Generally speaking, a data holder will be the entity that generates or collects the initial transaction records or data.

Example 1.1

BankY is a major Australian bank with many customers participating in the CDR regime; it regularly transfers those consumers' data at its consumer's direction.

BankY is a data holder for the banking sector. It generates and collects data that is subject to the CDR.

1.40 Data holders may also be prescribed in the consumer data rules. The consumer data rules may be used to specify circumstances where an accredited data recipient can handle CDR data as a data holder. This has the effect of changing the privacy protections applying to the CDR data with the APPs applying to a data holder's ongoing use of CDR data. ***[subsection 56AG(2)]***

1.41 For the banking sector, the instrument of designation will stipulate which Authorised Deposit-taking institutions (ADIs) the designation applies to and the data sets as captured by the designation. The consumer data rules will phase in ADIs, based on their size. It is expected that ADIs will need to transfer data collected or generated from 1 January 2017. The Government intends that the designation instrument will come into effect on 1 July 2019. The consumer data rules will detail

the phased implementation of Open Banking. ***[Schedule 1, item 1, subsection 56BA(2)]***

Accredited data recipients

1.42 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. CDR data held by accredited data recipients can also include data derived from consumer CDR data (including de-identified or aggregate data which is derived from CDR data). ***[Schedule 1, item 1, subsection 56AG(3)]***

1.43 In order to have had CDR data relating to a CDR consumer disclosed to it, the entity must hold an accreditation. Accreditation will initially be managed by the ACCC who will be the Data Recipient Accreditor. ***[Schedule 1, item 1, sections 56CA and 56CB]***

1.44 Further information on the accreditation process is outlined below, at paragraphs 1.64 to 1.74.

1.45 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 or if the consumer data rules mandate that outcome.

Example 1.2

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

Daniel 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 normally holds. BankY collects that data about Daniel as an accredited data recipient.

Because Daniel has transferred his banking business to BankY, and the consumer data rules provide that if a CDR consumer transfers their banking business the recipient bank is able to start treating all the CDR data it received under the CDR as a data holder (and subject to the APPs).

1.46 When in possession of a consumer's CDR data, an accredited entity can also be directed by a consumer to provide that data to other CDR participants. This is known as the principle of reciprocity.

1.47 In certain circumstances, CDR consumers can direct that their CDR data be provided to a non-accredited entity. Data that has been derived from CDR data, such as financial reports compiled from transaction data, may also be transferred by a CDR consumer out of the CDR system. For example, to their accountant. However, the collection, storage, use and disclosure of that information will be regulated via the APPs, if applicable. ***[Schedule 1, item 1, sections 56BB and 56BC)]***

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

CDR data and the CDR consumer

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

1.50 CDR data will be data that is outlined in the instrument designating a sector as a CDR sector and any information that is subsequently derived from that data. CDR data can include product information, transaction records or any other data specified in the designation; the data can relate to natural and legal persons. It will also include value-added data which is derived from the CDR data specified in the instrument.

1.51 Generally, there will broadly be three categories of CDR data – CDR data that relates to a CDR consumer or has been provided by the consumer, including CDR data that relates to a person's transactions, CDR data that relates to a product (such as product information data like that contained in a product disclosure statement) and CDR data that is derived from these 'primary' sources.

1.52 For the CDR regime, 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). As such, where information is primarily about a good or service, but may reveal information about a consumer's use of that good or service, it relates to the consumer.

1.53 The CDR consumer is broader than the CC Act definition of a consumer. This is because the CDR system will apply to business consumers. The CDR consumer is a person, including a small, medium or large business enterprise, for whom CDR data has been created or to whom it relates and that data is held by or on behalf of a data holder or accredited entity under the CDR system. ***[Schedule 1, item 1, subsections 56AF(4) and 56AF(5)]***

Example 1.3

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, MoneyDeals, 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.

1.54 It is an offence to knowingly engage in conduct that is or is likely to mislead another person into believing that a person is a CDR consumer or that they are making a valid direction to provide access to CDR data under the CDR when they are not. A civil penalty applies to actions that are likely to so mislead another person. ***[Schedule 1, item 1, section 56BM]***

Example 1.4

A phishing website misleads a consumer into believing they are logging into their bank to authorise CDR data access by a third party. They are actually being redirected to another site to capture login details.

The phishing website is breaching section 56BM.

Example 1.5

A person with stolen login details impersonates a CDR consumer to steal that consumer's CDR data. This is a breach of section 56BM.

Example 1.6

In order to gain access to a consumer's CDR data a business purports to be operating under the CDR system. As a result of this, the CDR consumer is misled into believing that they are transferring their CDR data under the CDR system and that, as a result, the access to and transfer of their CDR data would be protected by the applicable CDR consumer protections and remedies. Operating on this understanding, the CDR consumer transfers their CDR data to the business.

The business purporting to be operating under the CDR system is in breach of section 56BM.

Geographical application of this Part

1.55 Where data has been designated as CDR data, whether it is generated or collected outside of Australia is irrelevant if the CDR data has been generated or collected by or on behalf of a designated data holder who is either an Australian registered corporate entity or an Australian citizen or permanent resident. ***[Schedule 1, item 1, section 56AH]***

1.56 In practice this will mean that if a CDR consumer uses their Australian bank debit card to make a purchase in Singapore, then the transaction details for that transaction, being captured by the designation of CDR data for the banking sector, will be available for the CDR

consumer to direct their bank (as a data holder) to transfer within the CDR regime.

1.57 This is the intended outcome; if the data was collected or generated outside of Australia and the transaction occurred overseas, provided that the bank is registered in Australia.

Register of accredited entities and the Accreditation Registrar

1.58 For ease of reference by both consumers and other participants in the CDR system, a Register of Accredited Data Recipients (the Register) will be maintained by the Accreditation Registrar (the Registrar). Initially, the Registrar will be the ACCC but on an ongoing basis, the position of Registrar is subject to appointment by the Minister via a notifiable instrument. ***[Schedule 1, item 1, sections 56CK and 56CH]***

The Registrar

1.59 The Minister may appoint a person to act as the Registrar should the Registrar office become vacant on a temporary or permanent basis. ***[Schedule 1, item 1, section 56CI]***

1.60 Further, provision is made for the delegation of the functions or powers undertaken by the Registrar while that office is held by a Commonwealth entity. These delegations are to Australian Public Service (APS) officers at the Senior Executive Service (SES) level and below in order to ensure that lower level functions are appropriately performed by more junior public service staff. ***[Schedule 1, item 1, subsection 56CJ(1)]***

1.61 While the ACCC will undertake the role of the Registrar initially, this Bill allows for the role to be undertaken by a non-government entity in the future if the development of the data sharing ecosystem suggests that this is an appropriate option. In order to prepare for that possibility, provision is made for the Commonwealth to make a payment to the person or body in relation to their appointment to the role of Registrar or in relation to any other matters as prescribed by regulations made for the purposes of this section of the CC Act. ***[Schedule 1, item 1, subsection 56CH(4)]***

The Register of accredited entities

1.62 The Register must be made available in an electronic format. Matters relating to the ongoing maintenance of the Register including accuracy of entries, correction of errors, publication of all or part of the Register will be covered by consumer data rules, discussed below at paragraph 1.69. ***[Schedule 1, item 1, subsections 56CK(2) and (4)]***

1.63 To clarify, the Register is not a legislative instrument. Subsection 56CK(3) merely clarifies this and is not declaratory of the law. ***[Schedule 1, item 1, subsection 56CK(3)]***

Accreditation process

1.64 The Data Recipient Accreditor is responsible for the accreditation of entities to the CDR system. As noted above, initially the Data Recipient Accreditor will be the ACCC.

1.65 Accreditation will be based on criteria established in the consumer data rules about accreditation. While common criteria may be set to allow accreditation to be valid across sectors, the legislation provides flexibility for criteria to vary on a sector by sector basis.

1.66 Even if the person seeking accreditation is not registered as a corporation under the *Corporations Act 2001* they may apply for accreditation. ***[Schedule 1, item 1, paragraph 56CE(2)(a)]***

1.67 Similarly, a person does not have to be an Australian citizen nor a permanent resident in order to apply for accreditation. While there is no limitation of foreign entities becoming accredited, the rules may impose requirements to address any risks this may pose. ***[Schedule 1, item 1, paragraph 56CE(2)(b)]***

Example 1.7

A UK Fintech offers a budgeting app, which takes into account transaction data available under the UK Open Banking regime. They hold a UK Account Information Service Provider licence in order to do so under that regime. They wish to provide a similar service in Australia utilising account transaction data accessed under the Australian 'Open Banking' CDR system.

They must obtain accreditation under the CDR.

Example 1.8

Kathryn moves to the USA and wishes to transfer her banking and telecommunications information to Berkeley Bank, an American bank. Berkeley Bank is an accredited recipient under the CDR and offers to help Kathryn find the best telecommunications services in the USA for her needs. Kathryn is able to establish a line of credit in the USA using her Australian banking information, and Berkeley Bank helps her find internet and phone plans that allow her to call home as often as she did in Australia.

1.68 The accreditation process will also be detailed in the consumer data rules made by the ACCC.

1.69 Consumer data rules may be made:

- about the powers and functions of the Data Recipient Accreditor;
- about specific criteria to be applied to persons applying to be accredited under subsection 56CE(1);

- outlining that accreditations may only be provided subject to applicants meeting certain conditions, including the ongoing imposition of conditions on accredited entities after accreditation has been granted;
- allowing for accreditation to be provided at different levels taking into account the different risks associated with the kind of activities undertaken within that designated sector or the kinds of applicants;
- relating to the period, renewal, transfer, variation, suspension, revocation or surrender of accreditations;
- outlining transitional rules for when an accreditation is suspended or ends and the treatment of data under such circumstances; and
- about the Register of Accredited Data Recipients.

[Schedule 1, item 1, section 56BF]

1.70 It is expected that the ACCC will make rules to cover each of the above aspects of the accreditation process and that these rules may apply sector by sector or could apply to a range of sectors or all sectors subject to a designation.

1.71 The ACCC is provided with these broad rule making powers about the accreditation process in order to enable it to make rules specific to individual sectors of the economy. This will ensure that the accreditation process for each sector is appropriate and adapted to that sector. It will reduce unnecessary regulation and ensure that transitioning to the CDR system is as smooth as possible.

1.72 Enabling a differentiation for accreditations with regard to different levels of risk means that some entities will have to meet a higher standard in order to be accredited to receive certain types of higher risk data. In this way, accreditation may be tiered. ***[Schedule 1, item 1, paragraph 56BF(2)(a)]***

Example 1.9

An Australian Fintech, with the CDR consumer's consent, seeks only CDR data on the balance of an account. The rules might provide they only require a lower level of accreditation to access this data.

Example 1.10

Australian banks must comply with fit and proper person, confidentiality and information security requirements imposed by the Australian Prudential Regulation Authority. The accreditation criteria and the process for accreditation in the rules may provide for full or partial recognition of these arrangements, to provide for a streamlined process for accreditation.

1.73 The ACCC may also make a rule in relation to establishing a fee for accreditation. This fee is not a tax and, as such, must reflect the administrative cost of the accreditation process. ***[Schedule 1, item 1, subsection 56BF(2)]***

1.74 Consumer data rules may also be made in relation to reporting and record keeping requirements to be met by accredited data recipients. Further detail on these consumer data rules is below at paragraphs 1.99 to 1.102.

Review of decisions refusing to accredit

1.75 If the Data Recipient Accreditor refuses to grant an accreditation under subsection 56CE(1), the entity applying for an accreditation is able to seek review of the Data Recipient Accreditor's decision at the Administrative Appeals Tribunal (AAT). ***[Schedule 1, item 1, section 56CF]***

1.76 In addition, the consumer data rules may cover the variation, suspension or revocation of an accreditation. ***[Schedule 1, item 1, section 56BF]***

1.77 Where the consumer data rules do outline processes for the variation, suspension or revocation of accreditations, these rules may also provide for AAT review of those decisions. ***[Schedule 1, item 1, section 56BH and Note to section 56CF]***

1.78 In the absence of an express reference in the consumer data rules to AAT review of the ACCC decision respecting variation, suspension or revocation, these decisions are administrative in nature and will be subject to judicial review under the *Administrative Decisions (Judicial Review) Act 1977*.

Prohibition on holding out

1.79 In order to protect CDR consumers and others participating in the CDR system it is an offence to behave in such a way as to create or foster the perception by others that you are an accredited data recipient. This equally applies to a failure to correct the perception that you are accredited, when you are not. ***[Schedule 1, item 1, section 56CG]***

1.80 An act or omission which results in others holding the belief that you are a person with an accreditation under subsection 56CE(1) or that you are a person holding an accreditation that has been granted at a particular level and therefore able to deal with sensitive CDR data, when you do not have this level of accreditation, is an offence. ***[Schedule 1, item 1, section 56CG]***

Consumer Data Rules

1.81 Key elements of the CDR framework will be governed by consumer data rules.

1.82 The consumer data rule making powers provide substantial scope for the ACCC to make rules about the CDR. This is because it is important to be able to tailor the consumer data rules to sectors and this design feature acknowledges that rules may differ between sectors. Variance between sectors will depend on the niche attributes of the sector and consumer data rules will be developed with sectoral differences in mind in order to ensure existing organisational arrangements, technological capabilities and infrastructure are able to be leveraged and harnessed as appropriate. Regulatory burden will also be managed via this process. ***[Schedule 1, item 1, section 56BA]***

1.83 Within sectors, CDR data may fall into different categories or classes. Some categories of CDR data may require more stringent security standards with respect to storage of the data. As such, the ACCC is provided with the ability to make different rules about different classes of CDR data within designated sectors. ***[Schedule 1, item 1, paragraph 56BA(2)(b)]***

1.84 Consumer data rules will also enable the ACCC to make different rules relating to different classes of persons within designated sectors and how different classes of persons are able to receive CDR data. ***[Schedule 1, item 1, paragraphs 56BA(2)(c) and (d)]***

1.85 The ACCC may make consumer data rules on a range of elements of the CDR system. In particular, the consumer data rules may apply to:

- disclosure, use, accuracy, storage, security or deletion of CDR data; ***[Schedule 1, item 1, subsections 56BB(a) and (b) and section 56BC and 56BD]***
- accreditation of data recipients; ***[Schedule 1, item 1, subsection 56BB(c) and section 56BF]***
- reporting and record keeping; ***[Schedule 1, item 1, subsection 56BB(d) and section 56BG]***
- any other matters incidental to the CDR system. ***[Schedule 1, item 1, subsection 56BB(e) and section 56BH]***

1.86 While the scope of the potential rule making powers is very broad, this is by design. As noted above, it is important that the ACCC be able to make rules that can be tailored to vastly different sectors. While in the initial roll out it is expected that the banking, telecommunications and aspects of the energy sector will become designated and subject to the CDR, in the future it is possible that insurance information or retail loyalty cards, and the value-added data relating to those cards, may be subject to the CDR system.

1.87 As noted below, at paragraphs 1.125 to 1.130, the ACCC cannot make consumer data rules without the Minister's consent other than emergency rules where the Minister has the power to direct their

subsequent repeal or variation. The ACCC is required to consult publicly when making rules, and must consult the OAIC prior to seeking the Minister's consent.

1.88 It is important to note that any consumer data rules made by the ACCC are disallowable instruments. The Parliament will have the ability to oversee the making of consumer data rules and, in this way, will be able to reflect the views of the Australian public in relation to the new CDR system.

1.89 The consumer data rules cannot require a CDR participant to disclose CDR data before 1 July 2019 or impose a retrospective commencement or application. ***[Schedule 1, item 1, subsection 56BI(1)]***

1.90 Further, regulations may limit matters that the consumer data rules are able to deal with or the requirements the rules can impose about aspects of the CDR system including data sets or kinds of persons. ***[Schedule 1, item 1, subsection 56BI(3)]***

Disclosure, use, accuracy, storage, security or deletion of CDR data

1.91 The consumer data rules will outline requirements to be met by CDR participants (data holders, accredited entities or consumers), about disclosure of CDR data where that data relates to a person or in cases when it does not relate to a CDR consumer. Information which does not relate to a CDR consumer will include general product information.

1.92 The disclosure rules will cover matters such as how consumers consent to the disclosure of their CDR data and the processes under which data holders and accredited entities must disclose CDR data. The disclosure rules will work in conjunction with the CDR privacy safeguards in regulating the disclosure of CDR data. It is expected that if consent is required for the disclosure of a type of CDR data, that consent will be express. ***[Schedule 1, item 1, sections 56BB and 56EI]***

1.93 The CC Act is amended to enable the ACCC to make consumer data rules to ensure that there are appropriate safeguards in place for disclosure of CDR data in the two circumstances contemplated above – where there is an identifiable CDR consumer and where there are no CDR consumers for the information because it relates to a product or other information. ***[Schedule 1, item 1, sections 56BB, 56BC and 56BD]***

1.94 Importantly, authority to disclose CDR data is generally restricted and a valid request from the CDR consumer must be in place. The consumer data rules will establish the framework relating to requests, including establishing different levels of authorisation to be provided reflecting the more sensitive nature of some of the information that will become CDR data. ***[Schedule 1, item 1, subsection 56BC(b)]***

1.95 An important feature of the CDR is the consumer's consent to the disclosure of the CDR data. Consumer data rules will be made to

provide guidance to both CDR consumers as well as other participants in the CDR system on the matters that have to be satisfied in order to demonstrate that consent was obtained and the CDR consumer understood what it was they were consenting to. The rules will prescribe the process for obtaining consent and how to ensure that consent it genuine. However, it is not intended to make this element of the CDR system so complex as to discourage participation. The role of the consumer data rules is to balance the sensitivity of the CDR data with the need for security, efficiency and convenience.

1.96 The consumer data rules may also establish that a fee is payable in relation to the disclosure of certain class or classes of information under the CDR. These fees must not amount to taxation. The ability to set a fee acknowledges that some CDR data may be value-added data, or that in limited circumstances, provision of data for free would impact on incentives for data holders to collect data. In these cases, a fee for access and use may be appropriate or required if there is an acquisition of property (see paragraphs 1.266 to 1.271 below on acquisition of property). ***[Schedule 1, item 1, subsections 56BC(d) and (e) and 56BD(d) and (e)]***

Accreditation of data recipients

1.97 As noted above, at paragraphs 1.65 to 1.73, consumer data rules will be made about the accreditation of data recipients under the CDR system.

1.98 This will also include the processes for de-accreditation or suspension of accreditation should an accredited entity breach the consumer data rules (or other relevant Australian law).

Reporting and record keeping

1.99 The ACCC will make consumer data rules on reporting and record keeping including outlining the requirements for CDR participants to give specified reports to the ACCC, to the Information Commissioner or to the CDR consumer. ***[Schedule 1, item 1, section 56BG]***

1.100 The content and nature of these reports may vary between designated sectors and will depend on the information a CDR consumer requires to manage their authorisations and consents or information that the ACCC or the OAIC requires in order to fulfil its responsibilities regulating the relevant aspects of the CDR system.

1.101 It is expected that CDR participants will be required to provide specified reports to the ACCC or the OAIC for the purpose of those regulators enforcing compliance with all aspects of the CDR. ***[Schedule 1, item 1, subsection 56BG(b)]***

1.102 Record keeping requirements will relate to ensuring compliance with the consumer data rules and will be used by both regulators for this purpose.

Example 1.11

A CDR consumer in the banking sector wishes to review the CDR data access permissions they have granted, in order to determine which permissions to cancel. The consumer data rules require all banks to provide convenient online access to a dashboard displaying all of the permissions the CDR consumer has granted.

Example 1.12

A CDR consumer lodges a complaint with the OAIC that a bank disclosed their CDR data without their consent. The consumer data rules require banks to keep records regarding CDR consumers' directions to disclose CDR data.

The OAIC obtains these records as part of its investigation into the complaint.

Incidental or related matters

1.103 Consumer data rules may also be made about the following incidental matters:

- requirements about the data standards; ***[Schedule 1, item 1, subsection 56BH(a)]***
- circumstances where persons are relieved from compliance with the consumer data rules that would otherwise apply to them; ***[Schedule 1, item 1, subsection 56BH(b)]***
- consumer data rules with respect to internal review process that participants must establish and have in place for CDR as well as internal dispute resolution processes; ***[Schedule 1, item 1, subsections 56BH(d) and 56BH(f)]***
- consumer data rules may be made about external dispute resolution processes; ***[Schedule 1, item 1, subsections 56BH(g) and 56BH(h)]***
- transitional rules with regard to external resolution of disputes; ***[Schedule 1, item 1, subsection 56BH(i)]***
- requirements for documents to be provided in a form approved by either the Commission or the Information Commissioner; and ***[Schedule 1, item 1, subsection 56BH(e)***
- any other matters about the consumer data rules. ***[Schedule 1, item 1, subsection 56BH(i)]***

1.104 Some of these matters are covered by other Divisions of the Consumer Data Right Part (Part IVD of the CC Act). In particular, as

discussed below at paragraphs 1.151 to 1.156, dispute resolution processes are specifically required by participants in the CDR system.

1.105 Other matters, including requirements about approved forms and where CDR participants may be excused from compliance with certain consumer data rules are provided to enable both flexibility within the CDR system and to ensure that interactions between the regulators and CDR participants is smooth, clear and transparent and obligations established by the consumer data rules are well understood.

1.106 Consumer data rules are able to be made with respect to other matters including the data standards (discussed below at paragraphs 1.131 to 1.150), the de-accreditation and suspension of accreditation and other related matters as well as extensions or clarification of the privacy safeguards. Consumer data rules are not to be inconsistent with the privacy safeguards or any other part of the CDR legislation.

Matters not covered by the consumer data rules

1.107 There are also limitations on the scope of the consumer data rules. In line with the proposed commencement date for this Bill, the consumer data rules are unable to require a CDR participant to disclose data that becomes CDR data from 1 July 2019, prior to that date. ***[Schedule 1, item 1, subsection 56BI(1)]***

1.108 The consumer data rules may apply to require a person to do something in relation to CDR data that was generated or collected by the person on a date earlier than the commencement of this Bill. This is an important point as it ensures that CDR data that is generated prior to the designation of a sector is able to be accessed as soon as that sector becomes designated and, in practice, means that CDR consumers are able to access their CDR data without a lag period during which the relevant data holder collects information post-designation. ***[Schedule 1, item 1, subsection 56BI(2)]***

1.109 A further limit to the consumer data rules is possible via regulation. The regulations may provide that consumer data rules are unable to deal with matters specified in regulation or that the consumer data rules should not impose certain requirements. ***[Schedule 1, item 1, subsection 56BI(3)]***

1.110 Consumer data rules will also be limited by the designation instrument that will describe the CDR data sets and CDR data holders for the relevant sector. The ACCC's consumer data rule making power will be limited to data and entity types prescribed in the instrument. For the banking sector, the designation instrument will prescribe that all ADIs provide data as described in the designation and the rules. If non-ADI lenders are not captured by the Minister's designation, the ACCC would only be permitted to require non-ADI lenders to provide data they hold if

that data falls within the definition of CDR data for the banking sector, and if they were accredited data recipients.

1.111 Each of these elements works with the very nature of the consumer data rules, being legislative instruments and subject to Ministerial oversight and Parliamentary scrutiny, to ensure that the consumer data rules remain appropriate and adapted. So while it is clear that the ACCC is provided with significant scope in relation to the rule making power, this is both balanced and appropriate. As noted above, the consumer data rule making power enables the ACCC to tailor the rules to each sector as a 'one size fits all' approach would not be appropriate as the CDR roll out to varied sectors of the economy. The ability to come back to Parliament to make more rules at each new designation would limit the ability of the CDR to expand and provide competition benefits to consumers in various sectors of the economy as they access and direct their own information via CDR.

Example 1.13

A CDR consumer seeks to use the CDR system to access specified CDR data generated between 2002 and 2018. While the legislative framework potentially enables access to CDR data collected prior to the commencement of the CDR system, either the sector designation instrument (defining CDR data sets the CDR applies to in that sector) or regulations provide that data holders must only provide access to CDR data for a 6 year period from the commencement of the designation instrument.

The Minister set these limitations informed by the ACCC's sectoral assessment, which examined the data retention and retrieval arrangements for that sector. Nuances regarding some data sets that only started to be collected more recently were dealt with by the ACCC through the rules.

Compliance with the consumer data rules

1.112 It is a requirement of the CC Act that CDR participants comply with the consumer data rules. ***[Schedule 1, item 1, section 56BJ]***

1.113 A transaction will not be invalidated by a failure to comply with the consumer data rules. That is, merely because a CDR participant has not complied with a civil penalty provision or other requirement of the consumer data rules, the relevant transaction is not rendered invalid. Equally, any rights or obligations arising under or in relation to the transaction will not be impacted. ***[Schedule 1, item 1, section 56BL]***

1.114 The obligation to comply with the consumer data rules is capable of enforcement through the CC Act's existing infringement notice provisions located in Division 2A of Part IVB (relating to industry codes). ***[Schedule 1, item 1, section 56BK]***

1.115 Division 2A of Part IVB applies to the CDR as if references to civil penalties in the consumer data rules and Part IVD are a reference to an industry code. The ACCC is highly familiar with the existing infringement notice regime in the CC Act, and its extension to the consumer data rules is appropriate. ***[Schedule 1, item 1, section 56BK]***

1.116 In addition, section 155 of the CC Act is extended to apply to contraventions of Part IVD and the consumer data rules. This means that the ACCC will be empowered to obtain information, documents and evidence in order to determine whether there has been a breach of this Part or the consumer data rules. ***[Schedule 1, item 47, subsection 155(9AA)]***

1.117 The extension of the ACCC's existing coercive information gathering powers under subparagraph 155(2)(b)(i) of the CC Act is necessary to allow it to compel the provision of information for all of its CDR functions including sector designation, rule making, accreditation-related functions, as well as auditing and enforcement of the CDR. This extension of the ACCC"s section 155 powers will allow the ACCC to determine which data sets actually exist in new sectors by being able to request this information.

1.118 The ACCC will undertake a significant new role of accrediting data recipients for the CDR. The extension of subparagraph 155(2)(b)(i) allows the ACCC to randomly audit accredited data recipients to ensure their use of data is in accordance with consumer consents and security protections are in place. This will help to ensure confidence in the accreditation process, and confidence that consumer consent will be meaningful. Finally. The subparagraph 155(2)(b)(i) powers will allow the ACCC to monitor the broad 'data system' to ensure that it does not develop in a manner that could harm consumers or undermine the stability of other systems. Given the ACCC's familiarity with the existing powers conferred by section 155 of the CC Act, and the requirement for such powers to be made available for the CDR, it is appropriate that section 155 be extended rather than a new provision be created replicating the powers and functions in existing law. ***[Schedule 1, item 46, subparagraph 155(2)(b)(i)]***

Process for making consumer data rules

1.119 The ACCC is required to consider a range of matters prior to making consumer data rules. These matters include the likely impact of the proposed rules on the economy, with particular reference to the sector of the economy that has been designated. This should include consideration of the impact of the rules on consumers, competition, innovation, privacy and confidentiality and relevant markets. ***[Schedule 1, item 1, section 56BN]***

1.120 The ACCC must also consider the regulatory impact of the proposed consumer data rules. While it is important that the consumer

data rules enable a safe use of consumer data, this must be balanced with the likely regulatory burden arising from the rules. The ACCC will weigh each of these factors when both advising the Minister about designation and when making consumer data rules. ***[Schedule 1, item 1, section 56AD(2), 56AE(1) and 56BN]***

1.121 The CDR requires the ACCC to consult with the public, the Information Commissioner, the particular designated sector and any other persons prescribed by regulations before making consumer data rules. ***[Schedule 1, item 1, section 56BO]***

1.122 Consultation with each of these key communities is essential to ensure that the right balance is struck between protection of individuals' rights including the right to privacy, as well as making sure that the regulatory burden does not outweigh the broadly defined benefits to be gained from the consumer data rules. While a failure to consult will not invalidate the consumer data rules, it is expected that the ACCC will always consult. Again, the consumer data rules are disallowable instruments so the Parliament does have the capacity to intervene, if it considers a rule to be egregious.

1.123 A further protection and limitation on the ACCC's ability to make consumer data rules is that the ACCC must, except in emergency circumstances, obtain the Minister's consent, in writing, prior to making a rule. ***[Schedule 1, item 1, section 56BP]***

1.124 The Minister's consent is not a legislative instrument because it is covered by the exemption in table item 4 of section 6 of the *Legislation (Exemptions and other Matters) Regulation 2015*.

1.125 As noted above at paragraph 1.87, the ACCC may make consumer data rules without the Minister's consent in emergency situations. ***[Schedule 1, item 1, section 56BQ]***

1.126 This will provide the ACCC with the ability to make rules if the ACCC is of the view that making the rules is necessary or in the public interest to protect the efficiency, integrity and stability of any aspect of the Australian economy or if there is an imminent risk of serious harm to consumers. ***[Schedule 1, item 1, subsection 56BQ(1)]***

1.127 If the ACCC makes an emergency rule under section 56BQ then it is required to advise the Minister on the following day and to provide the Minister with a written explanation of the need for the emergency consumer data rules. ***[Schedule 1, item 1, paragraph 56BQ(2)(a)]***

1.128 The Minister may then respond by advising that the consumer data rule be either amended or revoked, in accordance with the written direction of the Minister. ***[Schedule 1, item 1, paragraph 56BQ(2)(b)]***

1.129 The Minister's direction to vary or revoke a rule is not a legislative instrument because it is also covered by the exemption in table

item 4 of section 6 of the *Legislation (Exemptions and other Matters) Regulation 2015*. ***[Schedule 1, item 1, section 56BQ(5)]***

1.130 The ACCC is provided with the scope to respond to an emerging issue, for example, a previously unforeseen practice which presents an imminent risk of harm to consumers, swiftly and with flexibility. The appropriate checks and balances still exist with Ministerial oversight and the ability of the Minister to amend or revoke the emergency consumer data rule, if the Minister considers that action necessary.

Data standards and the Data Standards Body

The Data Standards Body and the Chair of the Data Standards Body

1.131 The Bill creates a Data Standards Body function is in order to oversee the function of creating data standards which will apply to the CDR regime. The Bill does not create a new entity but rather allocates new functions and powers to an existing body.

1.132 The Minister will appoint both the Chair of the Data Standards Body and the Body tasked to undertake the function of the Data Standards Body. Initially, it is expected that the Data Standards Body and function will be undertaken by CSIRO's data arm, Data61. ***[Schedule 1, item 1, section 56FA]***

1.133 The length of appointment applying to the position of Chair of the Data Standards Body will be specified in the instrument appointing the Chair. This period must not exceed three years. ***[Schedule 1, item 1, subsection 56FA(2)]***

1.134 Minister may terminate the appointed Data Standards Chair with cause including misbehaviour, bankruptcy or physical or mental incapacity to undertake the duties of the Chair. ***[Schedule 1, item 1, subsections 56FA(4) and (5)]***

1.135 The Minister is able to terminate the appointment of the Data Standards Body without cause. This is appropriate given that the Chair is vested with the independence to make key decisions. The ability to terminate without cause may also support the future shifting of the Data Standards Body support function to other entities. These terminations must be in writing. ***[Schedule 1, item 1, subsections 56FA(5), (6) and (7)]***

1.136 The Bill confers a range of powers and functions on the Data Standards Body and the Chair of that Body. Primarily, the functions of the Chair include making data standards consistent with the consumer data rules relating to data standards. The functions of the Data Standards Body are limited to facilitating the Chair in this role.

1.137 Administrative provisions to enable the office of the Chair of the Data Standards Body to function are inserted including the ability to delegate any of the Data Standards Chair's powers or functions to staff of

the Data Standards Body. The delegation power does not include the Chair's ability to make data standards. ***[Schedule 1, item 1, section 56FD]***

1.138 Where a power or function has been delegated, the delegate must act consistently with a direction of the Data Standards Chair. ***[Schedule 1, item 1, subsection 56FD(5)]***

Data standards

1.139 Data standards will be made by the Data Standards Chair to complement the consumer data rules relating to data sharing in order to facilitate the sharing and use of consumer data within a designated sector. ***[Schedule 1, item 1, section 56FE]***

1.140 Matters that can be covered in the data standards will be subject to consumer data rules. That is, the ACCC may make rules to control the content and process of standards made by the Data Standards Chair including in relation to the process for making data standards, and when data standards are mandatory or voluntary. For example, the ACCC may recognise a data standard as mandatory by adopting it through the rules. ***[Schedule 1, item 1, subsection 56GB(2)]***

1.141 In this way, the ACCC will be able to monitor and limit the scope of standards made by the Data Standards Chair. The ACCC will be able to make rules providing the Data Standards Body with guidance on how the data standards should be made. These rules will cover the process for making, varying or revoking the data standards and can include rules relating to consultation requirements. ***[Schedule 1, item 1, subsection 56FE(4)]***

1.142 The ACCC may also make rules relating to the governance arrangements of the Data Standards Body. ***[Schedule 1, item 1, section 56BH)]***

1.143 The data standards are not legislative instruments. ***[Schedule 1, item 1, subsection 56FE(5)]***

1.144 The data standards will be largely in the nature of specifications for how information technology solutions must be implemented to ensure safe, efficient, convenient and interoperable systems to share data. They will only describe how the CDR must be implemented in accordance with the rules which will set out the substantive rights and obligations of participants.

1.145 These information technology specifications will be living documents subject to continual change, in order to adapt to changing demands for functionality and available technology solutions. This legislative framework is similar to the Market Integrity Rules (which are legislative instruments) and financial market operating rules (which are multilateral contracts) supported by section 793B of the *Corporations Act 2001*. It is designed to ensure maximum flexibility at the level of the data standards.

Legal effect and enforcement of the data standards

1.146 Data standards apply to data subject to the CDR. As such, they will prescribe the format of data, method of transmission and security requirements for data to be provided by a data holder or accredited data recipient to a consumer or to one another. If a data holder or an accredited data recipient is unwilling or unable to provide the designated data set in a format that is consistent with the data standards, then the party who is seeking the information is able to seek redress.

1.147 When a data standard is applied by the consumer data rules to a data holder or an accredited data recipient, that standard will operate as a multilateral contract between CDR participants. What this means is that a data holder or an accredited entity will be able to enforce the contractual right they have under the CDR to access data in a format and manner consistent with the data standards. Enforcement of these contractual rights would be subject to any dispute resolution arrangement provided for in the rules. ***[Schedule 1, item 1, section 56FF]***

1.148 This contractual obligation applies to data holders and accredited entities.

1.149 Further, the CDR provides a right to seek enforcement of the data standards in a court. If a person seeking CDR data has been unable to access that data in a format consistent with the data standards, then either the ACCC or the Information Commissioner or the person aggrieved by the inability to access the relevant data, may apply to the Court to have the matter resolved. ***[Schedule 1, item 1, section 56FG]***

1.150 The Court is provided with the ability to give directions in a matter brought before it about compliance with or enforcement of the data standards. ***[Schedule 1, item 1, subsection 56FG(2)]***

Dispute Resolution

1.151 As noted above at paragraphs 1.103 and 1.104, the consumer data rules may require CDR participants to have internal or external dispute resolution processes that either relate to the consumer data rules or meet criteria which are outlined in the consumer data rules. ***[Schedule 1, item 1, subsections 56BH(f) and (g)]***

1.152 Division 4 provides further guidance about external dispute resolution schemes and processes. Acknowledging that there are a variety of external dispute resolution schemes available within several sectors of the economy, such as AFCA, the Telecommunications Industry Ombudsman, and State and Territory Energy Ombudsmen, the CDR regime intends to leverage these existing schemes when appropriate. This is akin to the power of the Information Commissioner to recognise these schemes under the Privacy Act.

1.153 External dispute resolution schemes are generally utilised for disputes involving consumer complaints. The power for the consumer data rules to impose external dispute resolution arrangements can extend to arrangements not involving a standing scheme recognised under Division 4. For example, the use of independent commercial arbitrators which may be more appropriate for disputes between data holders and accredited data recipients or between accredited data recipients. ***[Schedule 1, item 1, subsections 56BH(f) and (g)]***

1.154 To facilitate this, the ACCC may, by notifiable instrument, recognise an external dispute resolution scheme for the resolution of issues relating to the consumer data rules or the CDR. ***[Schedule 1, item 1, section 56DA]***

1.155 To ensure the appropriateness of a proposed external dispute resolution scheme for the CDR system, the ACCC will consider how accessible the scheme is as well as the level of independence with which the scheme operates, prior to making an instrument which recognises any scheme for the CDR. ***[Schedule 1, item 1, subsection 56DA(3)]***

1.156 Acknowledging the dual role the ACCC plays with the OAIC and the Information Commissioner in regulating the CDR system, the ACCC is also required to consult with the OAIC prior to recognising an external dispute resolution scheme for the CDR. ***[Schedule 1, item 1, subsection 56DA(4)]***

Regulation of the CDR system by the ACCC and the OAIC

1.157 As noted above, the ACCC and the OAIC will work together in regulating conduct under the CDR. This will be achieved via various amendments to the CC Act and the *Australian Information Commissioner Act 2010* (AIC Act). Further, the CDR functions of the Information Commissioner are outlined at section 56GA. ***[Schedule 1, item 1, section 56GA]***

1.158 The AIC Act is amended at sections 9 and 29 to ensure that the OAIC and the Information Commissioner's privacy functions (as defined by the AIC Act) extend to Part IVD of the CC Act. This ensures that the regulatory framework supporting those Privacy Act functions may be applied to their CDR functions. ***[Schedule 1, items 3, 4 and 5, section 4, subsection 9(1) and paragraph 29(2)(a) of the Australian Information Commissioner Act 2010]***

1.159 Through amendment to the CC Act, the Commission may delegate any of its powers or functions under Part VI or section 155 relating to the consumer data rules to the Information Commissioner or a member of staff of the OAIC. ***[Schedule 1, items 7 and 8, subsection 26(1) and section 26]***

1.160 As noted below at paragraph 1.252, the dual regulatory model provided for the CDR enables the Information Commissioner to delegate

his or her privacy safeguard enforcement powers or functions to the Commission or a member of staff of the Commission. ***[Schedule 1, item 1, section 56EW]***

1.161 Further, section 157AA is inserted to the CC Act in order to enable the Commission or a Commission official to disclose information to the Information Commissioner or a member of staff of the OAIC. ***[Schedule 1, items 50 and 51, section 157AA]***

Compliance with and enforcement of Part IVD and the consumer data rules

1.162 As noted above in relation to compliance with Part IVD, to effectively ensure compliance with the consumer data rules, the rules may specify that a civil penalty applies to breaches of the rules. ***[Schedule 1, item 1, section 56BJ]***

1.163 This is considered necessary because the consumer data rules will be the primary mechanism through which consumers and their data are protected. This will also ensure that the competition elements of the CDR, such as the right to access and transfer CDR data, are able to be enforced. Given that the CDR may be rolled out across a broad range of industries, it is not practicable to place all of the detail that will be contained in the consumer data rules in the primary legislation. To do so would impede the ability of the CDR to be applied across varied sectors where consumers may be able to see the benefit of harnessing their own data and applying that to achieve a better deal on items such as banking and energy costs, telecommunication costs and grocery and fuel bills.

1.164 It is also worth noting that consumer data rules are disallowable instruments and, as such, the Parliament will have oversight of them and the ability to disallow the imposition of a civil penalty via the rules if the Parliament considered such a penalty to exceed requirements for compliance.

1.165 Civil penalty provisions of the consumer data rules will be enforced consistently with existing provisions of the CC Act. ***[Schedule 1, items 9 - 49, sections 76, 76B, 80, 82, 83, 84, 86, 86C, 86D, 86E, 86F, 87, 154A, 154V, 155 and 155AAA]***

1.166 The amendments outlined above extend the following existing provisions of the CC Act, and associated powers of the ACCC, to Part IVD:

- Section 76 – provides that the ACCC is able to seek the application of pecuniary penalties if a court is satisfied of a breach of relevant parts of the CC Act. This provision has been extended to apply to Part IVD the Consumer Data Right;
- Section 80 – provides that the ACCC may apply to the court for an injunction where a person is undertaking, or proposing to

undertake conduct which would contravene parts of the CC Act including Part IVD;

- Section 82 – creates an action for damages. This provision of the CC Act is amended to ensure that a person who suffers damage or loss as a result of a breach of Part IVD is able to recover the amount of the damage or loss sustained;
- Section 86C – non-punitive orders is extended to enable the ACCC to seek application of a non-punitive order for a breach of the consumer data rules and/or Part IVD of the CC Act;
- Section 86D – adverse publicity order may also be made by a court where a person has been found in contravention of Part IVD and has been ordered to pay a pecuniary penalty under section 76;
- Section 86E – the ability to apply for an order disqualifying a person from managing corporations is extended to breaches of Part IVD and/or the consumer data rules;
- Section 87 – this provision creates the ability to seek application of other orders. It is extended to breaches of Part IVD and/or the consumer data rules;
- Section 155 – this provision contains power to obtain information, documents and evidence and it is extended to cover Part IVD and the consumer data rules. This means that the ACCC and the Information Commissioner and OAIC, should a delegation be in place under section 26 of the CC Act, may use this power in order to obtain information and documents both in relation to a breach of Part IVD or the consumer data rules or the suspicion of a breach of this Part or the rules, or in their performance of a function or power under Part IVD (except as regards the privacy safeguards). As such, this power is extended to the CDR and will enable investigations to be undertaken to ensure compliance with the CC Act.
- Division 2A of Part IVB about infringement notices is also extended to the CDR regime as if reference to industry codes in that Division were also references to consumer data rules.

1.167 Given that the CDR system will operate in many varied sectors of the economy, it is important to clarify that a failure to comply with the consumer data rules will not impact the underlying transaction. That is, if for example a bank failed to comply with the consumer data rule to make transaction records available to a consumer in the specified form, that will not invalidate the underlying transactions between the consumer and their bank. ***[Schedule 1, item 1, section 56BL]***

CDR Privacy Framework

1.168 Division 5 creates the CDR privacy safeguards. It is useful to understand how the privacy safeguards work in relation to the Privacy Act and APPs. Generally speaking, the Privacy Act and the APPs will continue to apply to data holders under the CDR (as defined by section 56AG) placing additional requirements on data holders once a request for CDR data has been received.

1.169 For accredited data recipients (as defined by section 56AG), the privacy safeguards will substitute for the APPs so that if an action is inconsistent with the privacy safeguards, it will not be "required or authorised by law" by virtue of the APPs

1.170 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 all business participants in the CDR.

1.171 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.

1.172 The CDR privacy safeguards only apply to information that relates to identifiable or reasonably identifiable individual 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.

1.173 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.

1.174 The Bill clarifies the type 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.

1.175 The Bill provides coverage for CDR consumers irrespective of whether they are an individual or a business consumer through its application to data for which there are one or more CDR consumers.
[Schedule 1, item 1, section 56EB]

1.176 As the consumer data rules are able to clarify and extend the concepts covered in the privacy safeguards, the privacy safeguards act as a minimum requirement for matters the rules must address. However, should the consumer data rules be inconsistent with the privacy safeguards, the privacy safeguards prevail. ***[Schedule 1, item 1, section 56EC]***

Data holders – application of the privacy safeguards and the APPs

1.177 A data holder's collection, use, storage and disclosure of information protected by the Privacy Act will generally be subject to the operation of the APPs when the information relates to the data holder's own sector.

Example 1.14

George is a consumer with AnnaBank. All of her transaction information held by AnnaBank is treated consistently with the Privacy Act and APPs by AnnaBank.

George has a transaction (savings) account with AnnaBank but has been told by friends she can probably get a better interest rate elsewhere. Keen to make the most of the CDR, George has requested AnnaBank to transfer her CDR data relating to the transaction account to Meeks Banking Services.

At the time of receiving George's CDR data, Meeks Banking Services is required to handle the data in accordance with the CDR privacy safeguards.

George discovers that Meeks Banking Services will provide her a better interest rate on her transaction account. George closes her transaction account with AnnaBank and opens an account with Meeks Banking Services.

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

Consumer data rules enable Meeks Banking Services to also treat George's historical data as a data holder, and subject to the APPs.

Example 1.15

George subsequently hears of a service offered by Meeks Banking Services which is designed to enhance George's savings capacity. Meeks Banking Services is an accredited data recipient for the energy sector CDR designation and it offers to compare customers' energy bills and advise customers if savings could be made by switching providers.

George consents to the transfer of her energy bills from GasCo and PowerProvider to Meeks Banking Services. Meeks Banking Services must handle George's energy sector information in accordance with the privacy safeguards, as it is an accredited data recipient of this CDR data.

1.178 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 that CDR data will be subject to the privacy safeguards and the consumer data rules.

Consideration of CDR data privacy

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

1.179 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.

1.180 To assist in this, all CDR participants must have a policy about the management of CDR data. That policy must contain the following information:

- The kinds of CDR data collected by the CDR participant, how that data is collected as an accredited data recipient;
- The kinds of CDR data held by the CDR participant 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 privacy principles, the consumer data rules or the Data standards;
- How a CDR participant will address such a complaint; and
- Where a CDR participant is likely to disclose CDR data to an overseas accredited data entity, information about the country in which that entity is based.

[Schedule 1, item 1, section 56ED]

1.181 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.

1.182 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)]***

1.183 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

1.184 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)]***

1.185 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.

1.186 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.

1.187 Unless the consumer data rules specify instances where a CDR participant 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)]***

Collecting CDR data

CDR Privacy Safeguard 3 – Collecting solicited CDR data

1.188 A person must only collect CDR data consistently with Part IVD of the CC Act. A person will only be authorised to collect CDR data if:

- the person is an accredited entity under the CDR regime and they collect the data because of a disclosure that is required under the consumer data rules in response to a valid request from a CDR consumer for the data; or
- the collection is required or authorised by an Australian law, other than the APPs.

[Schedule 1, item 1, section 56EF]

1.189 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, except for the APPs. In that case, a person will be authorised to make the collection of the CDR data by that law. ***[Schedule 1, item 1, subsection 56EF(b)]***

1.190 If the person holds the CDR data as the consumer or a non-accredited entity, it will be subject to the Privacy Act and APPs rather than the CDR privacy safeguards.

Example 1.16

Naomi currently banks with BankOz but she has accepted a position with a company that will see her moving to New York at the end of the year. Naomi feels that the role will be ideal for her and is interested in purchasing a property in Manhattan as her New York base but she has no history with BankUSA who she wishes to transfer all of her savings and credit accounts to once she relocates to New York.

Naomi asks BankOz to transfer all of her personal information to BankUSA under APP 12, because BankUSA is not an accredited data recipient under the CDR.

BankOz must comply with APP 8 in relation to the cross border disclosure of Naomi's personal information as it is not covered by the privacy safeguards, due to BankUSA not being an accredited data recipient.

The transfer is of Naomi's personal information, rather than CDR data (even though it may be the same information), because it occurs under the Privacy Act.

CDR Privacy Safeguard 4 – Dealing with unsolicited CDR data

1.191 This privacy safeguard is included to cover scenarios where a person may not have solicited CDR data, but they find themselves in possession of it.

1.192 In such circumstances, the person is required to destroy the CDR data unless an Australian law (other than the Privacy Act or the APPs) requires that the recipient retain that data. ***[Schedule 1, item 1, section 56EG]***

1.193 This section makes it very clear than a 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

1.194 If a person collects data in accordance with privacy safeguard 3, then that 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 when collection occurs 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]***

1.195 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

Disclosure by a data holder

1.196 A data holder will be authorised to make disclosures under the CDR at any point in time provided that the CDR consumer has given their consent consistent with the consumer data rules. ***[Schedule 1, item 1, paragraph 56EI(1)(a)]***

1.197 Disclosures through the CDR by a data holder may also be permitted where they are required or authorised by an Australian law or an order of a court or tribunal.

1.198 It is not the intention that the CDR privacy safeguards restrict the ability of data holders to disclose CDR data outside of the CDR system where the disclosure is required or authorised under law, including under the Privacy Act. ***[Schedule 1, item 1, paragraph 56EI(b)]***

Use or disclosure by an accredited data recipient

1.199 An accredited data recipient may use or disclose CDR data if that use or disclosure relates to a purpose authorised by the consumer data rules. ***[Schedule 1, item 1, paragraph 56EI(2)(a)]***

1.200 CDR data collected under privacy safeguard 3 may be disclosed by an accredited recipient with the CDR consumer's consent. 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.

1.201 A use will be authorised where it is required or permitted by an Australian law or an order or a court or tribunal, except for the Privacy Act and the APPs. ***[Schedule 1, item 1, paragraph 56EI(2)(b)]***

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

1.202 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. ***[Schedule 1, item 1, section 56EJ]***

1.203 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 and small business personal information.

1.204 Contravention of this privacy safeguard may attract a civil penalty. This reflects the importance placed on consumer consent to the use and disclosure of their CDR data. Unless authorised by the consumer data rules, or specifically consented to by the CDR consumer, direct marketing is not permitted.

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

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

1.206 Section 56EK applies to disclosures of CDR data to offshore entities so that disclosure, in accordance with privacy safeguard 6, is permitted if the entity is an accredited data recipient. ***[Schedule 1, item 1, section 56EK]***

1.207 This acknowledges the requirements that will be placed on accredited entities and their willingness to participate in the CDR system. Accreditation is considered sufficient protection to ensure that the accredited entities will not breach the privacy safeguards.

1.208 The consumer data rules may also provide that a disclosure cross-border disclosure is authorised for CDR data. ***[Schedule 1, item 1, subsection 56EK(d)]***

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

1.209 As the CDR system develops, it is possible that CDR consumers may have CDR data sets that contain government identifiers, as defined in the Privacy Act. These can include things like a tax file number or a person's MyGov account log in information.

1.210 In order to protect government identifiers, they are not permitted to be used by an accredited data recipient or data holder as an identifier of a CDR consumer. ***[Schedule 1, item 1, subsection 56EL(2)]***

1.211 Similarly, it is not permissible for a data holder or an accredited data recipient to disclose CDR data containing a government identifier. The only exception to this is if the disclosure permitted is by the consumer data rules or is otherwise required or authorised under Australian law (except the APPs or Privacy Act) or by an order of a court of tribunal other than the APPs. ***[Schedule 1, item 1, subsection 56EL(3)]***

Integrity of CDR data

CDR Privacy Safeguard 10 – Quality of CDR data

1.212 It is important that the data in the CDR system be accurate, up to date and complete. As such, CDR participants must ensure the quality of CDR data they hold consistently with the consumer data standards. ***[Schedule 1, item 1, section 56EM]***

1.213 If the CDR participant is a data holder, the data holder must manage any of their data (including CDR data) that is protected by the Privacy Act in accordance with that Act and the APPs (see APP 10).

1.214 Privacy safeguard 10 requires that, prior to disclosing CDR data in relation to a CDR consumer, the CDR participant ensures that the CDR data is accurate, up to date and complete. Privacy safeguard 10 applies to all CDR participants, both data holders and accredited data recipients to ensure the quality of CDR data, including data that relates to business consumers. ***[Schedule 1, item 1, section 56EM]***

1.215 In the event that a disclosure of inaccurate CDR data is made by a CDR participant, subsection 56EM(2) places a requirement on the CDR participant to advise the CDR consumer about the disclosure of inaccurate information relating to them. ***[Schedule 1, item 1, subsection 56EM(2)]***

1.216 An affected CDR consumer is provided with the ability to require the CDR participant to disclose corrected CDR data to the recipient of the earlier disclosure and a CDR participant must comply with that request. ***[Schedule 1, item 1, subsection 56EM(3)]***

Example 1.17

Levi has sought disclosure of his mobile phone information to a fintech, TeleMarketDeals for the purpose of comparing whether a better rate for his international calls is available. TeleMarketDeals undertakes some analysis of Levi's calling patterns, in particular his overseas calls, and recommends CheepCalls.

TeleMarketDeals is then authorised, pursuant to Levi's request, to on-disclose Levi's information to CheepCalls who have offered the best rates for Levi to call his family in Peru.

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.

1.217 The importance of CDR data being accurate is emphasised by the application of a civil penalty for breach of privacy safeguard 10.

CDR Privacy Safeguard 11 – Security of CDR data

1.218 An integral element of the CDR system is the protection of consumers' CDR data. As such, privacy safeguard 11 places a requirement on collectors of CDR data (pursuant to privacy safeguard 3), 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)]***

1.219 In addition, if a person has collected the CDR data pursuant to privacy safeguard 3 or has data that is derived from the primary data, and the person is no longer using the data as permitted by the consumer data rules, then the redundant data must be destroyed or de-identified according to the consumer data rules applying to the relevant type of data. ***[Schedule 1, item 1, subsection 56EN(2)]***

1.220 Exceptions to this apply if the person is under an obligation at law, aside from the APPs, or pursuant to an order of a court or tribunal to retain the CDR data. ***[Schedule 1, item 1, subsection 56EN(2)]***

1.221 A civil penalty may apply for a breach of subsection 56EN(1).

Example 1.18

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 his credit account 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 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 1.19

Following on from example 1.18 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 since they received the CDR data from ZAP.

Bucks Banking complies with the ACCC's direction to destroy all CDR data that it is no longer using. Had it failed to do so, the ACCC could have sought the application of a civil penalty.

1.222 As noted in example 1.19 above, a civil penalty may also be applied to a failure to comply with this requirement to de-identify or destroy CDR data that is no longer being used by the accredited data recipient.

Correction of CDR data

CDR Privacy Safeguard 12 – Correction of CDR data

1.223 The requirement to correct CDR data applies to both data holders and accredited data recipients. This is in addition to APP 10 as it applies to data holders to ensure the quality of personal information they hold. ***[Schedule 1, item 1, section 56EO(1)]***

1.224 The consumer data rules may apply additional requirements in circumstances where CDR data is inaccurate and requires correction. These requirements can include correction of the inaccuracies as well as the inclusion of a statement with the CDR data. ***[Schedule 1, item 1, paragraph 56EO(2)(a)]***

1.225 Further, the consumer data rules may require that a notice is provided outlining the correction or outlining details of why a correction was considered to be unnecessary as appropriate in the circumstances. ***[Schedule 1, item 1, paragraph 56EO(2)(b)]***

1.226 The consumer data rules about correction of CDR data must be complied with or a civil penalty may be applied. ***[Schedule 1, item 1, subsection 56EO(1)]***

Compliance with the Privacy Safeguards

Guidance and education programs

1.227 Part IVD provides that the Information Commissioner shall promote compliance with the privacy safeguards. In order for the Information Commissioner to undertake this role, as noted above, the AIC Act is amended to extend the Commissioner's functions to include those under Part IVD.

1.228 The Information Commissioner is empowered to make guidelines about the privacy safeguards for the purpose of outlining when a breach may occur and the sorts of acts or practices that could result in breach of the privacy safeguards. ***[Schedule 1, item 1, paragraph 56EP(1)(a)]***

1.229 Acknowledging the shared regulation of the CDR regime, prior to making a guideline under paragraph 56EP(1)(a), the Information

Commissioner must consult with the ACCC about the proposed guidelines. ***[Schedule 1, item 1, subsection 56EP(2)]***

1.230 To the extent of any inconsistencies that may arise between the privacy safeguard guidelines made under section 56EP and the consumer data rules, the consumer data rules will take precedence. However, given the requirement to consult the ACCC prior to making privacy safeguard guidelines, the likelihood of any inconsistency is low. ***[Schedule 1, item 1, subsection 56EP(4)]***

1.231 Guidelines made by the Information Commissioner will be publicly available and the Information Commissioner is provided with the discretion to publish these documents as he or she considers appropriate. ***[Schedule 1, item 1, subsection 56EP(3)]***

1.232 The Information Commissioner's guidelines are not legally enforceable and, as such, are not legislative instruments within the meaning of subsection 8(1) of the *Legislation Act 2003*. ***[Schedule 1, item 1, subsection 56EP(5)]***

1.233 The Information Commissioner may also conduct educational programs in order to assist participants in CDR to understand their rights and responsibilities under the CDR regime. ***[Schedule 1, item 1, paragraph 56EP(1)(c)]***

Assessments of management and handling of CDR data

1.234 Under the Privacy Act, the Information Commissioner is provided with the ability to conduct an assessment relating to compliance with the APPs and to provide a report of the Commissioner's investigation to an act or practice to the Minister; in that case the Attorney-General (see sections 30 and 33C of the Privacy Act).

1.235 For the purpose of making an assessment of a CDR participant's compliance with the privacy safeguards, the Information Commissioner is provided with the power to conduct such an assessment in a manner he or she considers appropriate. ***[Schedule 1, item1, subsections 56EQ(1) and (2)]***

1.236 Once the Information Commissioner has conducted his or her assessment, a report is able to be provided to the Minister (in this case the Minister with portfolio responsibility for the CC Act – the Treasurer), the ACCC or the Data Standards Chair. ***[Schedule 1, item 1, subsection 56EQ(3)]***

Notifications of CDR data security breaches

1.237 The Privacy Act contains a regime for the management of personal information. This includes requirements to notify if an eligible data breach (within the meaning of that Act) has occurred under Part IIIC of the Privacy Act.

1.238 Part IVD contains provisions to apply Part IIIC of the Privacy Act to accredited data recipients and their conduct for CDR data. As such,

accredited data recipients are required to notify the Information Commissioner about CDR data security breaches. ***[Schedule 1, item 1, section 56ER]***

1.239 In addition, Part V of the Privacy Act is extended to apply to a CDR consumer's CDR data creating the power for the Information Commissioner to handle complaints and undertake investigations under the Privacy Act regarding the management and handling of CDR consumers' CDR data. ***[Schedule 1, item 1, subsection 56ER(2)]***

Enforceable civil penalty provisions, undertakings and injunctions

Civil penalties

1.240 To ensure compliance with Division 5 and the privacy safeguards, those provisions which are civil penalty provisions are enforceable under the *Regulatory Powers (Standard Provisions) Act 2014* (the Regulatory Powers Act). ***[Schedule 1, item 1, section 56ET]***

1.241 The Information Commissioner is an authorised applicant and will be able to seek the application of a civil penalty for contravention of the privacy safeguards in Division 5. ***[Schedule 1, item 1, subsection 56ET(2)]***

1.242 For the purposes of Part 4 of the Regulatory Powers Act, applications may be made to the Federal Court, the Federal Circuit Court or the court of a State or Territory with jurisdiction in relation to the matter. ***[Schedule 1, item 1, subsection 56ET(3)]***

1.243 In the event that the actions of a CDR participant contravene both a consumer data rule which contains a civil penalty for breach as well as a privacy safeguards provision also containing a civil penalty, a person can only be liable for one pecuniary penalty under Part 4 of the Regulatory Powers Act and Part IV of the CC Act for the same conduct. ***[Schedule 1, item 1, subsection 56ET(5)]***

1.244 It is not the intention that CDR participants be penalised twice for the same behaviour. While this is unlikely to materialise in practice, subsection 56ET(5) clarifies that penalties can only be applied once in relation to conduct resulting in a breach.

Enforceable undertakings

1.245 Part 6 of the Regulatory Powers Act is enlivened so that each provision of Subdivision B to F of Division 5 is able to be enforced via accepting and enforcing undertakings to comply with those provisions. Relevantly, this includes compliance with the requirements to:

- Manage CDR data in an open and transparent way (privacy safeguard 1, section 56ED);
- Enable anonymity and the use of pseudonyms consistently with the consumer data rules (privacy safeguard 2, section 56EE);

- Appropriate collection of CDR data (privacy safeguard 3, section 56EF);
- How to deal with unsolicited CDR data (privacy safeguard 4, section 56EG);
- Notifying about the collection of CDR data (privacy safeguard 5, section 56EH);
- Requirements respecting the use or disclosure of CDR data (privacy safeguard 6, section 56EI);
- Use of CDR data for the purpose of direct marketing (privacy safeguard 7, section 56EJ);
- Rules about cross-border disclosures of CDR data (privacy safeguard 8, section 56EK);
- Adoption or disclosure of government identifiers (privacy safeguard 9, section 56EL);
- The integrity of CDR data (privacy safeguard 10, section 56EM);
- The security of CDR data (privacy safeguard 11, section 56EN); and
- The correction of erroneous CDR data (privacy safeguard 12, section 56EO).

[Schedule 1, item 1, subsection 56EU(1)]

1.246 Under Part 6 of the Regulatory Powers Act, the Information Commissioner is able to seek an undertaking to enforce compliance with these provisions of the CDR regime relating to the use, collection, disclosure and storage of CDR data. ***[Schedule 1, item 1, subsection 56EU(2)]***

1.247 The Information Commissioner may apply for such undertakings in the Federal Court, the Federal Circuit Court or a court of a state or territory with jurisdiction to hear the matter. ***[Schedule 1, item 1, subsection 56EU(3)]***

Injunctions

1.248 The Information Commissioner is provided with similar powers for the enforcement of the provisions of Subdivision B to F of Division 5 about privacy safeguards via injunctions as discussed above at paragraphs 1.245 to 1.247 relating to enforceable undertakings.

1.249 Part 7 of the Regulatory Powers Act provides the standard provisions on injunctions to ensure compliance with statutory provisions. The Information Commissioner may seek compliance with a relevant provision via an application for injunctions to be applied. ***[Schedule 1, item 1, section 56EV]***

1.250 Consistently with the enforcement powers provided to the Information Commissioner to ensure compliance with the CDR regime (Division 5 of Part IVD), through enforceable undertakings and civil penalties, the power to seek injunctions under the Regulatory Powers Act is granted in preference to the power to seek an injunction under section 80 of the CC Act.

1.251 This ensures consistency with the Information Commissioner's specific powers to enforce compliance with the privacy safeguards.

Delegation to the Commission

1.252 Acknowledging the dual regulatory model provided for the CDR, section 56EW is inserted to enable the Information Commissioner to delegate his or her privacy safeguard enforcement powers or functions to the Commissioner or a member of staff of the ACCC (as referred to in section 27 of the CC Act). ***[Schedule 1, item 1, section 56EW]***

1.253 Such a delegation may be made in order to manage a joint investigation into the breach of the privacy safeguards where it is suspected that the breach by the CDR participant is part of a systemic pattern of conduct. In such circumstances, the Information Commissioner may consider it appropriate to conduct a joint investigation into the matter.

1.254 These delegations may only occur with the express written agreement of the Commission to the delegation. ***[Schedule 1, item 1, subsection 56EW(3)]***

Other matters

Incorporation of instruments by reference

1.255 Given the CDR may be applied to a broad range of industries, which could have industry codes or State or Territory laws applying to them, it is important that the consumer data rules, the regulations and the designations be able to refer to external instruments that may be in force from time to time. ***[Schedule 1, item 1, subsection 56GB]***

1.256 While this will displace subsection 14(2) of the *Legislation Act 2003*, it is important to have the flexibility to refer to or incorporate instruments or standards that may exist from time to time. For example, it may be that a consumer data rule will seek to refer to a particular International Organisation for Standardisation (ISO) information security standards as part of the criteria to obtain accreditation.

Protection from liability

1.257 The CDR applies to data that is captured within designated sectors and data sets. As such, it is primarily about the provision of

information by persons within the CDR system and consistently with the consumer data rules, the privacy framework and the Privacy Act.

1.258 Therefore, if a person provides information to another person or allows that person to access information, in good faith and complying with a CDR system requirement, the person providing the information is protected from liability. That is, a person so protected from liability will not be able to have an action taken against them, whether civil or criminal; for or in relation to the provision of the relevant CDR information. ***[Schedule 1, item 1, section 56GC]***

1.259 This protection understands that the CDR system is driven by the provision of data. Provided that data is transferred consistently with all elements of the CDR regime, then a person should be protected from liability where they have complied with a CDR obligation.

Exemptions and modifications by the ACCC and by regulations

1.260 The ACCC is provided with a broad power to exempt persons from the provisions of Part IVD or any regulations made for the purposes of that Part or the provisions of the consumer data rules. ***[Schedule 1, item 1, subsection 56GD(1)]***

1.261 It is possible for the ACCC to exempt a person or a class of persons or a data set or class of data from all of the specified provisions of the CDR regime. ***[Schedule 1, item 1, subsections 56GD(2) and56GD(3]***

1.262 The ACCC exemption may also apply unconditionally or subject to conditions. ***[Schedule 1, item 1, subsection 56GD(4)]***

1.263 Each of these powers provides the ACCC with the ability to ensure that the CDR system does not operate in an unintended or perverse way in exceptional circumstances. They provide the ACCC with scope to ensure that the CDR system works in the best way possible for consumers and designated industry.

1.264 Exemptions, on the basis described above in paragraphs 1.260 to 1.263, may also be made by regulations. ***[Schedule 1, item 1, subsection 56GE]***

1.265 The regulations will only seek to declare that provisions of the CDR (Part IVD) are modified or varied in exceptional circumstances. However, it is important to include the ability to modify the CDR regime via regulation in order to ensure that the system is dynamic and able to adapt quickly to a changing economy and the varied sectors within it. Regulations are, of course, disallowable instruments and the Parliament will have appropriate oversight over any regulation made under the CDR regime.

Alternative Constitutional basis and compensation for acquisition of property

1.266 The Commonwealth has been provided with specific legislative powers under the Constitution. In so far as the application of this Part might extend beyond those powers, section 56GF makes clear that the Part extends to those subjects which are consistent with the Constitutional law making powers of the Commonwealth. ***[Schedule 1, item 1, section 56GF]***

1.267 Having noted this, it is very likely that most data holders will, in the initial CDR years, be constitutional corporations. While accredited data recipients are also likely to be constitutional corporations, the possibility of an accredited data recipient not being a constitutional corporation is higher.

1.268 Additionally, the Commonwealth has Constitutional power with respect to some potential CDR sectors – including banking and telecommunications. This enables it to legislate all aspects of the regime as it applies in those sectors.

1.269 It is considered that the operation of this Part will not ordinarily result in an acquisition of property, but if that were to arise, section 56GG has been included in order to ensure that any acquisition of property within the meaning of section 51(xxxi) of the *Constitution* is actionable. ***[Schedule 1, item 1, section 56GG]***

1.270 The Commonwealth will not be liable for the acquisition of property by any entity other than the Commonwealth. Section 56GG provides that the person who has acquired relevant property will be liable to pay a reasonable amount of compensation to the person the property was acquired from. This provision operates with the ACCC's power to make rules setting a fee for access to CDR data, including where this may amount to an acquisition of property. ***[Schedule 1, item 1, subsection 56GG(2)]***

1.271 In the event that the two persons do not agree to the amount of reasonable compensation payable, they may commence proceedings in a court of competent jurisdiction. ***[Schedule 1, item 1, subsection 56GG(3)]***

Other matters

1.272 A range of consequential amendments are made to the CC Act as a result of the introduction of the CDR. These include the addition of new definitions at subsection 4(1). ***[Schedule 1, item 6, subsection 4(1)]***

Consequential amendments

1.273 Subsection 6E(1D) is inserted to the Privacy Act in order that small business operators who hold an accreditation under the CDR regime are treated as an organisation for the purposes of the Privacy Act in

respect of information that is not CDR data. ***[Schedule 1, item 52, subsection 6E(1D) of the Privacy Act 1988]***

1.274 This amendment means that individuals are assured that there will be no circumstances in which their personal information held by small business accredited data recipients is not protected by either the CDR privacy safeguards or the Privacy Act.

Review of the operation of this Part

1.275 Section 56GH requires that this Part be reviewed by an independent reviewer with a report provided to the Minister on or before 1 January 2023. ***[Schedule 1, item 1, subsections 56GH(1) and 56GH(2)]***

1.276 The Minister must then table copies of the report in each House of Parliament within 15 sitting days after the report is provided to the Minister. ***[Schedule 1, item 1, subsection 56GH(3)]***

1.277 Providing that this Part be reviewed acknowledges the novel nature of the CDR regime. As such, the review will provide designated sectors, consumers and interested parties with an opportunity to reflect on risks, issues and opportunities presented by the CDR as well as make recommendations for the improvement of the system.

Application and transitional provisions

1.278 This Bill applies from Royal Assent.

1.279 As noted above at paragraph 1.37, for the purposes of designation of the banking sector, subsections 56AD(2) and (3) of this Part do not apply. ***[Schedule 1, item 2]***

1.280 This is because the Open Banking Review undertook consultation with the banking sector and the community on the scope and application of the CDR to the banking sector. The Minister subsequently consulted on the recommendations of the Open Banking Report. Requiring the ACCC to undertake consultation and provide the Minister with a report following the extensive consultation undertaken in preparing the Open Banking Report is not considered to be necessary.

1.281 The application of Part IVD to the banking sector commences following the Minister's designation of that sector via instrument pursuant to subsection 56AC(2). Part IVD will apply to information within that sector covered by the definition of CDR data for the banking sector defined by the instrument of designation and the consumer data rules. Relevant information from 1 January 2017 will be captured. ***[Schedule 1, item 2]***