2016-2017-2018

THE PARLIAMENT OF THE COMMONWEALTH OF AUSTRALIA

HOUSE OF REPRESENTATIVES

TREASURY LAWS AMENDMENT (CONSUMER DATA RIGHT) BILL 2018

EXPLANATORY MEMORANDUM

(Circulated by authority of the
Hon Josh Frydenberg MP)

Table of contents

Glossary

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

Abbreviation	*Definition*
ACCC	Australian Competition and Consumer Commission
AIC Act	*Australian Information Commissioner Act 2010*
APPs	Australian Privacy Principles
Bill	Treasury Laws Amendment (Consumer Data Right) Bill 2018
CC Act	*Competition and Consumer Act 2010*
CDR	Consumer Data Right
Criminal Code	The Schedule to the *Criminal Code Act 1995*
Information Commissioner	Australian Information Commissioner
OAIC	Office of the Australian Information Commissioner

General outline and financial impact

Consumer Data Right

The Consumer Data Right (CDR) provides individuals and businesses with a right to efficiently and conveniently access specified data in relation to them held by businesses. The CDR authorises secure access to this data by trusted and accredited third parties. The CDR requires 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.

Date of effect: 1 July 2019

Proposal announced: This Bill fully implements the *National Consumer Data Right* measure from the 2018-19 Budget.

Financial impact: $45 million from 2018-19 to 2021-22.

Human rights implications: This Bill is compatible with human rights, and to the extent that it may limit human rights, those limitations are reasonable, necessary and proportionate. See *Statement of Compatibility with Human Rights* — Chapter 2, paragraphs 2.5 to 2.32.

Compliance cost impact: The measure will increase compliance costs in the banking sector and for accredited parties by an average of $86.6 million per year, and in the energy sector by an average of $9.9 million per year, on an annualised basis (with common accreditation costs not duplicated in the latter figure). The regulatory impact for other sectors, including the telecommunications sector, will be considered on a sector by sector basis both when designating those sectors and when writing rules for those sectors.

Summary of regulation impact statement

Regulation impact on business

The Government considered the regulatory impacts of the CDR through the *Competition Policy Review 2015* (the Harper Review), the Productivity Commission *Inquiry Report into Data Availability and Use* (the PC Data Report), Innovation and Science Australia's 2017 Report: *Australia 2030: Prosperity through Innovation Review* (the ISA Report), and the Government's *Review into Open Banking in Australia 2017* (the Open Banking Report).

On 9 August 2017, consultation on a model for open banking began and took place for six weeks. 41 submissions were received from entities such as banks, FinTech businesses, industry bodies, consumer advocates and private individuals.

A further 74 submissions (seven confidential) were received over six weeks of public consultation in early 2018 ahead of the Government's response to the Review.

The Bill was released for public consultation twice. Consultation occurred from 15 August 2018 to 7 September2018 and then from 24 September 2018 to 12 October 2018. 65 submissions (two confidential) were received and 25 submissions were received respectively.

Extensive bilateral meetings and roundtables were conducted.

Chapter 1
Consumer Data Right

Outline of chapter

1.1 The CDR provides individuals and businesses with a right to efficiently and conveniently access information held by businesses about the transactions they enter into as consumers 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 consumers 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.

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

1.3 The primary aim of the CDR is to give consumers the ability to access and use more information about themselves, and about their use of goods and services, in a manner that allows them to make more informed decisions about both themselves and the good and services they use. By doing so, the CDR aims to increase competition, enable consumers to fairly harvest the value of their data, and enhance consumer welfare.

1.4 The CDR will reduce the barriers that currently prevent potential customers from shifting between service providers. By 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.

1.5 The CDR places the value of consumer 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 created. 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.

1.6 Strong privacy and information security provisions are a fundamental element of the CDR. These protections include privacy safeguards. The OAIC will advise on and enforce these privacy protections. Consumers will have a range of avenues to seek remedies for

breaches of their privacy including access to internal and external dispute resolution.

1.7 The ACCC has responsibility for advising the Minister on matters such as competition and making the consumer data rules.

Context of amendments

1.8 On 26 November 2017, the Government announced, as a partial response to the PC Data Report, the introduction of a CDR with application initially in the banking, energy and telecommunications sectors. On 1 May 2018, as part of its full response to the PC Data Report, The Government confirmed its commitment to the CDR and announced the creation of a new National Data Commissioner.

1.9 The Government announced that the 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 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. Key features of the right are that access must be provided in a timely manner and in a useful digital format.

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

1.11 The CDR implements recommendations from a wide range of reviews. Notably, 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 PC Data Report, and the ISA Report.

1.12 A number of reviews have recommended data portability rights in specific sectors including the *Financial System Inquiry 2015*, the *Northern Australia Insurance Premiums Taskforce Final Report 2016*, the *Review of the Four Major Banks 2016*, the *Independent Review into the Future Security of the National Electricity Market – Blueprint for the Future 2017*, the Productivity Commission's report on *Competition in the Australian Financial System 2018*, Council of Australian Governments' 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.*

1.13 The CDR provides a mechanism for accessing a broader range of information within designated sectors than is provided for by APP 12 in the *Privacy Act 1988*. 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.

1.14 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 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 lead on matters relating to the protection of individual and small business consumer participants' privacy and confidentiality, and compliance with the CDR Privacy Safeguards (Privacy Safeguards).

1.15 A data standards body will also be established to assist a Data Standards Chair in making data standards. These data standards will explain the format and process by which data needs to be provided to consumers and accredited data recipients within the CDR system. Initially, this function will be undertaken by Data61 of the Commonwealth Scientific and Industrial Research Organisation (CSIRO).

Summary of new law

1.16 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.

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

1.18 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 data recipients including other banks, telecommunications providers, energy companies or companies providing comparison services. CDR also allows consumers to access their own data without directing that the data be provided to a

third party. The CDR system may also see the emergence of new data driven service providers.

1.19 The ACCC is provided with the power to make rules, in consultation with the Information Commissioner to determine how CDR functions in each sector.

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

1.21 For some sectors, the Minister may designate a gateway to facilitate the transfer of information from a data holder to an accredited person or the consumer themselves.

1.22 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 1988.*

1.23 The data must be provided in a format which complies with the data 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.

1.24 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 the Australian Financial Complaints Authority.

1.25 The CDR provides the Information Commissioner with the function of enforcing the Privacy Safeguards and providing individual remedies to individuals and small business. The ACCC is responsible for enforcing the balance of the regime and for taking strategic enforcement actions.

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

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. By 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 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 the consumer data rules made by the ACCC.	The *Privacy Act 1988* 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 outline how APP entities must handle personal information. APP 12 establishes a principle to deal with requests for access to personal information.
The ACCC is able 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, the Data Standards Body and the format of CDR data and the data standards.	No equivalent.
The CDR includes privacy safeguards to protect CDR data relating to an identifiable CDR consumer. This includes protection of information not covered by the APPs. The privacy safeguards provide minimum protections for the treatment of CDR data. They can be supplemented by the consumer data	The APPs apply to the the handling of personal information (including its collection, use, disclosure and storage), as defined in the *Privacy Act 1988*.

New law	***Current law***
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 authorise the disclosure of CDR data where this disclosure is prohibited under the CDR regime. The APPs will be switched off and substituted by the CDR Privacy Safeguards for accredited data recipients of CDR data. In most circumstances, the APPs continue to apply to CDR data held by data holders and designated gateways.	
Under the CDR, all businesses will be able to access information covered by designated data sets about themselves.	The *Privacy Act 1988* does not protect or facilitate access to businesses' information about themselves.
A designated gateway may be designated by the Minister to facilitate the transfer of information between an accredited data recipient and the data holder.	No equivalent.
The *Privacy Act 1988* will protect 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.	With some exceptions, the *Privacy Act 1988* does not bind small businesses.
The Information Commissioner's functions include those conferred on him or her under the CDR regime. The Information Commissioner (and the OAIC) will work with the ACCC in administering the CDR regime.	The Information Commissioner undertakes his or her functions as established by the *Privacy Act 1988* and other legislation which confers a power or function on the Information Commissioner.

Detailed explanation of new law

1.27 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. ***[Schedule 1, item 1, sections 56AA and 56AB]***

1.28 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.

1.29 The Bill establishes a framework to enable the CDR to be applied to various sectors of the economy over time. The framework relies on four key participants – consumers, data holders, accredited persons and accredited data recipients, and designated gateways. However, the system is flexible and may also provide via the consumer data rules, for interactions between consumers and non-accredited entities.

1.30 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 oversees the CDR from a consumer and competition perspective with particular focus on systemic enforcement. The ACCC is also responsible for establishing the consumer data rules, in consultation with the OAIC. Each of the elements of the CDR system is explained below.

1.31 The CDR will be applied across different sectors of the economy which are already subject to various regulatory regimes. As a result, the CDR framework balances the need to provide clear direction to the ACCC on the types of consumer data rules that can be made with the flexibility to create rules that are tailored to different sectors of the economy that may be designated over time.

1.32 The CDR provisions bind the Crown, although other than the enforceable undertakings which may be made for the Privacy Safeguards and other breaches of the CDR, enforcements and remedies do not apply to the Crown. ***[Schedule 1, item 1, section 56AQ]***

Designated sectors

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

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

1.35 The CDR is intended to eventually apply across the economy. The designation process is therefore a process to aid in the prioritisation of sectors, and to identify data sets where the potential benefits for consumers to access and transfer their information exceed the potential costs.

1.36 The Minister designates a sector by specifying:

- classes of information and those classes for which a fee can be charged (CDR data is explained at paragraphs 1.113 to 1.121 and the fee arrangements are explained at paragraphs 1.132 to 1.148); and
- persons who hold one or more of those classes of information (Data holders are explained at paragraphs 1.77 to 1.88).

[Schedule 1, item 1, paragraphs 56AC(2)(a), 56AC(2)(b) and 56AC(2)(d)]

1.37 If the sector is to have a gateway the Minister will designate this person in the instrument. A gateway is a person whose role it is to facilitate the transfer of data between certain participants in the CDR regime. Designated gateways are explained in more detail at paragraphs 1.95 to 1.99. ***[Schedule 1, item 1, paragraph 56AC(2)(e)]***

1.38 The designation instrument will also set out the earliest day that the CDR will apply. That is, certain information may be subject to the CDR even though it was generated and collected prior to the commencement of the CDR. However, the Bill places a limit on this period. The instrument cannot specify a day earlier than 1 January two years before the instrument is made. ***[Schedule 1, item 1, paragraph 56AC(2)(c) and subsection 56AC(4)]***

1.39 The Bill includes an example to clarify the earliest day the CDR can apply. For an instrument made on 1 July 2019, the earliest day that the instrument can apply to information and persons is 1 January 2017.

1.40 The Bill places a number of obligations on the Minister, the ACCC and the Information Commissioner about factors that must be considered prior to the designation instrument being made (see paragraphs 1.43 to 1.71). The Bill also requires that the ACCC undertake consultation, including public consultation and consultation with the primary regulator of the sector proposed to be designated. However, in the banking sector and energy sector these obligations do not apply because this consultation has already taken place. ***[Schedule 1, items 2 and 3]***

1.41 The Government has indicated that 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 of public consultation on that report was also undertaken by the

Minister from 9 February 2018. A further three weeks of consultation on the draft designation instrument was undertaken by the Minister from 24 September 2018.

1.42 The Government has also indicated that the energy sector will be designated as the second sector of the economy to which the CDR applies. Public consultation was undertaken as part of the process of preparing the Council of Australian Governments' report *Facilitating Access to Consumer Energy Data*. The first round of consultation involved both public and targeted stakeholder consultations that were held in November and December 2017. The second round of consultation on this paper sought public submissions from 1 March 2018 for four weeks. The third round of consultation involved targeted stakeholder consultation in June 2018.

Minister's tasks before designating a sector

1.43 The Minister must consider a range of factors prior to making a designation. The ACCC will be responsible for advising the Minister on these matters with the exception of the impact on the privacy and confidentiality of the information, which is the responsibility of the Information Commissioner. ***[Schedule 1, item 1, sections 56AD, 56AE and 56AF]***

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

1.45 Other factors are the effect of the designation on market efficiency, and promoting competition and data-driven innovation. The ways the designation will enhance these matters must be considered prior to the designation of a sector. ***[Schedule 1, item 1, subparagraphs 56AD(1)(a)(ii), 56AD(1)(a)(iv) and 56AD(1)(a)(v)]***

1.46 The Minister must also consider the impact on the intellectual property rights of participants in the CDR of designating a data set and the likely impact of making the instrument on the public interest. ***[Schedule 1, item 1, subparagraphs 56AD(1)(a)(vi) and 56AD(1)(a)(vii)]***

1.47 In considering the public interest, the Minister may consider a range of factors such as whether designation of that data set will promote public health by providing information that enables individuals to better manage their health, or promote other social goals.

1.48 The Minister must also consider the impact the designation will have on the privacy of individuals and confidentiality of business consumers and must consult the Information Commissioner on these matters. ***[Schedule 1, item 1, subparagraph 56AD(1)(a)(iii) and subsection 56AD(3)]***

1.49 The Minister may also consider any other relevant factors. This could include considering whether there are existing processes that are

efficient, convenient and safe, and that allow consumers access to data. ***[Schedule 1, item 1, paragraph 56AD(1)(e)]***

1.50 The CDR is intended to enhance competition and should not create significant regulatory burden or disruption unless the broadly defined benefits of designation outweigh the regulatory impact.

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

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

1.53 The Bill also lists specific factors the Minister must consider before designating data sets for which a fee can be charged, either for the use or disclosure of the information. ***[Schedule 1, item 1, subparagraph 56AD(1)(c)]***

1.54 These factors are:

- whether requiring the data to be disclosed or used would constitute an acquisition of property under Australia's Constitution;
- whether the data holder currently charges consumers for access to that data set;
- whether requiring that data to be disclosed would reduce the incentives to generate, collect, hold or maintain that data set; and
- the marginal cost of disclosing that data.

[Schedule 1, item 1, paragraph 56AD(1)(c)]

1.55 It is anticipated that the majority of designated data sets would be made available for free. Only in rare circumstances, for example, where the marginal cost of disclosure would be significant, would it be appropriate for a data set to be designated as a chargeable data set.

1.56 Before designating a sector, the Minister must consult with the ACCC as well as any other person or body prescribed by regulations. When considering the effect of making the instrument on the privacy or confidentiality of a person's information, the Minister must consult the

Information Commissioner. ***[Schedule 1, item 1, subsections 56AD(2) and 56AD(3)]***

1.57 The Bill sets out the process by which the ACCC and Information Commissioner must consult and then publish their reports from these consultations. Paragraphs 1.60 to 1.71 explain this process.

1.58 After the ACCC has published its report on the consultations on the proposed designation, the Minister must wait at least 60 days before making the designation instrument. ***[Schedule 1, item 1, paragraph 56AD(2)(b)]***

1.59 A designation instrument is not invalid if the Minister or the ACCC fail to consult about the proposed instrument or if the Information Commissioner fails to analyse the likely effect of a proposed instrument on the privacy or confidentiality of consumers' information. ***[Schedule 1, item 1, section 56AH]***

ACCC's role in sector designations

1.60 When the Minister consults the ACCC, the ACCC must consider the factors that the Minister must consider, and consult the public about those factors. ***[Schedule 1, item 1, paragraphs 56AE(1)(a) and 56AE(1)(b)]***

1.61 Public consultation must take place for at least 28 days and must include making information on the proposed designation available on the ACCC's website. ***[Schedule 1, item 1, subparagraphs 56AE(1)(b)(i) and 56AE(1)(b)(ii)]***

1.62 The ACCC must also consult the Information Commissioner, the primary regulator of the sector the instrument would designate (if there is one) and any persons prescribed in the regulations. ***[Schedule 1, item 1, paragraph 56AE(1)(c)]***

1.63 Once consultation has concluded, the ACCC must report to the Minister about its analysis and the consultation, and publish that report on the ACCC's website. ***[Schedule1, item 1, paragraph 56AE(1)(d) and subsection 56AE(2)]***

1.64 Due to the operation of the *Acts Interpretation Act 1901,* the same processes must be followed when an existing instrument is varied or revoked.

1.65 The ACCC may also, on its own initiative, recommend to the Minister that a sector is designated or that an existing instrument, designating a sector, is varied or revoked. The ACCC must publish this recommendation on its website. ***[Schedule 1, item 1, section 56AG]***

1.66 However, before making this recommendation, the ACCC must go through the same consultation processes it would as if it had been consulted by the Minister. That is, it must consult publicly for 28 days, consult the Information Commissioner, primary regulator and other

persons prescribed in regulations and publish its report to the Minister on its website. ***[Schedule 1, item 1, subsection 56AG(2)]***

1.67 The Minister cannot make an instrument in response to the ACCC's recommendation for at least 60 days after the ACCC has published its recommendation. While the Minister will not need to consult the ACCC again, the Minister will need to consult the OAIC before making the instrument. ***[Schedule 1, item 1, subsections 56AG(3) and 56AG(4)]***

Information Commissioner's role in sector designations

1.68 The Minister must also consult the Information Commissioner about the likely effect of designating a sector on the privacy or confidentiality of a person's information. ***[Schedule 1, item 1, sections 56AD(3)]***

1.69 When the Minister consults the OAIC, it must analyse the likely effect of designating a sector on the privacy or confidentiality of a person's information and report to the Minister. ***[Schedule 1, item 1, subsection 56AF(1)]***

1.70 The Information Commissioner must publish this report on its website but may exclude parts of the report where those parts would prejudice Australia's security, defence or international relations or might unreasonably disclose the personal affairs of a person. ***[Schedule 1, item 1, subsections 56AF(2) and 56AF(3)]***

1.71 The circumstances where certain parts of a report can be excluded are linked to existing section 33 of the *Privacy Act 1988* which sets out the circumstances when the Information Commissioner can exclude parts from a report he or she gives under that Act. ***[Schedule 1, item 1, subsection 56AF(3)]***

Participants in the Consumer Data Right system

1.72 There are four key players in the CDR system.

- Data holders, who broadly speaking are the holders of the original data that the right to transfer applies to (see paragraphs 1.77 to 1.88).
- Accredited persons who are 'licensed' to receive the data through the CDR system. Accredited data recipients are accredited persons who have received CDR data and must maintain strict privacy safeguards (see paragraphs 1.89 to 1.94).
- Designated gateways which will be entities designated by the Minister as responsible for facilitating the transfer of information between data holders and accredited persons (see paragraphs 1.95 to 1.99).

- Consumers, who, broadly speaking are the persons or entities that have the right to request that their information is transferred from the data holder to the accredited data recipient (see paragraphs 1.100 to 1.112).

1.73 A person or entity can have multiple roles in the CDR system but will only have one role for particular data. It is the particular CDR data that is being considered which determines which role the person or entity is performing.

1.74 Government entities, such as State or Territory government departments or organisations established by a Commonwealth, State or Territory may be accredited data recipients, data holders or a designated gateway. ***[Schedule 1, item 1, section 56AR]***

1.75 However, a State or Territory entity will only be subject to the CDR where the Minister has declared that the entity is subject to the CDR after the relevant State or Territory has agreed to participate in the CDR. The Minister may also revoke a declaration that an entity is a participating entity. ***[Schedule 1, item 1, sections 56AS and 56AT]***

1.76 A State or Territory entity does not need to agree, and the Minister does not need to make a declaration, in order for such an entity to participate as a consumer and exercise their data right. ***[Schedule 1, item 1, subsections 56AR(3)]***

Data holders

1.77 Data holders are entities or persons that hold the data included in the designation instrument, or data derived from that data. ***[Schedule 1, item 1, subsection 56AJ(1)]***

1.78 Data holders are potentially subject to rules mandating data access at the request of a consumer.

1.79 The day that the person begins to hold the CDR data is important in determining whether the person is a data holder for that data. If the person began holding the data before the earliest date included in the designation instrument, then the person will not be a data holder for that data. ***[Schedule 1, item 1, paragraph 56AJ(1)(b)]***

1.80 Where the entity or person holds the data included in the designation instrument and began to hold this information on or after the date included in the instrument, then the person will be a data holder in the following scenarios.

Case 1: Designated data holders

1.81 Generally speaking, a data holder will be the entity that is specified in the designation instrument that holds the data included in the

designation instrument but not as a result of the data being disclosed to the entity under the consumer data rules. ***[Schedule 1, item 1, subsection 56AJ(2)]***

Example 1.1

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

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

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

EVBank is a data holder for the data it generates and collects that is listed in the designation instrument.

Case 2: Reciprocal data holders

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

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

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

Example 1.2

LendMeMoney is an accredited data recipient. It holds an Australian credit licence and provides credit to its customers. As part of this service it generates and holds lists of the transactions for each consumer.

For the data that it holds about its own customers which reflects the credit services it provides its customers, LendMeMoney would be a data holder and potentially subject to access rights under the consumer data rules.

1.85 The accredited data recipient will continue to be an accredited data recipient for the data it holds that was transferred to it under the consumer data rules. For this data it will need to meet the Privacy Safeguards included in the Bill.

Case 3: Receiving data holders

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

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

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

- the data is of a class that the accredited data recipient would generate or collect in the ordinary course of its business outside of the CDR; and
- the accredited data recipient would use the information for the same purpose as their ordinary business.

Example 1.3

EVBank became an accredited person so that it is able to receive CDR data.

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

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

EVBank will be considered a data holder for Martin's historical banking information and this information will be subject to the APPs.

Example 1.4

EVBank became an accredited person so that it is able to receive CDR data.

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

EVBank receives this data comprising energy information of the type EVBank does not ordinarily hold. EVBank collects that data about Sean as an accredited data recipient. EVBank would be considered an accredited data recipient for the energy information it receives and would need to meet the associated Privacy Safeguards.

Accredited persons and accredited data recipients

1.89 An accredited person is a person who holds an accreditation. To be granted an accreditation, the person must satisfy the criteria in the consumer data rules for accreditation. As discussed above, an accredited data recipient is an accredited person who has received CDR data. They are only an accredited data recipient in relation to that CDR data. The legislation uses the terms accredited person and accredited data recipient to differentiate between processes in the flow of CDR data. [***Schedule 1, item 1, subsection 56CA]***

1.90 It is the nature of the particular CDR data which will determine when an entity or person is an accredited data recipient for that data and not a data holder or designated gateway.

1.91 An accredited data recipient for CDR data is 'licensed' to receive CDR data through the CDR system and has received that data as a result of a disclosure made in accordance with the CDR rules. ***[Schedule 1, item 1, subsection 56AK]***

1.92 Being an accredited data recipient will be essential in order to be able to receive data about a consumer. The consumer data rules will provide that a CDR consumer's right to access their data and direct a data holder to transfer the data to another entity under the CDR, exists only where the entity is an accredited person.

1.93 The Bill achieves this outcome by imposing a limitation on the ACCC's rule making power. The ACCC can only write rules which mandate disclosure of a consumer's data, where the disclosure is to an accredited person, a designated gateway, or the consumer themselves. ***[Schedule 1, item 1, subsection 56BD(1)]***

1.94 The consumer data rules will set out the process and criteria for an entity or person to seek an accreditation. The Bill also describes the functions of a data recipient accreditor which will be undertaken by a Commonwealth entity and whose primary role will be to accredit persons and entities.

Designated gateway

1.95 The Minister may also designate a 'gateway', or multiple 'gateways' to facilitate the transfer of data between a data holder and accredited data recipient or the consumer. The Government expects that there will be limited circumstances when a gateway will be designated. ***[Schedule 1, item 1, subsection 56AL(2)]***

1.96 A factor that would be considered in deciding whether to designate a gateway would be whether there was an entity that already had a relationship with the data holders and that transferring data through the gateway would be an efficient and cost effective way to exercise the data

right. Another factor may include the relative risk of the data sets that would be expected to flow through the gateway.

1.97 The Government expects that the gateway would be a Commonwealth body or entity, or within the effective control of the Commonwealth or a State or Territory.

1.98 An example of where a gateway may be designated is for the energy sector. One option being considered would be to designate the Australian Energy Market Operator (AEMO) as the gateway. In this scenario, the ACCC would make rules requiring the data holders in the energy sector to meet an obligation to disclose CDR data by disclosing the data to AEMO. Similarly the ACCC would make a rule requiring AEMO to disclose the data to the accredited persons or the consumer in accordance with the request made by the consumer.

1.99 Recognising the distinct role of the gateway, the ACCC's rule making powers about a gateway are limited by the Bill.

CDR consumer

1.100 A CDR consumer is the person or entity that holds the 'rights' to access the data held by a data holder and to direct that this data be shared with an accredited person. For the purposes of the CDR a consumer can be an individual or a business. The existing definition in the CC Act is narrower and so the Bill inserts a new definition of CDR consumer into the CC Act for the purposes of the CDR which means that the ordinary broader meaning of consumer applies for the CDR. ***[Schedule 1, item 1, subsections 56AI(3) and 56AI(4)]***

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

1.102 Whether a person or entity is a CDR consumer depends on the data in question and whether the person or entity can be identified, or reasonably identified, from that data or from data that is already held by the data holder or accredited data recipient and whether it 'relates' to that person or entity.

1.103 Determining whether a person can be 'reasonably' identified from the data requires contextual consideration, including the nature and amount of information, other information that may be available to the persons who will have access to the information, and the practicability of using that information to identify a person.

1.104 An important consideration in whether data can be considered to relate to a 'reasonably identifiable' person is what motivations there may

be to attempt re-identification. A person will be reasonably identifiable where:

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

1.105 The consumer data rules, OAIC guidance and data standards may provide further requirements for when information can be considered to be de-identified.

1.106 The concept of 'relates to' is a broader concept than information 'about' an identifiable or reasonably identifiable person under the *Privacy Act 1988*. For example, using this term is intended to capture meta-data of the type found not to be about an individual in *Privacy Commissioner v Telstra Corporation Limited* [2017] FCAFA 4 (19 January 2017).

1.107 'Relates' can include reference to an identifier such as a name, an identification number, location data of the person or of products that would reasonably be expected to be co-located with either the person or their address, an online identifier (including cookie identifiers and internet protocol addresses) or to one or more factors specific to the physical, physiological, genetic, mental, behavioural (including predictions of behaviours or preferences), economic, cultural or social identity or characteristics of that person.

1.108 Where information is primarily about a good or service, but reveals information about a consumer's use of that good or service, it relates to the consumer.

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

1.110 The rules can specify which consumers have the rights to access and direct the disclosure of data. It is expected that the consumer who will have access to the right will be significantly narrower due to the operation of the rules on a sector by sector basis. For example, in the banking sector, it is expected that for individuals, an associate will mean an account holder, or, in the case of credit cards, additional card holders.

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

Example 1.5

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

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

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

Example 1.6

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 banking data to a FinTech, McDanMoney, to check whether it is getting the best banking services.

The consumer data rules provide that large consumers have the right to access data and request a transfer of their data where the consumer receives services that are generally available.

Stately Bank has data about TBM that is covered by the designated data set applying to the banking sector, and TBM uses banking services that are generally available (and not bespoke), TBM is a CDR consumer and is able to participate in the CDR system.

CDR data

1.113 CDR data is data outlined in the instrument designating a sector and any information that is subsequently derived from that data. CDR data can include product information or records of usage of a good or service. The data can relate to natural and legal persons, for example a company. ***[Schedule 1, item 1, subsections 56AI(1) and 56AI(2)]***

1.114 The definition of CDR data includes data that is 'derived' from data listed in the designation instrument. It means that the Privacy Safeguards continue to apply to CDR data that relates to a consumer even if it has been subsequently transformed in the hands of the accredited data recipient.

1.115 While the definition of CDR data may appear broad, there are limits on the data that data holders may be required to give access to:

- For data that relates to a CDR consumer, a data holder can only be required to disclose that data to an accredited person, designated gateway or the consumer themselves. In this circumstance the data is also limited to data that is specified in the instrument and does not include data that is derived from data specified in the instrument. ***[Schedule 1, item 1, subsection 56BD(1)]***
- For data about a product, good or service, a data holder can only be required to disclose data about the eligibility criteria, terms and conditions, price, availability or performance of the product, good or service. Disclosure about the availability or performance can only be mandated where this data is publicly available. ***[Schedule 1, item 1, subsection 56BF(1)]***

1.116 CDR data is also subject to geographical limitations. Information of a class specified in a designation instrument will be treated as CDR data where it is generated or collected in Australia:

- by an Australian person (for example a telecommunications company), or
- relates to an Australian person, or goods or services offered to an Australian person (for example a CDR consumer).

1.117 Information of a class specified in a designation instrument will be treated as CDR data where it is generated or collected outside Australia:

- by an Australian person (for example a telecommunications company), and
- relates to an Australian person (for example a CDR consumer), or to goods or services offered to an Australian person (for example a CDR consumer).

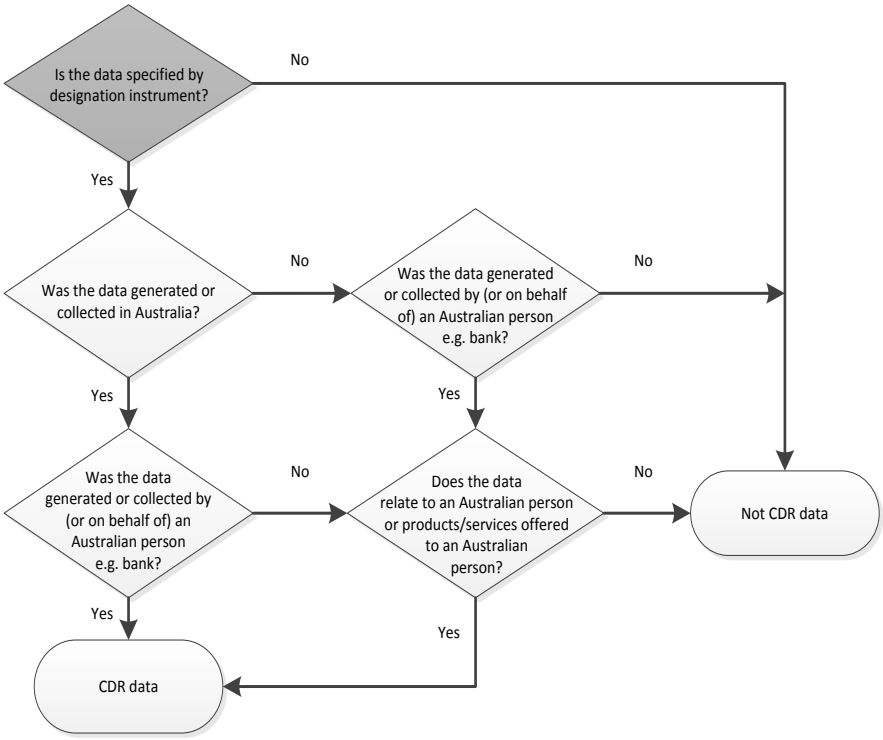
[Schedule 1, item 1, subsection 56AC(3)]

1.118 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.

1.119 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 and it relates to an Australian consumer.

1.120 These geographical limitations are illustrated by diagram 1.1.

Diagram 1.1 What is 'consumer data'?



1.121 Australian person includes a body corporate, an Australian citizen or permanent resident, or person who is ordinarily resident within greater Australia, or a Government entity. ***[Schedule 1, item 1, subsection 56AO(5)]***

Principle of Reciprocity

1.122 The consumer data rules may provide that a consumer can direct an accredited data recipient to provide access to certain CDR data to the consumer or other accredited persons. This is known as the principle of reciprocity.

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

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

1.125 Reciprocity operates to allow the ACCC to write rules requiring certain accredited data recipients to provide consumers access to, or the ability to request transfer of CDR data, to accredited persons.

1.126 Reciprocity is a right for consumers, and as such, data is only able to be disclosed according to the principle of reciprocity when a consumer has made a valid request.

1.127 The principle of reciprocity may apply in three circumstances. First where an entity is included in a designation instrument but there is not a consumer data rule requiring that data holder (as defined in case 1 at 1.81) to disclose that information.

1.128 An example of this would be where a small ADI is not required to disclose banking information at a consumer's request before 1 July 2020. However, if the small ADI becomes an accredited data recipient before this date, the consumer data rules may require the small AD to transfer data at the request of the consumer.

1.129 Similarly, the principle of reciprocity may apply where an accredited data recipient is not included in the designation but holds data that it has generated or collected itself outside of the CDR. For example, a non-ADI lender would hold data that is included in the designation instrument. The consumer data rules may require the accredited data recipient to transfer data at the request of the consumer.

1.130 The final circumstance where the principle of reciprocity may apply is where the ACCC writes rules requiring accredited data recipients to disclose data that they have received through the CDR to another accredited person at the consumer's request.

1.131 If an accredited data recipient does not hold data that falls within a class designated in a designation instrument, reciprocity cannot apply. That is, reciprocity only applies to data included in the designation instrument. This is because the transfer of the data needs to be supported by data standards to occur efficiently.

Chargeable data

1.132 The Bill also introduces the idea of 'chargeable data'. This is the data that a person is required to disclose where the Minister has stated in the designation instrument that specific persons can charge a fee, either for the use or disclosure of the data, or both. The Minister may also specify, in the designation instrument, the circumstances when a person can charge a fee for that data. The Minister cannot make determinations about fees regarding merely authorised (but not required) disclosures of CDR data. ***[Schedule 1, item 1 paragraph 56AC(2)(d) and section 56AM; and Schedule 1, item 10, subsection 4(1)]***

Example 1.7

Data holders in sector X are designated in respect of data set A. Data set A is intellectual property.

There are strong competition, consumer, and privacy benefits to the designation of data set A.

The Minister designates data set A as a chargeable data set for the use of data set A. Data holders are able to set their own reasonable fees for the disclosure and licence to use data set A.

Example 1.8

Data holders in sector Y are designated in respect of data set B. Data holders in sector Y are not legally required to collect or hold data set B, but choose to do so for their own reasons.

There is a strong consumer welfare benefit to consumers being able to access data set B.

There is compelling evidence that if data set B is designated, data holders in sector Y would stop collecting and holding data set B. If allowed to charge a fee for the disclosure of data set B, data holders in sector Y would continue to collect and hold data set B.

The Minister designates data set B as a chargeable data set for both the disclosure and use of data set B. Data holders are able to set their own reasonable fees for the disclosure and licence to use data set B.

1.133 If data is not listed as chargeable data in the designation instrument the person cannot charge a fee for the data. Similarly, the person cannot charge a fee for the use or disclosure where the circumstances specified in the designation instrument have not been met. ***[Schedule 1, item 1, sections 56AM and 56BT]***

Example 1.9

Data holders in sector A are designated in respect of data set Z. Data holders incur initial costs of $100 million to meet their obligations under CDR, but their additional costs per disclosure of CDR data are minimal.

The Minister designates data set Z and does not specify that data set Z is a chargeable data set. Data set Z is a fee-free data set and data holders are not able to set fees for the disclosure or use of data set Z.

1.134 A civil penalty applies where a data holder charges a fee and was not permitted to do so. This is explained further at paragraph 1.406.

1.135 For fee-free data sets, persons would still be able to incorporate the cost of disclosing data into their cost base for provision of the original good or service. They must not put in place arrangements that have the effect of requiring a person who uses the system to pay more than persons who do not. Persons who make authorised (but not required) disclosures

under the CDR are also able to choose what charge, if any, may apply to that authorised disclosure.

1.136 Generally, where a person can charge a fee for CDR data, the Government expects the person to determine and set their own reasonable fee.

1.137 However, the ACCC can determine that a fee is unreasonable and set a fee amount for a particular data holder or an accredited data recipient or a class of data holders or accredited data recipients. This power only applies to fees for required disclosures and does not extend to fees for authorised disclosures. ***[Schedule 1, item 1, section 56BU]***

1.138 The term 'unreasonable' is not defined in the Bill. The Government expects that the ACCC will issue guidance to explain how it will exercise its intervention powers.

1.139 However, the Bill does include factors that the ACCC must have regard to in deciding that a fee is unreasonable. These factors are the effect of the fee on:

- consumers;
- efficiency of relevant markets; and
- promoting competition.

[Schedule 1, item 1, subsection 56BU(3)]

1.140 The ACCC will also consider whether requiring the disclosure of the data and allowing the use of the data would include any intellectual property; would be an acquisition of property, whether data holders in that sector currently charge a fee for the data, the marginal cost to the person of disclosing the data and any other matters the ACCC considers relevant. ***[Schedule 1, item 1, subsection 56BU(3)]***

1.141 For example, a fee may be considered unreasonable because the person charges different fees to different persons or entities depending on the business relationship the person has with the recipient.

1.142 When determining the fee amount or method to determine the fee, the ACCC must seek to ensure the amount is reasonable having regard to the matters set out in paragraphs 1.139 and 1.140. In addition the ACCC should seek to ensure that the resulting fee will cover the costs incurred by the person that were necessary and reasonable to meet its CDR obligations for the chargeable matter. For example, if the data set is chargeable only for the disclosure of the data set, the fee would reflect the costs that are necessary and reasonable to meet the disclosure obligation. ***[Schedule 1, item 1, subsection 56BU(2)]***

1.143 A civil penalty will apply if a CDR participant charges a fee higher than the fee set by the ACCC or that is worked out under the method set by the ACCC after determining that the original fee was

unreasonable. This is explained further at paragraph 1.406. ***[Schedule 1, item 1, section 56BT(2)]***

1.144 When the determination is made about a particular CDR participant, the CDR participant included in the determination or a person affected by the determination may apply to have the determination reviewed by the Australian Competition Tribunal (the Tribunal). The application must be made within 21 days of the determination. ***[Schedule 1, item 1, section 56BV]***

1.145 If the Tribunal receives an application it must review the determination and may either make a decision affirming, setting aside or varying the original determination. ***[Schedule 1, item 1, subsections 56BV(3) and 56BW(1)]***

1.146 A decision made by the Tribunal is taken to be a determination of the ACCC. The Tribunal may require the ACCC to give the Tribunal any information or assistance it requires. The Tribunal may also consider any information or evidence given to the ACCC when making the original determination as part of the review. ***[Schedule 1, item 1, subsections 56BW(2), 56BW(3) and 56BW(4)]***

1.147 A determination made about a class of data holders or accredited data recipients will be a legislative instrument and will be subject to disallowance by Parliament. ***[Schedule 1, item 1, subsection 56BU(4)]***

1.148 Division 1 of Part IX of the CC Act does not apply to a review by the Tribunal. ***[Schedule 1, item 1, section 56BX]***

Extraterritorial operation of the CDR provisions

1.149 The CDR regime generally applies both within and outside of Australia. ***[Schedule 1, item 1, section 56AN and subsection 56AO(1)]***

1.150 Where the CDR data is held within Australia obligations under the CDR regime apply to both Australian and foreign persons. ***[Schedule 1, item 1, subsection 56AO(2)]***

1.151 Where the CDR data is held outside of Australia, the CDR applies to acts or omissions:

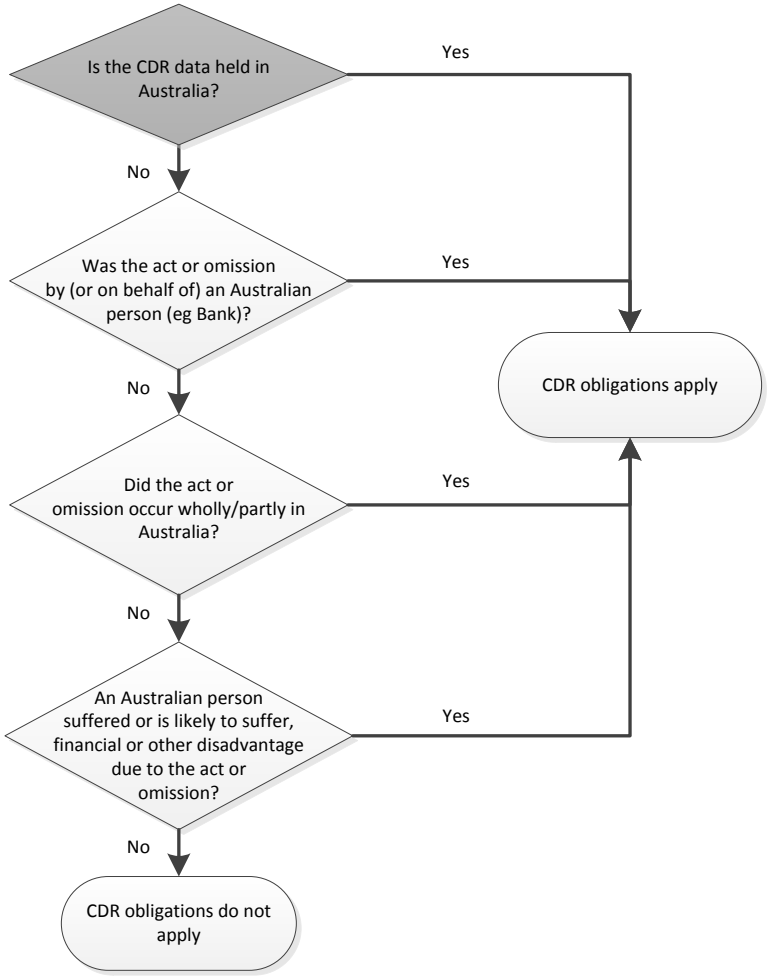
- by (or on behalf of) an Australian person;
- that occur wholly or partly in Australia; or
- that occur wholly outside Australia and an Australian person suffers, or is likely to suffer financial or other disadvantage as a result of the conduct. ***[Schedule 1, item 1, subsection 56AO(3)]***

1.152 An act or omission that occurs partly in Australia includes sending, refusing to send, causing to be sent, or refusing to cause to be sent CDR data from a foreign country to Australia, and from Australia to a foreign country. ***[Schedule 1, item 1, subsection 56AO(4)]***

1.153 Division 14 (Standard geographical jurisdiction) of the Criminal Code does not apply to an offence against the CDR provisions. ***[Schedule 1, item 1, section 56AP]***

1.154 The extraterritorial operation of the CDR regime is illustrated in the diagram below.

Diagram 1.2 Extraterritorial application



Consumer Data Rules

1.155 Key elements of the CDR framework will be governed by consumer data rules, including turning on a consumer's 'rights' to access or disclose CDR data.

1.156 The ACCC may make consumer data rules on a range of elements of the CDR system. ***[Schedule 1, item 1, subsection 56BA(1)]***

1.157 In particular, the consumer data rules may apply to:

- disclosure, use, accuracy, storage, security or deletion of CDR data***; [Schedule 1, item 1, paragraphs 56BB(a) and 56BB(b), and sections 56BC and 56BE]***
- designated gateways for CDR data; ***[Schedule 1, item 1, paragraph 56BB(c) and section 56BG]***
- accreditation of data recipients; ***[Schedule 1, item 1, paragraph 56BB(d) and section 56BH]***
- reporting and record keeping; ***[Schedule 1, item 1, paragraph 56BB(e) and section 56BI]***
- any other matters incidental to the CDR system. ***[Schedule 1, item 1, paragraph 56BB(f) and section 56BJ]***

1.158 A person who fails to comply with the consumer data rules may be subject to a civil penalty as defined in the *Regulatory Powers (Standard Provisions) Act 2014* (Regulatory Powers Act). However, the civil penalty regime which applies to the consumer data rules is established in the CC Act not the Regulatory Powers Act. The consumer data rules can apply lower civil penalty amounts than the amounts in the Bill. See paragraph 1.406 for an explanation of the civil penalties. ***[Schedule 1, item 1, section 56BL]***

1.159 The consumer data rule making power provides 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, paragraph 56BA(2)(a)]***

1.160 Nevertheless, when making rules, the ACCC should seek to ensure that rules between sectors are as consistent as possible to allow for interoperable standards. Consistency and interoperability will facilitate the emerging data transfer system and ensure consumers are able to navigate the emerging data economy as active participants.

1.161 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)]***

1.162 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 56BA(2)(d)]***

1.163 There are checks and balances on the ACCC rule making powers and the process for making rules. 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.

1.164 The 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 about the new CDR system.

1.165 Due to the operation of the *Acts Interpretation Act 1901,* the same processes must be followed when existing rules are varied or revoked.

1.166 There are also limitations on the rules the ACCC can make. 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 56BK(1)]***
- require the disclosure of information about a consumer unless that information is specified in the designation instrument and the disclosure is to a CDR consumer, accredited person or designated gateway; ***[Schedule 1, item 1, subsection 56BD(1)]***
- require the disclosure of information about a product or a good or service unless the data is about eligibility criteria, terms and conditions, price, or publicly available information about the availability or performance of the product; ***[Schedule 1, item 1, subsection 56BF(1)]***
- allow a fee to be charged for data for which a fee cannot be charged; ***[Schedule 1, item 1, subsections 56BD(2) and 56BF(2)]***
- impose deletion obligations on a data holder for CDR data about a consumer; ***[Schedule 1, item 1, paragraph 56BD(3)(a)]***
- require the data holder to do anything in relation to the use, accuracy, storage or security of the CDR data unless those rules also relate to the disclosure of the CDR data under the consumer data rules; and ***[Schedule 1, item 1, paragraph 56BD(3)(b)]***
- require or authorise a designated gateway to do anything in relation to the collection, use, storage, or disclosure of the CDR data unless those rules also relate to the gateway

facilitating the transfer of CDR data between data holders, accredited data recipients or the consumer. ***[Schedule 1, item 1, subsection 56BG(3)]***

1.167 Regulations may further limit matters that the consumer data rules are able to deal with or the requirements the rules can impose on the CDR system including data sets or kinds of persons. ***[Schedule 1, item 1, subsection 56BK(3)]***

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

1.168 The consumer data rules will outline requirements to be met by data holders, accredited persons and accredited data recipients, designated gateways or consumers about disclosure, collection, use, accuracy, storage or security of CDR data where that data relates to a CDR consumer or in cases when it does not relate to a CDR consumer (for example product information). ***[Schedule 1, item 1, sections 56BC, 56BE and 56BG]***

1.169 The disclosure rules will cover matters such as how consumers consent to the disclosure of CDR data and the processes under which data holders, accredited data recipients and designated gateways must disclose CDR data. The disclosure rules will work in conjunction with the Privacy Safeguards in regulating the disclosure of CDR data which relates to a consumer. The Government expects that if consent is required for the disclosure of a type of CDR data, that consent will be express. ***[Schedule 1, item 1, sections 56BC, 56BE and 56EI]***

1.170 Authority to disclose CDR data is generally restricted. The consumer data rules will establish the framework about consumer requests to disclose CDR data about the consumer and may include different levels of consent to be provided reflecting the more sensitive nature of some of the information that will become CDR data. ***[Schedule 1, item 1, subsection 56BC(1)(b)]***

1.171 Consumer data rules will be set out for CDR consumers, data holders, accredited data recipients and designated gateways 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.

1.172 The consumer data rules may also deal with circumstances when a CDR participant is authorised, but not required to disclose CDR data to a person and the way a consumer can consent to this disclosure. ***[Schedule 1, item 1, subsection 56BC(2)]***

1.173 For example, a consumer may want an accredited data recipient to share certain information with a person outside of the CDR system. In

order to do this, the consumer data rules may set out how the consumer may consent and the types of statements and notifications that the accredited data recipient must give to the consumer before the disclosure is made.

1.174 The consumer data rules may also deal with other matters such as when the CDR data needs to be deleted and how it will be deleted by accredited data recipients, accredited persons, CDR consumers or other persons depending on whether the CDR data relates to a CDR consumer or is product data. ***[Schedule 1, item 1, paragraph 56BC(3)(c) and subsection 56BE(d)]***

Accreditation of data recipients

1.175 Consumer data rules will be made about the accreditation of data recipients under the CDR system. ***[Schedule1, item 1, section 56BH]***

1.176 Consumer data rules may be made:

- about the powers and functions of the Data Recipient Accreditor;
- specifying the criteria for a person to be accredited;
- outlining that accreditations may only be provided subject to applicants meeting certain conditions, including that conditions may be applied 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;
- about 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 56BH]

1.177 The consumer data rules 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). ***[Schedule 1, item 1, subsection 56BH(3)]***

1.178 Any rules which enable decisions to be made about the granting, revocation, variation or suspension of accreditations must also allow for the review of those decisions by the Administrative Appeals Tribunal. ***[Schedule 1, item 1, subsection 56BH(4)]***

1.179 Paragraphs 1.231 to 1.251 further explain the accreditation process.

Rules about designated gateways

1.180 Where a gateway has been designated for a sector the consumer data rules may require use of that designated gateway to facilitate the transfer of data between the data holder and consumer or accredited person where the data relates to a consumer. ***[Schedule 1, item 1, section 56BG]***

1.181 The consumer data rules will set out the role of, and may impose requirements on, the designated gateway. These rules would include the process for a consumer to make a valid request for the disclosure of information and other rules about the disclosure, use, collection accuracy, storage, security or deletion of the CDR data. ***[Schedule 1, item 1, paragraphs 56BG(1)(c) and 56BG(2)(b)]***

1.182 The consumer data rules may also impose requirements on a designated gateway to facilitate the transfer of product data between the data holder and consumer or and person requesting the information. ***[Schedule 1, item 1, subsection 56BG(2)]***

1.183 Consumer data rules about a designated gateway may include rules for when the designated gateway ceases to be the designated gateway. These rules may deal with the deletion of CDR data by the former designated gateway and a requirement that the former designated gateway transfer CDR data to another gateway. ***[Schedule 1, item 1, subsection 56BG(3)]***

Reporting and record keeping

1.184 The ACCC will make consumer data rules on reporting and record keeping including outlining the requirements for data holders, accredited data recipients, accredited persons and designated gateways to give specified reports to the ACCC, to the Information Commissioner or to the CDR consumer. ***[Schedule 1, item 1, section 56BI]***

1.185 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. ***[Schedule 1, item 1, section 56BI]***

1.186 It is expected that data holders, accredited data recipients and designated gateways 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, paragraphs 56BI(1)(d), 56BI(1)(e) and 56BI(1)(f)]***

1.187 Record keeping requirements will relate to ensuring compliance with the consumer data rules and will be used by both regulators for this purpose. ***[Schedule 1, item 1, paragraph 56BI(1)(g)]***

Example 1.10

Soh-Yeon, a CDR consumer in the banking sector wishes to review the CDR data access permissions she has 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 1.11

Soh-Yeon lodges a complaint with the OAIC that a bank disclosed her CDR data without her 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.

1.188 Consumer data rules may also be made which require the Data Recipient Accreditor, Accreditation Registrar or Data Standards Chair to give reports to the ACCC or OAIC about the functions or powers of those entities. ***[Schedule 1, item 1, paragraph 56BI(1)(h)]***

1.189 The consumer data rules may also require data holders, accredited data recipients, designated gateways, or accredited persons to give the ACCC or OAIC copies of the records required to be kept by the consumer data rules or information in these records. ***[Schedule 1, item 1, subsection 56BI(2)]***

1.190 This information could be required to be given in an approved form. ***[Schedule 1, item 1, paragraph 56BJ(e)]***

Incidental or related matters

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

- requirements about the data standards; ***[Schedule 1, item 1, subsection 56BJ(a)]***
- circumstances where persons are relieved from compliance with the consumer data rules that would otherwise apply to them; ***[Schedule 1, item 1, subsection 56BJ(b)]***
- a rule that depends on a person or body being satisfied of one or more specified matters; ***[Schedule 1, item 1, subsection 56BJ(c)]***
- the internal review processes that participants must establish and have in place for CDR or for making applications to the Administrative Appeals Tribunal as well as internal dispute resolution processes; ***[Schedule 1, item 1, paragraphs 56BJ(d) and 56BJ(g)]***

- the manner in which persons or bodies may exercise powers under the consumer data rules or must meet the requirements under consumer data rules; ***[Schedule 1, item 1, paragraph 56BJ(e)]***
- requirements for documents to be provided in a form approved by either the ACCC or the Information Commissioner; ***[Schedule 1, item 1, paragraph 56BJ(e)]***
- the manner in which a data holder or accredited data recipient may charge a fee, the time in which a fee can be paid and how the fee needs to be communicated; ***[Schedule 1, item 1, paragraph 56BJ(f)]***
- external dispute resolution processes, including the criteria that the process must meet; ***[Schedule 1, item 1, paragraph 56BJ(g)]***
- external dispute resolution schemes including access to such schemes; ***[Schedule 1, item 1, paragraph 56BJ(h)]***
- transitional rules with regard to external resolution of disputes; and ***[Schedule 1, item 1, paragraph 56BJ(i)]***
- other matters about the consumer data rules. ***[Schedule 1, item 1, paragraph 56BJ(j)]***

1.192 Some of these matters are covered by other parts of the CDR. In particular, as discussed below at paragraphs 1.290 to 1.295, dispute resolution processes are specifically required by participants in the CDR system.

1.193 Other matters, including requirements about approved forms and where data holders, accredited data recipients, accredited persons and designated gateways 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 participants is smooth, clear and transparent and obligations established by the consumer data rules are well understood.

1.194 Consumer data rules are able to be made with respect to other matters including the data standards, the de-accreditation and suspension of accreditation, and other related matters as well as extensions or clarification of the Privacy Safeguards.

1.195 The consumer data rules are not to be inconsistent with the Privacy Safeguards or any other part of the CDR legislation. Were this to occur, the primary legislation would prevail. ***[Schedule 1, item 1, subsection 56EC(1)]***

Limitations on matters that can be included in the consumer data rules

1.196 As discussed above, there are limitations on the scope of the consumer data rules.

1.197 In line with the proposed commencement date for the Bill, the consumer data rules are unable to require a CDR participant to disclose data prior to 1 July 2019. ***[Schedule 1, item 1, subsection 56BK(1)]***

1.198 However, on or after this date the consumer data rules may require a person to do something with CDR data that was generated or collected by the person earlier than the commencement of the Bill. This 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 time the relevant data holder collects information post-designation. ***[Schedule 1, item 1, subsection 56BK(2)]***

1.199 The consumer data rules can also be limited via regulation. The regulations may provide that consumer data rules are unable to deal with matters specified in regulations or that the consumer data rules should not impose certain requirements as specified in the regulations. ***[Schedule 1, item 1, subsection 56BK(3)]***

1.200 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.

1.201 For example, a designation instrument for the banking sector may 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 the data falls within the definition of CDR data for the banking sector, and if they were accredited data recipients (see the explanation of the principle of reciprocity at paragraphs 1.122 to 1.131).

1.202 These limitations, along with the Ministerial oversight and Parliamentary scrutiny of the consumer rules as legislative instruments, will ensure that the rules remain appropriate and adapted. So while the ACCC has broad rule making powers, this is both balanced and appropriate to enable rules to be tailored as the CDR is rolled out across sectors of the economy. A requirement to come back to Parliament to make rules for each new designation, or to make changes to existing rules, would limit the ability of the CDR to expand and provide competition benefits to consumers in various sectors of the economy.

Example 1.12

Paul seeks to use the CDR system to access specified CDR data generated between 2002 and 2018 for CDR data that was designated in December 2019.

The designation instrument is only able to capture data that was generated or collected two years prior to the designation. In addition,

the regulations provide that a data holder does not need to provide access to data older than six-years old.

Paul seeks to access this data in December 2022. He is able to access CDR data that was generated or collected from 1 January 2017 to December 2022. In this instance Paul's access to older data is limited by the designation instrument.

Paul seeks to access this data in December 2025. He is able to access CDR data that was generated or collected from December 2019 to December 2025. In this instance Paul's access to older data is limited by the regulations.

The Minister set these limitations informed by the ACCC's sectoral assessment, which examined the data retention and retrieval arrangements for that sector.

Process for making consumer data rules

1.203 Before making the consumer data rules the ACCC is required to consider the same matters that the Minister must consider before designating a sector but not the factors the Minister considers when determining that data is 'chargeable'. ***[Schedule 1, item 1, section 56BP]***

1.204 These matters include the likely impact of the proposed rules on consumers, competition, innovation, privacy and confidentiality, the public interest, intellectual property and relevant markets.

1.205 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 56BP]***

1.206 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 the consumer data rules. ***[Schedule 1, item 1, paragraph 56BQ(1)(b)]***

1.207 Consultation with each of these key stakeholders seeks to ensure that the right balance is struck between protection of individuals' rights including the right to privacy and making sure that the regulatory burden does not outweigh the broadly defined benefits to be gained from the consumer data rules.

1.208 The ACCC must consult for at least 28 days and is unable to make the rules for at least 60 days from when the rules were released for public consultation. ***[Schedule 1, item 1, paragraphs 56BQ(1)(a) and 56BQ(1)(c)]***

1.209 A failure to consult will not invalidate the consumer data rules. However, the consumer data rules are disallowable instruments so the

Parliament has the capacity to intervene and disallow the rules. ***[Schedule 1, item 1, subsection 56BQ(2)]***

1.210 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 56BR]***

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

1.212 Due to the operation of the *Acts Interpretation Act 1901*, the same processes (consultation and the Minister's consent) must be followed when an existing consumer data rule is varied or revoked.

1.213 As noted above, the ACCC may make consumer data rules without the Minister's consent in emergency situations after it has consulted with the Information Commissioner. ***[Schedule 1, item 1, subsection 56BS(1)]***

1.214 This will provide the ACCC with the ability to make rules if the ACCC is of the view that making the rules is necessary to avoid a risk of serious harm to the efficiency, integrity and stability of any aspect of the Australian economy or the interests of consumers. ***[Schedule 1, item 1, subsection 56BS(1)]***

1.215 Given the nature of the CDR regime, a significant data breach could be considered to cause serious harm to the interests of consumers.

1.216 The ACCC is provided with this emergency rule making power to respond to an emerging issue, for example a previously unforeseen practice which presents a 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.

1.217 If the ACCC makes an emergency rule 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 56BS(2)(a)]***

1.218 The Minister may respond by advising that the consumer data rule be either amended or revoked, in accordance with a written direction of the Minister. ***[Schedule 1, item 1, paragraph 56BS(2)(b) and subsection 56BS(3)]***

1.219 The Minister's direction to vary or revoke a rule is not a legislative instrument because it is not a legislative instrument within the meaning of subsection 8(1) of the *Legislation Act 2003*. ***[Schedule 1, item 1, subsection 56BS(6)]***

1.220 The requirement to consult does not apply where the Minister has directed the ACCC to repeal or revoke an emergency rule. ***[Schedule 1, item 1, subsection 56BS(7)]***

1.221 A failure to consult the Information Commissioner does not invalidate the emergency consumer data rules. However, if the ACCC does not consult the Information Commissioner before making the emergency rules but the Minister does not direct the ACCC to vary or revoke the emergency rule, the rule will cease to be in force 6 months after the day it was made. ***[Schedule 1, item 1, subsections 56BS(3), 56BS(4) and 56BS(5)]***

The Data Recipient Accreditor

1.222 As discussed above, a person or entity wanting to receive CDR data that relates to a consumer will need to be accredited.

1.223 The Data Recipient Accreditor is responsible for the accreditation of entities and any other functions included in the consumer data rules or that are necessary for the performing of the Data Recipient Accreditor's functions. ***[Schedule 1, item 1, subsections 56CA(1), 56CH(1) and 56CH(2)]***

1.224 The Data Recipient Accreditor is appointed by the Minister and can be an accountable authority of a Commonwealth entity or a Commonwealth entity. An example of an 'accountable authority' would be Secretary of a Department. The Minister can terminate the appointment at any time. ***[Schedule 1, item 1, section 56CG]***

1.225 If the Minister does not make an appointment, the ACCC is the Data Recipient Accreditor. It is the Government's intention that the Data Recipient Accreditor will initially be the ACCC. ***[Schedule 1, item 10, subsection 4(1)]***

1.226 The functions of the appointed authority or entity are taken to include the functions of the Data Recipient Accreditor as well as the functions that are normally undertaken by the person or entity. ***[Schedule 1, item 1, subsection 56CH(3)]***

1.227 The Minister can give binding directions of a general nature to the Data Recipient Accreditor about the performance of the Accreditor's functions and powers. ***[Schedule 1, item 1, section 56CI]***

1.228 The Data Recipient Accreditor may also delegate any of its powers and functions. 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. Where a power or function is delegated, the delegate must comply with any directions given by the Data Recipient Accreditor. ***[Schedule 1, item 1, section 56CJ]***

1.229 The ability for the Data Recipient Accreditor to delegate any or all of the functions or powers of that role to APS employees not at the SES level is necessary. Given the broad nature of the CDR regime requiring an SES level officer to undertake all delegated functions would be burdensome where the tasks would be more appropriately undertaken by a more junior officer. The delegations allow for the best use of resources.

1.230 The Bill provides that each annual report prepared by the Data Recipient Accreditor must include information about the performance of the Data Recipient Accreditor's functions and exercise of the Data Recipient Accreditor's power during that period. The Bill does not require Data Recipient Accreditor to prepare an annual report. Any such requirement is specified by existing laws where appropriate. The Bill simply requires that the annual report include information about the person or entity's role as Data Recipient Accreditor. ***[Schedule 1, item 1, subsection 56CH(4)]***

Accreditation process

1.231 Accreditation will be based on criteria established in the consumer data rules. 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.

1.232 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 56CA(2)(a)]***

1.233 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. The rules are also capable of recognising foreign licences. ***[Schedule 1, item 1, paragraph 56CA(2)(b)]***

Example 1.13

A FinTech organisation offers a budgeting app, which takes into account transaction data available under the UK Open Banking regime. The FinTech holds 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 but the rules may allow for a more streamlined process in recognition that the FinTech's existing license under the UK Open Banking regime.

Example 1.14

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 data 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.

1.234 Accreditation is granted on the basis that no compensation is payable if the accreditation is varied, transferred, suspended, revoked or suspended in anyway. ***[Schedule 1, item 1, subsection 56CA(3)]***

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

1.236 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.

1.237 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 56BH(1)(d)]***

Example 1.15

Will's Energy Solutions, an Australian energy tech, with Kathryn's consent, seeks only CDR data on the balance of Kathryn's account. The rules might provide that Will's Energy Solutions only requires a lower level of accreditation to access this data.

Example 1.16

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.

1.238 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 56BH(2)]***

1.239 Consumer data rules may also be made about reporting and record keeping requirements to be met by accredited data recipients. Further detail on these consumer data rules is at paragraphs 1.184 to 1.190.

1.240 Accreditation requirements under the CDR do not remove the need for accredited persons to obtain any other required licences for business they are undertaking. For example, if a FinTech is providing financial services as defined in the *Corporations Act 2001* and the *Corporations Regulations 2001*, it will also be required to hold an Australian Financial Services licence.

Review of decisions refusing to accredit

1.241 If the Data Recipient Accreditor refuses to grant an accreditation, the entity applying for an accreditation is able to seek review of the Data Recipient Accreditor's decision at the Administrative Appeals Tribunal. ***[Schedule 1, item 1, section 56CB]***

1.242 Where the consumer data rules outline processes for the variation, suspension or revocation of accreditations, these rules must also provide for Administrative Appeals Tribunal review of those decisions. ***[Schedule 1, item 1, subsection 56BH(4)]***

Prohibition on 'holding out'

1.243 In order to protect CDR consumers and others participating in the CDR system it is an offence for a person to create or foster the perception by others that they are an accredited data recipient. This equally applies to a failure by a person to correct the perception that they are accredited, when they are not. The Bill refers to this as the person 'holding out' that they are accredited. ***[Schedule 1, item 1, sections 56CC and 56CD]***

1.244 An act or omission by a person which results in others holding the belief that they are a person with an accreditation or that they are a person holding an accreditation that has been granted at a particular level and therefore able to deal with sensitive CDR data, when they do not have this level of accreditation, is an offence and civil penalty. ***[Schedule 1, item 1, section 56CC and 56CD]***

1.245 For an offence, the fine for a body corporate includes three possible penalty amounts taking into account the benefit gained from committing the offence and the size of the business, based on the body corporate's annual turnover. ***[Schedule 1, item 1, subsection 56CC(2)]***

1.246 If the court can determine the value of the benefit obtained from the offence then the maximum penalty is the greater of:

- $10 million; or
- the value of the benefit obtained from the offence, either directly or indirectly, by the body corporate and any related bodies corporate – three times the value of the benefit.

[Schedule 1, item 1, subsection 56CC(2)]

1.247 If the court cannot determine the value of the benefit obtained as a result of committing the offence then the maximum penalty is the greater of:

- $10 million; or
- 10 per cent of the annual turnover of the body corporate, for the 12 month period ending the month before the offence happened.

[Schedule 1, item 1, subsection 56CC(2)]

1.248 The definition of 'annual turnover' already exists in the CC Act. ***[Schedule 1, item 1, subsection 56CC(3)]***

1.249 Where the offence is committed by a person, other than a body corporate, the offence is punishable by no more than five years imprisonment or a fine not more than $500,000, or both. ***[Schedule 1, item 1, subsection 56CC(4)]***

1.250 The maximum civil penalty for 'holding out' for a body corporate also relies on three possible amounts and leverages the existing civil penalty provision in the CC Act. ***[Schedule 1, item 14, paragraph 76(1A)(b)]***

1.251 The maximum civil penalty for 'holding out' for a person that is not a body corporate is $500,000. ***[Schedule 1, item 16, paragraph 76(1B)(aa)]***

The Accreditation Registrar and Register of Accredited Persons

1.252 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).

1.253 The Registrar must establish and maintain a register of accredited persons and undertake any other functions included in the consumer data rules. ***[Schedule 1, item 1, subsections 56CE(1) and section 56CL]***

1.254 The Registrar is appointed by the Minister and can be an accountable authority of a Commonwealth entity or a Commonwealth entity. An example of an accountable authority would be the Secretary of a Department. The Minister can terminate the appointment at any time. ***[Schedule 1, item 1, section 56CK]***

1.255 If the Minister does not make an appointment, the ACCC is the Registrar. It is the Government's intention that the Registrar will initially be the ACCC. ***[Schedule 1, item 10, subsection 4(1)]***

1.256 The Minister can give binding directions of a general nature to the Registrar about the performance of the Registrar's functions and powers. ***[Schedule 1, item 1, section 56CM]***

1.257 The Registrar may also delegate any of its powers and functions. These delegations are to APS officers or SES officers. Allowing the delegations to be made to lower level ensure functions are appropriately performed by more junior public service staff. Where a power or function is delegated, the delegate must comply with any directions given by the Registrar. ***[Schedule 1, item 1, section 56CN]***

1.258 The ability for the Registrar to delegate any or all of the functions or powers of that role to APS employees not at the SES level is considered necessary. Given the broad nature of the CDR regime requiring an SES level officer to undertake all delegated functions would be burdensome where the tasks would be more appropriately undertaken by a more junior officer. The delegations allow for the best use of resources.

1.259 The Bill provides that each annual report prepared by the Registrar must include information about the performance of the Registrar's functions and exercise of the Registrar's power during that period. The Bill does not require the Registrar to prepare an annual report. Any such requirement is specified by existing laws where appropriate. The Bill simply requires that the annual report include information about the person or entity's role as Registrar. ***[Schedule 1, item 1, subsection 56CL(4)]***

The Register of Accredited Persons

1.260 The Register must be made available in 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. ***[Schedule 1, item 1, subsections 56CE(2) and 56CE(4)]***

1.261 The Register is not a legislative instrument as the Register does not fall within in the definition of legislative instrument in subsection 8(1) of the *Legislation Act 2003*. ***[Schedule 1, item 1, subsection 56CE(3)]***

1.262 The Register is admissible as *prima facie* evidence. That is, where a person has taken the matters contained in the Register as being correct and acted on this basis, the person cannot be taken to be at fault. For example, where a data holder disclosed CDR data to an entity on the basis that the entity was listed in the Register as being an accredited person, the data holder cannot be at fault if the receiving entity was incorrectly listed as being accredited. ***[Schedule 1, item 1, section 56CF]***

Data standards, the Data Standards Chair and the Data Standards Body

Data standards

1.263 Data standards will explain the format and process by which data needs to be provided to consumers and accredited data recipients within the CDR system. Data standards will be made by the Data Standards Chair who is appointed by the Minister by written instrument. ***[Schedule 1, item 1, sections 56FA, 56FF and 56FG]***

1.264 The data standards are not a legislative instrument. 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. ***[Schedule 1, item 1, subsection 56FA(4)]***

1.265 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.

1.266 The Data Standards Chair may make one or more data standards about:

- the format and description of CDR data;
- the disclosure of CDR data;
- the collection, use, accuracy, storage, security and deletion of CDR data;
- de-identifying CDR data; or
- matters included in regulations.

[Schedule 1, item 1, subsection 56FA(1) and 56FB]

1.267 Matters to 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 about the process for making data standards, and when data standards are mandatory or voluntary. A data standard will be binding if the consumer data rules require it. ***[Schedule 1, item 1, subsection 56FA(3)]***

1.268 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 about consultation requirements. If the data standards are inconsistent with the consumer data rules, the rules prevail. ***[Schedule 1, item 1, subsections 56FA(2) and 56FD(3)]***

1.269 The data standards must be published on the internet and be freely available. ***[Schedule 1, item 1, section 56FC]***

Legal effect and enforcement of the data standards

1.270 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 an 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.

1.271 When a data standard is applied by the consumer data rules to a data holder or an accredited person or designated gateway, that standard will operate as a multilateral contract between those participants. This means that a data holder or an accredited person 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 56FD]***

1.272 This contractual obligation applies to data holders, accredited data recipients and designated gateways. ***[Schedule 1, item 1, section 56FD]***

1.273 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 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 56FE]***

1.274 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 56FE(2)]***

Data Standards Chair

1.275 As noted above, data standards are made by the Data Standards Chair who is appointed by the Minister in a written instrument. The length of the Data Standards Chair appointment will be specified in the instrument which appoints the Chair but must not exceed three years. The Data Standards Chair will hold the office on terms and conditions determined by the Minister. ***[Schedule 1, item 1, section 56FG and section 56FM]***

1.276 The Bill gives a number of functions to the Data Standards Chair. Primarily, the functions of the Chair include making data standards consistent with the consumer data rules; reviewing those standards regularly and other functions prescribed in regulations. ***[Schedule , item 1, subsection 56FH(1)]***

1.277 The powers placed on the Data Standards Chair are to establish committees, advisory panels and consultative groups and all other things necessary or convenient to be done in connection with the performance of the functions of the Data Standards Chair. ***[Schedule 1, item 1, subsection 56FH(2)]***

1.278 The Minister may also by legislative instrument give written directions of a general nature to the Data Standards Chair. ***[Schedule 1, item 1, section 56FI]***

1.279 The 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, sections 56FR]***

1.280 The Data Standards Chair may resign from the position by giving the Minister a written resignation. ***[Schedule 1, item 1, section 56FQ]***

1.281 The Bill includes administrative provisions so the office of the Data Standards Chair can function with flexibility including the ability to delegate the Data Standards Chair's powers or functions to staff of the Data Standards Body, the ACCC or in the Department (in this case, the Department of the Treasury). The delegation power does not include the Chair's ability to make data standards. ***[Schedule 1, item 1, section 56FS]***

1.282 The ability for the Data Standards Chair to delegate some of its functions and powers is considered necessary so that the functions and powers of the Chair can be performed in a timely manner. The ability for the delegation to be made to an SES officer or APS employee means that those tasks that would be more appropriately allocated to an APS staff member can be so allocated. However, noting the key role of the Chair to make Data Standards, the Chair is prevented from delegating this power.

1.283 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 56FS(3)]***

1.284 The Minister may also appoint a person to act as the Data Standards Chair during a vacancy of the office or when the Data Standards Chair is absent and unable to perform the duties of the Data Standards Chair. ***[Schedule 1, item 1, section 56FL]***

1.285 The Data Standards Chair is to be remunerated for performing the role, an amount determined by the Remuneration Tribunal or if no amount is determined, the amount set in regulations. ***[Schedule 1, item 1, section 56FN]***

1.286 The Data Standards Chair may be granted leave by the Secretary of the Department on the terms and conditions determined by the Secretary. In this case, the Department refers to the Department of the Treasury. ***[Schedule , item 1, section 56FO]***

1.287 For the purposes of the *Public Governance, Performance and Accountability Act 2013* the Data Standards Chair is an official of the Department. The performance of the Data Standards Chair's functions and powers must be included in the annual report prepared by the Department. In this case, the Department refers to the Department of the Treasury. ***[Schedule , item 1, section 56FP]***

Data Standards Body

1.288 The Minister may also appoint the Department (in this case, the Department of the Treasury) or another Commonwealth entity to perform the functions of the Data Standards Body. ***[Schedule 1, item 1, section 56FJ]***

1.289 The function of the Data Standards Body is to assist the Data Standards Chair. The ACCC may also make rules relating to the governance arrangements of the Data Standards Body or the Body's composition. The Data Standards Body must comply with any rules that have been made by the ACCC. ***[Schedule 1, item 1, section 56FK]***

Dispute Resolution

1.290 As noted above, the consumer data rules may require data holders, accredited data recipients or designated gateways 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, paragraphs 56BJ(g) and 56BJ(h)]***

1.291 Acknowledging that there are a variety of external dispute resolution schemes available within several sectors of the economy, such as Australian Financial Complaints Authority, 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 1988*.

1.292 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. 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.

1.293 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. ***[Schedule 1, item 1, section 56DA]***

1.294 Prior to making an instrument which recognises an external dispute resolution scheme for the CDR, the ACCC will consider a number of factors including how accessible the scheme is as well as the level of independence with which the scheme operates. ***[Schedule 1, item 1, subsection 56DA(3)]***

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

CDR Privacy Framework

1.296 The privacy and confidentiality of CDR data which relates to a CDR consumer is an important element of the CDR regime. The Bill establishes 'Privacy Safeguards' to protect the privacy and confidentiality of CDR data. It is useful to understand how the Privacy Safeguards work in conjunction with the *Privacy Act 1988* and APPs. ***[Schedule 1, item 1, section 56EA]***

1.297 Generally speaking, the *Privacy Act 1988* and the APPs will continue to apply to data holders under the CDR with the exception of accuracy and correction rights and notification of disclosure obligations once a valid request for CDR data has been received. In this instance the Privacy Safeguards apply and the APPs do not. ***[Schedule 1, item 1, paragraphs 56EC(4)(b), 56EC(4)(c) and 56EC(5)(a)]***

1.298 For accredited data recipients, the Privacy Safeguards will substitute the APPs and the APPs will not apply to CDR data that has been received by an accredited data recipient through the CDR regime. ***[Schedule 1, item 1, paragraph 56EC(4)(a)]***

1.299 For a designated gateway, the *Privacy Act 1988* and the APPs will continue to apply with the exception of use and disclosure of the CDR data, including for direct marketing purposes and the security of the CDR data. In this instance the Privacy Safeguards apply and the APPs do not. ***[Schedule 1, item 1, paragraphs 56EC(4)(d) and 56EC(5)(b)]***

1.300 The definitions of CDR data, CDR consumer, data holder, accredited person, accredited data recipient and designated gateway operate to determine when each of the Privacy Safeguards apply and the data that the Privacy Safeguard apply to.

1.301 Part IIIA of the *Privacy Act 1988*, which regulates the credit reporting regime in Australia is not limited by the CDR. However, Regulations may be made which mean that in certain circumstances the

CDR will operate as if parts of the credit reporting regime did not apply. ***[Schedule 1, item 1, subsection 56EC(3); and Schedule 1, item s 57, 59, 60, 61, subsection 6(1), paragraphs 20E(2)(b) and (3)(e), 21G(2)(d) and (3)(f) and 22E(2)(b) and (3)(b) of the Privacy Act 1988]***

1.302 Currently, Part IIIA of the *Privacy Act 1988* allows a credit reporting body, credit provider or another person such as a credit manager to use or disclose certain information if the use or disclosure is allowed under another Australian law despite that information normally being subject to restrictions under the credit reporting regime. The Bill amends the *Privacy Act 1988* to exclude the consumer data rules as an Australian law that would permit the use or disclosure of this information. The CDR cannot override the restrictions in the credit reporting regime. ***[Schedule 1, items 79, 80, 81, paragraphs 20E(2)(b) and (3)(e), 21G(2)(d) and (3)(f), and 22E(2)(b) and (3)(b) of the Privacy Act 1988]***

Application of Privacy Safeguards by CDR participant

CDR Participant	*Which Privacy Safeguard (PS) apply?*
Data holder	PS 1 – applies concurrently to APP 1 PS 10 – applies to the disclosure of CDR data and there is no similar requirement under the *Privacy Act 1988*. PS 11, PS 13 – apply to the disclosure of CDR data and substitute for APPs 10 and 13 for disclosed CDR data.
Accredited person	PS 1, PS 3, PS 4, PS 5 – the APPs apply concurrently, but with the more specific Privacy Safeguards prevailing.
Accredited data recipient	PS 1, PS 2, PS 6, PS 7, PS 8, PS 9, PS 10, PS 11, PS 12 and PS 13 – apply and substitute the APPs which do not apply to an accredited data recipient for CDR data that has been received under the CDR rules or is derived from that data.
Designated gateway	PS 1 – applies concurrently to APP 1. PS 6, PS 7 and PS 12 – apply to the use and disclosure of CDR data under the CDR rules and substitute for APPs 6, 7 and 11.

Example 1.17

Max is a consumer with AllenBank. All of his transaction information held by AllenBank is treated consistently with the *Privacy Act 1988* and APPs by AllenBank.

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

At the time of receiving Max's CDR data, HIZAI Banking Services is required to handle the data in accordance with the CDR Privacy

Safeguards because HIZAI Banking Services is an accredited data recipient for Max's data.

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

All new data created by HIZAI Banking Services about Max's savings account is subject to the *Privacy Act 1988* and the APPs.

The consumer data rules may enable HIZAI Banking Services to manage Max's historical banking data as a data holder rather than as an accredited data recipient. If this was the case the historical data would be subject to the APPs. See *Case 3: Receiving data holder* in the definition of data holder (paragraphs 1.86 to 1.88).

Example 1.18

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

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

1.303 Unlike the APPs, the Privacy Safeguards will also apply to CDR data where the CDR consumer is a business. Broadly, the APPs apply to natural persons. ***[Schedule 1, item 1, section 56EB]***

1.304 The *Privacy Act 1988* 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.

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

1.306 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. It is intended that the term 'de-identification' be interpreted by reference to this threshold.

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

Consideration of CDR data privacy

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

1.308 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.

1.309 To assist in this, all data holders, accredited data recipients and designated gateways, must have policy, procedures and systems in place that ensure compliance with the CDR regime and management of CDR data. ***[Schedule 1, item 1, subsection 56ED]***

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

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

[Schedule 1, item 1, subsection 56ED(4)]

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

- the kinds of CDR data held by the accredited data recipient and how that data is held;
- the purposes for collecting, holding, using and disclosing the CDR data with the consent of the consumer;
- 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 an accredited data recipient to comply with the CDR regime;
- how the accredited data recipient will address such a complaint;

- if the accredited data recipient is likely to disclose CDR data to an overseas accredited data entity, information about the country in which that entity is based;
- the circumstances when the accredited data recipient will disclose the data to a person that does not hold an accreditation;
- the events that the CDR consumer will be notified about; and
- the circumstances when the accredited data recipient must destroy or de-identify CDR information at the request of the consumer.

[Schedule 1, item 1, section 56ED(5)]

1.312 For a designated gateway, the policy about the management of CDR data must contain an explanation of how the entity will act between other participants in the CDR to facilitate the disclosure of the CDR data, accuracy of the CDR data or other matters included in the consumer data rules. The policy must also include how a CDR consumer can complain about the failure of designated gateway to comply with the CDR regime. ***[Schedule 1, item 1, subsection 56ED(6)]***

1.313 The 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.

1.314 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(7)(a)]***

1.315 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(8)]***

CDR Privacy Safeguard 2 – Anonymity and pseudonymity

1.316 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(3)]***

1.317 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. Similar to how APP 2 operates under the *Privacy Act 1988*, it is possible for a CDR consumer to interact anonymously or pseudonymously

with a CDR participant and yet still be reasonably identifiable from the circumstances.

1.318 Unless the consumer data rules specify instances where an accredited data recipient is unable to provide a CDR consumer with the ability to use a pseudonym, a pseudonym is permitted. The option may be given through a designated gateway. ***[Schedule 1, item 1, subsections 56EE(1) and 56EE(2)]***

1.319 The Government would not expect that a consumer could use a pseudonym when exercising their consumer data right in the banking sector. A consumer cannot typically engage with the banking sector without identifying themselves.

1.320 Privacy Safeguard 2 does not apply to data holders or a designated gateway. As applicable, the *Privacy Act 1988* and APPs will apply to data holders.

Collecting CDR data

CDR Privacy Safeguard 3 – Collecting solicited CDR data

1.321 An accredited person must only seek to collect CDR data in accordance with the CDR regime if the CDR consumer has given a valid request for the accredited person to collect the data under the consumer data rules. The collection of the data could be made directly from another CDR participant or via a designated gateway. ***[Schedule 1, item 1, section 56EF]***

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

1.323 An accredited person who contravenes Privacy Safeguard 3 may be subject to a civil penalty. See paragraphs 1.437 to 1.449.

CDR Privacy Safeguard 4 – Dealing with unsolicited CDR data

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

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

1.326 Privacy Safeguard 4 makes clear that an accredited person will not be able to retain unsolicited CDR data, except if required to do so under an Australian law or by order of a court or tribunal. This holds whether or not the accredited data recipient collected the data via a

designated gateway or directly from a data holder. ***[Schedule 1, item 1, subsection 56EG(2)]***

1.327 An accredited person who contravenes Privacy Safeguard 4 may be subject to a civil penalty. See paragraphs 1.437to 1.449.

CDR Privacy Safeguard 5 – Notifying the collection of CDR data

1.328 If an accredited person collects data in accordance with Privacy Safeguard 3, then the accredited person must comply with the consumer data rules relating to advising the CDR consumer about the collection of their data. ***[Schedule 1, item 1, section 56EH]***

1.329 This notice must also be given to the CDR consumers specified in the consumer data rules relating to Privacy Safeguard 5 notices. ***[Schedule 1, item 1, paragraph 56EH(b)]***

1.330 Failing to notify the CDR consumer under Privacy Safeguard 5 may give rise to a civil penalty. See paragraphs 1.437 to 1.449.

Dealing with CDR data

CDR Privacy Safeguard 6 – Use or disclosure of CDR data

Accredited data recipients

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

1.332 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.

1.333 An accredited data recipient must not use or disclose CDR data unless it is consistent with a requirement or authorisation under the consumer data rules. ***[Schedule 1, item 1, paragraph 56EI(1)(b)]***

1.334 An example of where the consumer data rules may authorise a use or disclosure without the consent of the consumer would be to third party as part of a data storage arrangement.

1.335 A use or disclosure will be allowed without the consumer's consent under the consumer data rules where it is required or permitted by an Australian law or an order of a court or tribunal. The APPs are not an Australian law for the purposes of this Privacy Safeguard. ***[Schedule 1, item 1, paragraph 56EI(1)(c)]***

1.336 The accredited data recipient must make a written note where it uses or discloses the CDR data under an Australian law or an order of a court or tribunal.

1.337 An accredited data recipient may be subject to a civil penalty if it uses or discloses CDR data in a way that is not permitted under Privacy Safeguard 6. See paragraphs 1.437 to 1.449.

Designated gateway

1.338 A designated gateway must not use CDR data unless the use is authorised by the consumer data rules, or is required or authorised by another Australian law (except the APPs) or a court or tribunal. ***[Schedule 1, item 1, subsection 56EI(2)]***

1.339 A designated gateway must not disclose CDR data unless the consumer data rules require or authorise the disclosure. ***[Schedule 1, item 1, subsection 56EI(2)]***

1.340 An Australian law, other than the consumer data rules or the APPs, may also authorise or require a designated gateway to disclose CDR data, as can an order of a court or tribunal. ***[Schedule 1, item 1, paragraph 56EI(2)(c)]***

1.341 The designated gateway must make a written note, in accordance with the consumer data rules, where it uses or discloses the CDR data under an Australian law or an order of a court or tribunal. ***[Schedule 1, item 1, paragraph 56EI(2)(c)]***

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

1.342 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 is not permitted unless authorised or required by the consumer data rules and specifically consented to by the CDR consumer. ***[Schedule 1, item 1, section 56EJ]***

1.343 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.

1.344 A civil penalty may apply if an accredited entity or designated gateway uses or discloses CDR data for direct marketing purposes where it is not permitted. See paragraphs 1.437to 1.449.

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

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

1.346 The Bill limits the disclosure of CDR data by accredited data recipients to overseas entities except in some limited circumstances. ***[Schedule 1, item 1, paragraphs 56EK(1)(a) and 56EK(1)(b)]***

1.347 One circumstance where disclosure of CDR data to an offshore entity is permitted, is if the entity is an accredited data recipient. ***[Schedule 1, item 1, paragraph 56EK(1)(c)]***

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

1.349 An accredited data recipient may also disclose information to an overseas recipient which is not an accredited entity if:

- the accredited data recipient takes reasonable steps to ensure the recipient does not breach the relevant Privacy Safeguards; or
- the accredited data recipient believes that the recipient is subject to a law or scheme that provides at least the equivalent protections as the Privacy Safeguards and the CDR consumer will be able to enforce those protections.

[Schedule 1, item 1, paragraphs 56EK(1)(d) and 56EK(1)(e)]

1.350 The consumer data rules may also provide that a cross-border disclosure is authorised for CDR data where conditions specified in the consumer data rules are met. It is the Government's expectation that these conditions would be similar to those included in Privacy Safeguard 8, adjusted for business consumers. ***[Schedule 1, item 1, paragraph 56EK(1)(f)]***

1.351 If the receiving entity breaches the Privacy Safeguards after the accredited data recipient took reasonable steps to make sure that it would not, the accredited data recipient is taken to have breached the Privacy Safeguards and may be subject to a civil penalty. ***[Schedule 1, item 1, subsections 56EK(2) and 56EK(3)]***

1.352 An accredited data recipient may be subject to a civil penalty for a contravention of Privacy Safeguard 8. See paragraphs 1.437 to 1.449.

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

1.353 As the CDR system develops, it is possible that CDR consumers who are individuals may have CDR data sets that contain government related identifiers, as defined in the *Privacy Act 1988*. This could include a tax file number.

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

1.355 The exception is where the use is allowed under an Australian law (other than the consumer data rules), or an order of a court or tribunal or subclause 9.3 of APP 9 applies. ***[Schedule 1, item 1, paragraphs 56EL(1)(c) and 56EL(1)(d)]***

1.356 Similarly, it is not permissible for an accredited data recipient to disclose CDR data about an individual containing a government related identifier. The only exception to this is if the disclosure is permitted by an Australian law (except the consumer data rules), or by an order of a court or tribunal or subclause 9.3 of APP 9 applies. ***[Schedule 1, item 1, subsection 56EL(2)]***

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

1.358 An accredited data recipient may be subject to a civil penalty for a contravention of Privacy Safeguard 9. See paragraphs 1.437 to 1.449.

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

1.359 Unlike the other Privacy Safeguards discussed to this point (with the exception of Privacy Safeguard 1), Privacy Safeguard 10 applies to a data holder as well as an accredited data recipient.

1.360 Where a data holder has disclosed CDR data consistent with the consumer data rules the data holder must notify the consumer as required by the consumer data rules. ***[Schedule 1, item 1, subsection 56EM(1)]***

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

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

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

1.364 The obligation to notify the consumer applies even if the disclosure was made via a designated gateway. ***[Schedule 1, item 1, subsection 56EM(3)]***

1.365 An accredited data recipient or data holder who fails to notify the consumer in accordance with Privacy Safeguard 10 may be subject to a civil penalty. See paragraphs 1.437 to 1.449.

Integrity of CDR data

CDR Privacy Safeguard 11 – Quality of CDR data

1.366 Privacy Safeguard 11 also applies to data holders. Where a data holder discloses CDR data as required or authorised by the consumer data rules, the data holder must ensure that the CDR data is accurate, up to date and complete for the purpose for which it is held. APP 10 (Quality of Personal Information) does not apply to a data holder who is subject to Privacy Safeguard 11. ***[Schedule 1, item 1, paragraph 56EC(4)(b) and subsection 56EN(1)]***

1.367 The CDR data is not held for the purpose of being required to be disclosed under the consumer data rules. For example, a data holder that is an ADI collects transaction data for the purpose of providing a banking service to its customer. It does not hold transaction data for the purpose of being required disclose the data under the CDR regime. ***[Schedule 1, item 1, subsection 56EN(5)]***

1.368 Similarly, an accredited data recipient must ensure that the data it discloses as required or authorised by the consumer data rules is accurate, up to date and complete for the purpose for which it is held. It is not held for the purpose of disclosing the CDR data under the consumer data rules. ***[Schedule 1, item 1, subsections 56EN(2) and 56EN(5)]***

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

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

Example 1.19

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

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

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

1.371 A civil penalty may apply where a data holder or accredited data recipient fails to comply with a requirement to:

- take reasonable steps to keep data accurate, up to date and complete;
- notify the consumer where the data holder or accredited recipient becomes aware that the data that was disclosed was not accurate, up to date or complete; or
- respond to a request from the consumer to disclose the subsequently corrected data. See paragraphs 1.437 to 1.449.

CDR Privacy Safeguard 12 – Security of CDR data

1.372 An integral element of the CDR system is the protection of consumers' CDR data. As such, Privacy Safeguard 12 places a requirement on accredited data recipients and designated gateways, 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 56EO(1)]***

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

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

Example 1.20

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

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

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

The four other banks, who received Nick's credit card information are required by the consumer data rules to 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 1.21

Following on from the example 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.

1.375 Failure to comply with Privacy Safeguard 12 may result in the accredited data recipient or designated gateway being subject to a civil penalty. See paragraphs 1.437 to 1.449.

Correction of CDR data

CDR Privacy Safeguard 13 – Correction of CDR data

1.376 A CDR consumer has correction rights for CDR data that has been disclosed by a data holder in response to a valid request from that consumer. APP 13 (Correction of Personal Information) does not apply to a data holder who is subject to Privacy Safeguard 13. ***[Schedule 1, item 1, subsection 56EP(1)]***

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

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

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

1.380 The purpose for which the data is held does not include the data being required to be disclosed under the consumer data rules. ***[Schedule 1, item 1, subsection 56EP(4)]***

1.381 Failure to correct the CDR data or otherwise comply with Privacy Safeguard 13 may mean the data holder or accredited data recipient is subject to a civil penalty. See paragraphs 1.437 to 1.449.

Regulation of the CDR system by the ACCC and the OAIC

1.382 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 AIC Act.

1.383 The Information Commissioner has any powers given to him or her under the CDR regime or legislative instruments made under the CDR and is responsible for advising the Minister, ACCC or Data Standards Chair about matters relevant to the CDR. ***[Schedule 1, item 1, section 56GA]***

1.384 The AIC Act is amended to ensure that the OAIC and the Information Commissioner's privacy functions (as defined by the AIC Act) extend to the CDR regime established in the CC Act. This ensures that the regulatory framework supporting its privacy functions may be applied to its CDR functions. ***[Schedule 1, items 4, 5, 6 and 7, sections 3 and 4, subsection 9(1) and paragraph 29(2)(a) of the AIC Act 2010]***

1.385 The Bill also extends the ACCC's existing information gathering powers. Section 155 of the CC Act is extended to apply to contraventions of the CDR regime 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 the CDR regime (except the Privacy Safeguards) including the consumer data rules. ***[Schedule 1, items 63, 64 and 65 , paragraph 155(2)(a), subparagraph 155(2)(b)(i), and subsection 155(9)]***

1.386 The extension of the ACCC's existing information gathering powers in 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 powers will allow the ACCC to determine which data sets exist in new sectors by requesting this information.

1.387 The ACCC will undertake a significant new role of accrediting data recipients for the CDR. The extension of the ACCC's powers to obtain information, documents and evidence allows the ACCC to 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.

1.388 Finally, the extension of the information gathering powers to the ACCC's CDR functions will help ensure that the CDR regime 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.

1.389 The Bill amends the CC Act so that the ACCC can delegate certain enforcement powers, infringement notice provisions or information gathering powers (such as the ones described above) to the extent that the powers or functions are about the CDR regime including the consumer data rules. ***[Schedule 1, items 14 and 15, subsection 26(1) and section 26]***

1.390 The ACCC may delegate these powers or functions to the Information Commissioner or a member of staff at the OAIC if the Information Commissioner agrees to the delegation in writing and the staff member is of sufficient seniority. ***[Schedule 1, item 15, section 26]***

1.391 The amendments to existing section 155 mean that the ACCC, the Information Commissioner and the OAIC may, should a delegation be in place under section 26 of the CC Act, use this power in order to obtain information and documents both in relation to a breach of the CDR regime or the consumer data rules or possible breach of the CDR regime or the rules, or in their performance of a function or power under the CDR regime (except as regards the Privacy Safeguards).

1.392 The dual regulatory model provided for by the CDR enables the Information Commissioner to delegate his or her privacy safeguard enforcement powers or functions to the ACCC or a member of staff of the ACCC. ***[Schedule 1, item 1, section 56EZ]***

1.393 Further, the CC Act is amended so that the ACCC can disclose information to the Information Commissioner or a member of staff of the OAIC or to a foreign agency that undertakes a similar regulatory role for CDR data. ***[Schedule 1, items 68 and 69, section 157A]***

1.394 Where the information is disclosed to the Information Commissioner or a member of staff of the OAIC, the information may only be used for the purpose of the CDR and the functions and powers given to the Information Commissioner as part of the CDR regime. ***[Schedule 1, item 69, section 157A]***

1.395 Protections may apply to information shared with foreign agencies by way of conditions imposed by the ACCC. ***[Schedule 1, item 69, section 157A]***

Compliance with the consumer data right (other than the privacy safeguards) and the consumer data rules

1.396 Setting the right penalties is integral to the CDR regime. It is important that the penalties act as a deterrent and are not seen as a cost of doing business. The enforcement and remedy regime which will apply under the CDR is consistent with the existing regime in the CC Act. This

approach allows Courts the flexibility to deal with large and small business and serious and minor contraventions.

1.397 Misuse of CDR data has the potential to cause significant harm to consumers and affect confidence in the entire system. The CDR will inherently have a greater volume and velocity of data flows than transfers under the *Privacy Act 1988*, meaning that breaches may affect the data of a larger number of consumers. Strong penalties will discourage misuse of CDR data and prevent this misuse from being seen as a cost of doing business.

1.398 The Bill prohibits conduct which misleads a person to believe that a person is a CDR consumer or is acting in accordance with a valid request or consent from a CDR consumer when in fact they are not. ***[Schedule 1, item 1, sections 56BN and 56BO]***

Example 1.22

Julie makes a request to Elec Watch, an accredited data recipient, for Elec Watch to collect Julie's CDR energy data. Elec Watch screen scrapes Julie's energy provider's online portal, instead of sending a disclosure request in accordance with the CDR rules. Julie thinks she has made a request as a CDR consumer, but she has not.

Elec Watch should have told Julie that the request she was making was not being processed as a CDR request.

1.399 Where the offence is committed by a body corporate, the offence is punishable by a fine of not greater than three possible amounts taking into account the benefit gained from committing the offence and the size of the business, based on the body corporate's annual turnover. ***[Schedule 1, item 1, subsection 56BN(3)]***

1.400 If the court can determine the value of the benefit obtained from the offence then the maximum penalty is the greater of:

- $10 million; or
- the value of the benefit obtained from the offence, either directly or indirectly, by the body corporate and any related bodies corporate – three times the value of the benefit.

[Schedule 1, item 1, subsection 56BN(3)]

1.401 If the court cannot determine the value of the benefit obtained as a result of committing the offence then the maximum penalty is the greater of:

- $10 million; or
- 10 per cent of the annual turnover of the body corporate, for the 12 month period ending the month before the offence happened.

[Schedule 1, item 1, subsection 56BN(3)]

1.402 Annual turnover has the meaning given in Division 1 of Part IV of the CC Act. ***[Schedule 1, item 1, subsection 56BN(4)]***

1.403 Where the offence is committed by a person, other than a body corporate, the offence is punishable by no more than five years imprisonment or a fine not more than $500,000, or both. ***[Schedule 1, item 1, subsection 56BN(5)]***

1.404 A person may be subject to a civil penalty if they engage in conduct that is misleading or deceptive. ***[Schedule 1, items 1, 16, 17, 18, 20, section 56BO, subsection 75B(1), subparagraph76(1)(a)(ia), paragraphs76(1A)(b) and 76(1B)(aa)]***

1.405 For both an offence penalty or contravention of the civil penalty about conduct that is misleading or deceptive, the provision does not apply if the conduct is not misleading or deceptive in a material particular. However, a person who wishes to rely on this defence bears the burden of adducing or pointing to evidence. This is appropriate as this 'evidence' would most likely be known to the person. ***[Schedule 1, item 1, subsections 56BN(2), 56BO(2) and 56BO(3)]***

1.406 The Bill extends existing enforcement and remedy provisions and associated powers of the ACCC, to the CDR regime:

- 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 the consumer data right and the consumer data rules ***[Schedule 1, items 1, 16, 17, 18, 19, 20, 21 sections 56BO, 56BT and 56CD, subsection 75B(1), subparagraph 76(1)(a)(ia), paragraphs 76(1A)(b), 76(1A)(ca), 76(1B)(aa) and 76(1B)(aaa)];***
- Section 80 – provides that a person, including the ACCC may apply to the court for an injunction where another person is undertaking, or proposing to undertake conduct which would contravene parts of the CC Act. This provision has been extended to apply to contraventions of the consumer data right and the consumer data rules. As is currently the case, when seeking an injunction for the contravention of a criminal offence, the person seeking the injunction does not

need to make an undertaking about damages ***[Schedule 1, items 28 and 29, subparagraph 80(1)(a)(iia) and paragraphs 80(9)(a) and (b)]***;

- 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 the CDR regime or the consumer data rules is able to recover the amount of the damage or loss sustained ***[Schedule 1, item 30, subsection 82(1)]***;
- Section 83 – allows a finding of fact established in earlier proceedings to be used in proceedings by private litigants. This is extended to include where direct action is taken as a result of a breach or contravention of the CDR. ***[Schedule 1, items 31 and 32, subparagraph 83(1)(a)(ii) and paragraph 83(1)(b)]***
- Section 84 – provides that the conduct of a director, employee or someone acting on behalf of a body corporate establishes the 'state of mind' of the body corporate for civil or criminal offences. This is extended to the CDR and consumer data rules ***[Schedule 1, items 33, 34, 35, 36, 37, and 38, paragraphs 84(1)(a) and 84(1)(b), subsection 84(2), paragraphs 84(3)(a) and 84(3)(b), and subsection 84(4)]***
- Section 86C – non-punitive orders are extended to enable the ACCC to seek application of a non-punitive order for a breach of the consumer data rules or the consumer data right ***[Schedule 1, item 42, subsection 86C(4)]***;
- Section 86D – adverse publicity order may also be made by a court where a person has been found in contravention of an offence provision of the consumer data right ***[Schedule 1, items 43 and 44, paragraph 86D(1)(b) and subsection 86D(1A)]***;
- Section 86E – the ability to apply for an order disqualifying a person from managing corporations is extended to contraventions of the consumer data right or the consumer data rules ***[Schedule 1, items 45 and 46, paragraphs 86E(1)(a) and 86E(1A)(a)]***;
- Section 86F – this provision provides that a person is not able to refuse to comply with the CC Act on the basis that it might expose the person to a penalty or order under section 86E. It automatically applies to the CDR but to ensure there is no doubt it is amended to refer to the consumer data rules. ***[Schedule 1, items 47 and 48, subsections 86F(1) and 86F(3)]***
- Section 87 – this provision provides the ability to seek application of other orders. It is extended to contraventions of the consumer data right and consumer data rules ***[Schedule 1, items 49, 50, 51, 52, 53, 54, 55, 56, 57 and 58, subsection 87(1),***

paragraphs 87(1A)(a) and (b), paragraphs 87(1A)(baa), 87(1A)(ba) and 87(1B)(a), subsection 87(1BAA), paragraph 87(1BA)(a) and subsection 87(1C)];

- Section 87B – gives the ACCC the ability to accept written undertakings and automatically applies to the CDR. The provision is extended to make clear the ACCC can also accept written undertakings about consumer data rules. ***[Schedule 1, item 59, subsection 87B(1)]***
- Division 5 of Part XI about infringement notices is also extended to civil penalties under the CDR regime and consumer data rules in a corresponding way to how Division 5 of Part XI applies to Part 2-2 of the Australian Consumer Law ***[Schedule 1, item 1, section 56BM]***;
- Part XID – gives the ACCC search and seizure powers to discover whether there has been a contravention of the CC Act. It automatically applies to the CDR but to ensure there is no doubt, it is amended to refer to the consumer data rules. ***[Schedule 1, items 60, 61 and 62, sections 154 and 154A, and paragraph 154V(2)(a)]***

1.407 The consumer data rules may specify that a civil penalty applies to breaches of the rules. Where a civil penalty does apply to a breach of the rules the rules may also specify a lower penalty amount than the default maximum. If the rules do not specify an amount, then the maximum civil penalty is as per the amount worked out under section 76 of the CC Act. ***[Schedule 1, items 1, 16, 17, 18, 19, 20, 21 section 56BL, subsection 75B(1), subparagraph76(1)(a)(ia), paragraphs 76(1A)(b), 76(1A)(ca), 76(1B)(aa) and 76(1B)(aaa)]***

1.408 This is considered necessary because the consumer data rules are a key mechanism through which consumers and their data are protected (in conjunction with the Privacy Safeguards). 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.

1.409 High penalties reflect the importance of consumer data rules (together with the Privacy Safeguards) to the core protections for consumers and their data. It is through the rules that the ACCC will be able to enforce the data standards that are a fundamental element of those protections. Significant penalties recognise the potential damage where contraventions expose sensitive personal data and provide flexibility as other sectors are brought within the regime and the potential to include derived or value-added data.

1.410 It is also appropriate for the high maximum penalties to apply equally to small business and large multi-nationals. The application of such penalties has been successfully managed by the ACCC and the Courts for other contraventions and has not had the effect of deterring

normal business conduct. It would align with the introduction of higher penalties under the Australian Consumer Law.

1.411 The CC Act allows the ACCC the discretion to determine the appropriate enforcement tool to apply to small businesses and multi-nationals who may have engaged in misconduct. In selecting the appropriate enforcement tool, the ACCC considers a range of factors including: the size of the business, the capacity of the business to benefit from the misconduct, and the sophistication of the business' compliance strategies. If the ACCC successfully litigates against a business, the Court decides the appropriate penalty amount up to the maximum. The Court considers similar factors including:

- the nature and extent of the contravening conduct;
- the amount of loss or damage caused;
- the circumstances in which the conduct took place;
- the size of the contravening company;
- the degree of power it has, as evidenced by its market share and ease of entry into the market;
- the deliberateness of the contravention and the period over which it extended;
- whether the contravention arose out of the conduct of senior management or at a lower level;
- whether the company has a corporate culture conducive to compliance with the CC Act, as evidenced by educational programs and disciplinary or other corrective measures in response to an acknowledged contravention; and
- whether the company has shown a disposition to co-operate with the authorities responsible for the enforcement of the CC Act in relation to the contravention.

1.412 It is appropriate that the court retain the discretion to impose a penalty that is appropriate in the particular circumstances. Those circumstances will cover a broad range of conduct and may vary significantly across different sectors. It is expected that the maximum penalty would be imposed in the most serious of circumstances, and not in circumstances involving, for example, honest mistakes.

1.413 Existing section 76B of the CC Act prevents a Court from making a pecuniary penalty order against a person if the person has already been convicted of an offence for substantially the same conduct. This provision is amended to incorporate the new criminal and civil penalty provisions introduced for the CDR. That is, the misleading and

deceptive conduct or holding out. ***[Schedule 1, items 22, 23 and 24, section 76B, subsections 76B(2), (3) and (4) and paragraph 76B(5)(a)]***

1.414 Provisions about the enforcement and recovery of certain fines are amended to incorporate references to CDR offence provisions. As are provisions which preference compensation for victims over paying pecuniary penalties or fines. ***[Schedule 1, items 25, 26 and 27, subparagraphs 79A(1)(a)(i) and 79B(a)(ii) and paragraph 79B(a)]***

1.415 Jurisdiction of the CDR and consumer data rules is given to the Federal Court; jurisdiction is given to the Federal Circuit Court for civil proceedings instituted by a person other than the Minister; and jurisdiction is given to courts of the States or Territories where the civil proceeding is instituted by a person other than the Minister or ACCC. ***[Schedule 1, items 39 and 40, subsection 86(1) and subsections 86(1A) and (2)]***

1.416 A civil proceeding about the CDR or consumer data rules instituted by a person other than the Minister or ACCC which is pending in the Federal Court may be transferred to a court of the State or Territory. ***[Schedule 1, item 41, paragraph 86A(1)(b)]***

1.417 A number of consequential amendments are required to incorporate the CDR offence and civil penalty provisions and references to the consumer data rules into existing provisions of the CC Act. These include to which court a prosecution can be brought; instituting a proceeding seeking a court to make a declaration; and when the ACCC may institute proceedings. ***[Schedule 1, items 70, 71, 72, 73, 74, 75 and 76, paragraph 163(2)(a), subsections 163A(1) and 163A(3), paragraph 163A(4)(a), subsection 163A(4B), paragraph 163A(4C)(a) and subsection 163A(4D)]***

Compliance with the Privacy Safeguards

Guidance and education programs

1.418 The Bill amends the CC Act to provide that the Information Commissioner shall promote compliance with the privacy safeguards. In order for the Information Commissioner to undertake this role the AIC Act is amended to extend the Commissioner's functions to include those under the CDR Regime.

1.419 The Information Commissioner is empowered to make guidelines outlining the sorts of acts or practices that could result in breach of the privacy safeguards. ***[Schedule 1, item 1, paragraph 56EQ(1)(a)]***

1.420 Acknowledging the shared regulation of the CDR regime, the Information Commissioner must consult with the ACCC prior to making the proposed guidelines. ***[Schedule 1, item 1, subsection 56EQ(2)]***

1.421 To the extent of any inconsistencies that may arise between the privacy safeguard guidelines 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 56EQ(4)]***

1.422 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 56EQ(3)]***

1.423 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 56EQ(5)]***

1.424 The Information Commissioner also has a role promoting an understanding of the Privacy Safeguards. ***[Schedule 1, item 1, paragraph 56EQ(1)(b)]***

1.425 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 56EQ(1)(c) and subsection 56EQ(6)]***

Assessments of management and handling of CDR data

1.426 Under the *Privacy Act 1988*, the Information Commissioner is provided with the ability to conduct an assessment relating to compliance with the APPs and to provide a report to the Minister; in that case the Attorney-General (see sections 32 and 33C of the *Privacy Act 1988*).

1.427 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, item 1, section 56ER]***

1.428 Once the Information Commissioner has conducted an assessment, he or she may provide a report 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 56ER(3)]***

Notifications of CDR data security breaches

1.429 The *Privacy Act 1988* 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 1988*.

1.430 CDR is subject to Part IIIC of the *Privacy Act 1988* in respect of accredited data recipients and designated gateways and their handling of CDR data. As such, accredited data recipients and designated gateways are required to notify the Information Commissioner about CDR data security breaches. ***[Schedule 1, item 1, section 56ES]***

1.431 In addition, Part V of the *Privacy Act 1988* 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 1988* regarding the management and handling of consumers' CDR data. ***[Schedule 1, item 1, section 56ET]***

Enforceable civil penalty provisions, undertakings and injunctions

1.432 The Bill triggers a number of the provisions in the Regulatory Powers Act to establish an enforcement and remedy framework for the Privacy Safeguards.

1.433 These powers apply to the civil penalty provisions for the Privacy Safeguards and enable the Information Commissioner to accept enforceable undertakings and seek injunctions to ensure compliance with the Privacy Safeguards.

1.434 The Information Commissioner has similar powers under the *Privacy Act 1988* when enforcing the APPs.

1.435 The *Privacy Act 1988* allows:

- the Information Commissioner to accept a written undertaking from an entity that the entity will take specific action (or refrain from a specific action) in order to comply with the APPs and seek an order from a court if the entity has breached the undertaking.
- the Federal Court or Federal Circuit Court to grant an injunction in response to an application from the Information Commissioner which would restrain a person from certain conduct that contravene the *Privacy Act 1988*; and
- the Information Commissioner to seek a civil penalty for contraventions of the *Privacy Act 1988*.

1.436 Therefore, applying the Regulatory Powers Act for the Privacy Safeguards is consistent with the Information Commissioner's current regulatory powers.

Civil penalties

1.437 As noted above, certain Privacy Safeguards are civil penalty provisions which are enforceable under the Regulatory Powers Act. ***[Schedule 1, item 1, section 56EU]***

1.438 Aligning the civil penalties for the CDR Privacy Safeguards with the civil penalties that apply to other breaches of the CDR Regime reflects the enhanced level of protection which the Privacy Safeguards look to provide and the central role of the CDR Privacy Safeguards to the regime. Many of the Privacy Safeguards require compliance with the

consumer data rules or work in conjunction with those rules and so it is appropriate that the penalties which may be imposed are consistent.

1.439 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. ***[Schedule 1, item 1, subsection 56EU(3)]***

1.440 For the purposes of Part 4 of the Regulatory Powers Act, applications may be made about a Privacy Safeguard penalty provision to the Federal Court or the court of a State or Territory with jurisdiction in relation to the matter. ***[Schedule 1, item 1, subsection 56EU(4)]***

1.441 Proceedings may be taken against a person where the conduct breaches both one or more Privacy Safeguard penalty provisions and one or more civil penalty provisions in the consumer data rules. ***[Schedule 1, item 1, subsection 56EU(5)]***

1.442 In the event that the actions of a data holder, accredited data recipient or designated gateway contravene both a consumer data rule which contains a civil penalty as well as a Privacy Safeguard provision containing a civil penalty, a person can only be liable for one pecuniary penalty under Part 4 of the Regulatory Powers Act and Part VI of the CC Act for the same conduct. ***[Schedule 1, item 1, subsection 56EU(6)]***

1.443 It is not the intention that CDR participants be penalised twice for the same behaviour. While this is unlikely to materialise in practice, the Bill clarifies that penalties can only be applied once in relation to conduct resulting in a breach.

1.444 The amount of the pecuniary penalty is worked out in accordance with the Bill, not the Regulatory Powers Act. ***[Schedule 1, item 1, subsection 56EV(1)]***

1.445 The maximum civil penalty for a contravention of the Privacy Safeguards by a body corporate relies on three possible amounts.

1.446 If the court can determine the value of the benefit obtained from a contravention of the Privacy Safeguards then the maximum penalty is the greater of:

- $10 million; or
- the value of the benefit obtained from the contravention, either directly or indirectly, by the body corporate and any related bodies corporate – three times the value of the benefit.

[Schedule 1, item 1, subsection 56EV(2)]

1.447 If the court cannot determine the value of the benefit obtained from a contravention of the Privacy Safeguards then the maximum penalty is the greater of:

- $10 million; or
- 10 per cent of the annual turnover of the body corporate, for the 12 month period ending the month before the breach happened.

[Schedule 1, item 1, subsection 56EV(2)]

1.448 The definition of annual turnover relies on the existing definition in Division 1 of Part IV of the CC Act. ***[Schedule 1, item 1, subsection 56EV(3)]***

1.449 The maximum civil penalty for a contravention of the privacy safeguards for a person that is not a body corporate is $500,000. ***[Schedule 1, item 1, subsection 56EV(4)]***

Enforceable undertakings

1.450 Part 6 of the Regulatory Powers Act is applied so that each of the Privacy Safeguards is able to be enforced by accepting and enforcing undertakings to comply with those provisions. ***[Schedule 1, item 1, subsection 56EW(1)]***

1.451 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 56EW(2)]***

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

Injunctions

1.453 The Information Commissioner is provided with similar powers for the enforcement of the Privacy Safeguards via injunctions.

1.454 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 56EX]***

1.455 The Information Commissioner may apply for an injunction in the Federal Court or a court of a state or territory with jurisdiction to hear the matter. ***[Schedule 1, item 1, subsection 56EX(3)]***

1.456 These powers mean that the Information Commissioner may use discretion in the circumstances and seek an enforceable undertaking or injunction that is not a pecuniary penalty to address misconduct. Similarly, when considering what pecuniary penalty is appropriate, the

court may exercise discretion. It is expected that the maximum penalty would be imposed in the most serious of circumstances, and not in circumstances involving honest mistakes.

Delegation to the Commission

1.457 Acknowledging the dual regulator model provided for the CDR, the Information Commissioner is able to delegate his or her Privacy Safeguard enforcement powers or functions to the ACCC. ***[Schedule 1, item 1, subsection 56EZ(2)]***

1.458 These Privacy Safeguard enforcement powers and functions are:

- the power for the Information Commissioner to conduct an assessment of a data holder, accredited data recipient or designated gateway to ensure that CDR data is being handled in accordance with the privacy safeguards or the consumer data rules that relates to the privacy or confidentiality of the CDR data;
- the powers and functions the Information Commissioner has under Part IIIC or V of the *Privacy Act 1988* as those parts apply as a result of the Bill; and
- the powers and functions the Information Commissioner has under Parts 4, 6 or 7 of the Regulatory Powers Act as a result of the Bill (civil penalty provisions, enforceable undertakings and injunctions).

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

1.459 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 data holder or accredited data recipient is part of a wider pattern of conduct that breaches the CDR. In such circumstances, the Information Commissioner may consider it appropriate to conduct a joint investigation into the matter.

1.460 These delegations may only occur with the express written agreement of the ACCC to the delegation and the ACCC is satisfied of the seniority of the staff member. ***[Schedule 1, item 1, subsection 56EZ(3)]***

Direct rights of action

1.461 The Bill also creates a direct action for damages where a person who suffers damage or loss, including injury to the person's feelings or humiliation as a result of a breach of the Privacy Safeguards or consumer data rules about the privacy or confidentiality of CDR data. The person is able to recover the amount of the damage or loss sustained. ***[Schedule 1, item 1, section 56EY]***

1.462 The action would need to commence within six years after the day the action that caused the loss or damage occurred. A finding of any

fact by a Court or an admission of any fact made by the person against who the action is being taken, can be used as *prima facie* evidence in subsequent proceedings. ***[Schedule 1, item 1, subsections 56EY(2), 56EY(3) and 56EY(4)]***

Other matters

Incorporation of instruments by reference

1.463 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]***

1.464 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

1.465 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 1988*.

1.466 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]***

1.467 A person who wants to rely on a protection from liability bears an evidential burden of proof. This is appropriate given that the person will know whether or not they received evidence of a valid consent or request and otherwise met the obligations in the CDR regime. ***[Schedule 1, item 1, subsections 56GC(2) and 56GC(3)]***

Exemptions and modifications by the ACCC and by regulations

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

1.469 It is possible for the ACCC to exempt a person in respect of particular CDR data, or one or more classes of CDR data, the CDR or part

of the CDR obligations. The exemption will be made in a written notice. The exemption may or may not be time limited and may also apply unconditionally or subject to conditions. ***[Schedule 1, item 1, subsections 56GD(2) and 56GD(3)]***

1.470 The ACCC must publish the details of each exemption on its website. ***[Schedule 1, item 1, subsection 56GD(4)]***

1.471 The written instruments will not be legislative instruments because of table item 19 in section 6 of the *Legislation (Exemptions and Other Matters) Regulation 2015*.

1.472 Applications may be made to the Administrative Appeals Tribunal for a review of a decision of the ACCC to exempt or refuse to exempt a person from the CDR. ***[Schedule 1, item 1, subsection 56GD(5)]***

1.473 Exemptions, on the basis described above at paragraph 1.469, may also be made by regulations. ***[Schedule 1, item 1, section 56GE]***

1.474 The regulations will only seek to declare that provisions of the CDR 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 disallowable instruments and the Parliament will have appropriate oversight over any regulation made under the CDR regime.

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

Constitutional basis and compensation for acquisition of property

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

1.477 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.

1.478 The operation of the CDR will not ordinarily result in an acquisition of property, but if it were to arise, the Bill amends the CC Act 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]***

1.479 The Commonwealth will not be liable for the acquisition of property by any entity other than the Commonwealth. The Bill provides that the person who has acquired the relevant property will be liable to pay a reasonable amount of compensation to the person the property was acquired from. ***[Schedule 1, item 1, subsection 56GG(2)]***

1.480 In the event that the two persons do not agree to the amount of reasonable compensation payable, they may commence proceedings in the Federal Court or a Supreme Court of a State or Territory. ***[Schedule 1, item 1, subsection 56GG(3)]***

Consequential amendments

Competition and Consumer Act 2010

1.481 A range of consequential amendments are made to the CC Act as a result of the introduction of the CDR. These include new definitions. ***[Schedule 1, items 1 and 10, subsections 56AL(1) and 4(1)]***

1.482 The term 'consumer data rules' is added to various provisions in the CC Act to reflect that certain powers or functions under the Act should also refer to powers and functions in the consumer data rules as a result of the implementation of the CDR regime. ***[Schedule 1, items 11, 12 and 13, subsection 8A(4), subsections 19(1) and (7), and subsection 25(1)]***

1.483 Functions related to the CDR and consumer data rules are also added to the definition of 'core statutory provision' in subsection 155AAA(21) to ensure that the protection of certain information also includes the CDR. ***[Schedule 1, items 66 and 67, subsection 155AAA(21)]***

Privacy Act 1988

1.484 Subsection 6E(1D) is inserted into the *Privacy Act 1988* so that small business operators who hold an accreditation under the CDR regime are treated as an organisation for the purposes of the *Privacy Act 1988* in respect of information that is not CDR data. ***[Schedule 1, item 78, subsection 6E(1C) of the Privacy Act 1988]***

1.485 This amendment ensures that in all circumstances personal information held by small business accredited data recipients is protected by either the Privacy Safeguards or the *Privacy Act 1988*.

1.486 A definition of consumer data rules is also inserted into the *Privacy Act 1988* to support amendments required to that Act as a result of the CDR. ***[Schedule 1, item 77, subsection 6(1) of the Privacy Act 1988]***

Australian Information Commissioner Act 2010

1.487 The matters that must be included in an annual report released by the Information Commissioner have also been extended to include

information on its functions and powers about the CDR regime. ***[Schedule 1, items 8 and 9, sections 30 and 32]***

Review of the operation of this Part

1.488 A review of the CDR regime is required to be undertaken by an independent reviewer with a report provided to the Minister on or before 1 January 2022. ***[Schedule 1, item 1, subsections 56GH(1) and 56GH(2)]***

1.489 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)]***

1.490 Providing for a statutory review acknowledges the unique nature of the CDR regime. 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

1.491 The Bill applies from Royal Assent.

1.492 As noted above at paragraph 1.40, for the purposes of designation of the banking sector the Minister is not required to consult the ACCC or Information Commission if the designation instrument is made prior to 1 January 2020 or three months after the Bill commences, whichever is later. ***[Schedule 1, item 2]***

1.493 Similarly, the ACCC does not need to consult on consumer data rules about the banking sector provided that the consumer data rules are made prior to 1 January 2020 or three months after the Bill commences, whichever is later. ***[Schedule 1, item 2]***

1.494 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.

1.495 The Minister is also not required to consult the ACCC or Information Commissioner if the designation instrument designating the energy sector is made prior to 1 January 2020 or three months after the Bill commences, whichever is later. ***[Schedule 1, item 3]***

1.496 However, the ACCC is still required to consult on consumer data rules made about the energy sector.

Contingent amendments

1.497 The Bill makes provision for section 3 of the *Federal Circuit Court and Family Court of Australia Act 2018* commencing. This Act will update the name of the 'Federal Circuit Court' to 'Federal Circuit and Family Court of Australia (Division 2)'. The contingent amendment will make the necessary changes to references to the 'Federal Circuit Court' in our Bill if that Act commences. ***[Schedule 1, item 82, paragraphs 56EU(4)(b), 56EW(3)(b), 56EX(3)(b) and 56EY(5)(a)]***

Chapter 2
Statement of Compatibility with Human Rights

Prepared in accordance with Part 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*

Treasury Laws Amendment (Consumer Data Right) Bill 2011

2.1 This Bill is compatible with the human rights and freedoms recognised or declared in the international instruments listed in section 3 of the *Human Rights (Parliamentary Scrutiny) Act 2011*.

Overview

2.2 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.

2.3 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. It is expected to provide benefits to consumers such as more choice in where they take their business or more convenience in managing their money and services.

2.4 A person may commit an offence or contravene a civil penalty provision if they fail to comply with certain obligations in the CDR regime.

Human rights implications

2.5 The Bill engages the following human rights:

- the right to protection from arbitrary or unlawful interference with privacy;
- the right to a fair trial and public hearing; and
- the right to be presumed innocent until proved guilty according to law.

Protection from arbitrary or unlawful interference with privacy

2.6 The Bill engages the right to protection from unlawful or arbitrary interference with privacy under Article 17 of the International

Covenant on Civil and Political Rights (ICCPR) because it enables a person to direct another person or entity to transfer personal information about themselves to another person or entity.

2.7 In order for an interference with the right to privacy to be permissible, the interference must be authorised by law, be for a reason consistent with the ICCPR and be reasonable in the particular circumstances. The UN Human Rights Committee has interpreted the requirement of 'reasonableness' to imply that any interference with privacy must be proportional to the end sought and be necessary in the circumstances of any given case.

2.8 The CDR is a right for consumers to authorise data sharing and use. The consumer data right will provide individuals and businesses with a right to access data relating to them; and to authorise secure access to their data by persons who have been 'licensed' to receive the data – 'accredited data recipients'.

2.9 Underpinning the CDR regime is a requirement that the disclosure between entities of personal information is only permitted with the express consent of the individual. The consumer data right does not allow businesses who hold or receive data to transfer or use data without the customer's consent.

2.10 It is intended that the CDR, by giving consumers improved access to data, will support better comparison services by taking into account Australians' actual circumstances and promoting more convenient switching between products and providers.

2.11 The Bill protects against arbitrary interference with privacy by establishing a set of CDR specific privacy safeguards, modelled off the existing Australian Privacy Principles (APPs) but with additional obligations.

2.12 The privacy safeguards included in the CDR are:

- restrictions on the use, collection and disclosure of information received through the consumer data rules, including information derived from this information, to circumstances where the consumer has given express consent;
- requirements to have privacy policies in place which are easily accessible and clearly explain the complaints handling process;
- obligations on data holders and accredited data recipients to correct information;
- obligations on data holders and accredited data recipients to notify the consumer when information is disclosed;

- requirements to destroy information that is purported to have been shared under the consumer data rules but has been disclosed in error;
- strong powers and significant funding for regulators, including the Office of the Australian Information Commissioner (OAIC);
- only allowing direct marketing with the express consent of the consumer; and
- remedies for breaches, including through external dispute resolution arrangements.

2.13 The OAIC will advise on and enforce privacy protections, and provide complaint handling for breaches of the Privacy Safeguards. Consumers will have a range of avenues to seek remedies for breaches of their privacy or confidentiality including access to internal and external dispute resolution and direct rights of action.

2.14 The accreditation process is a key protection against arbitrary or unlawful interference with privacy. Only trusted and accredited third parties will be able to access data from data holders at the customer's direction. The ACCC will initially be responsible for accrediting entities. The requirements that need to be met will be set out in legislative instrument and will address matters such as:

- having systems, resources and procedures in place which enable the entity to comply with their CDR obligations including the security of information; and
- having internal dispute resolution procedures in place and being a member of a recognised external dispute resolution body.

2.15 These limitations are consistent with the prohibition on arbitrary interference with privacy as they are directed at legitimate objectives and are reasonable and proportionate to those objectives.

Penalty provisions

Assessment of civil penalties

2.16 Civil penalty provisions may engage criminal process rights under Articles 14 and 15 of the ICCPR regardless of the distinction between criminal and civil penalties in domestic law. This is because the word 'criminal' has an autonomous meaning in international human rights law. When a provision imposes a civil penalty, an assessment is therefore required as to whether it amounts to a 'criminal' penalty for the purposes of Articles 14 and 15 of the ICCPR.

2.17 The civil penalty provisions in the Bill should not be considered 'criminal' for the purposes of international human rights law. While the civil penalty provisions included in the Bill are intended to deter people from not complying with their obligations under the CDR regime, none of the civil penalty provisions included in the Bill carry a penalty of imprisonment for non-payment of a penalty.

New criminal offences

2.18 The Bill includes two new criminal offence provisions for misleading conduct and holding out that you are 'licensed' to receive data under the CDR when you are not.

2.19 It is considered appropriate to apply criminal penalties for these offences as this type of conduct directly undermines the protections put in place in the CDR Regime.

2.20 These criminal offences do not amend any of the criminal process or procedural rights that currently exist and are upheld in accordance with article 14 of the ICCPR.

Evidentiary burden

2.21 An offence provision which requires a defendant to carry an evidential burden may be considered to engage the right to the presumption of innocence. Section 56GC of the Bill engages the right to the presumption of innocence because a defendant bears an evidential burden.

2.22 Section 56GC of the Bill protects a person from liability if the person (the first person) provided information to another person (the second person) or allowed the second person access to information in good faith and complying with the requirements of the CDR regime.

2.23 Section 56GC of the Bill protects the first person from liability so that the person will not be able to have an action taken against them, whether civil or criminal, about the provision of the CDR information.

2.24 However, a person who wants to rely on a protection from liability bears an evidential burden. This is appropriate as the person will know whether or not they received evidence of a valid consent or request and otherwise met the obligations in the CDR regime.

2.25 The effect of the limitation is that the defendant must merely provide evidence that suggests a reasonable possibility that the person disclosed the information in good faith and in accordance with the CDR requirements. Once this has occurred the prosecution must refute this beyond reasonable doubt to obtain a conviction (see section 13.3 of the Criminal Code).

2.26 This material will be within the person's knowledge. A person disclosing information will need to meet certain record keeping

requirements, and would, for example be able to demonstrate that the correct consent documents had been received and that the recipient was listed on the accreditation register. Being able to produce this material should place no additional burden on the person.

2.27 To the extent this provision might be considered to limit the presumption of innocence, the limitation is reasonable in all circumstances.

Right to a fair and public hearing

2.28 Article 14 of the ICCPR ensures that everyone shall be entitled to a fair and public hearing by a competent, independent and impartial tribunal established by law.

2.29 The Bill may be considered to engage the right to a fair and public hearing as it extends the existing infringement notice provisions in the CC Act so that an infringement notice may be given where a person has contravened a civil penalty provision.

2.30 However, the right to a fair and public hearing by a competent, independent and impartial hearing is not limited by the Bill because the person may still elect to have the matter heard by a court rather than pay the amount specified in the infringement notice. This right will be stated in any infringement notice.

2.31 For these reasons the Bill is not considered to limit the right to a fair and public hearing.

Conclusion

2.32 The Bill is compatible with human rights because to the extent that the Bill may limit human rights, those limitations are reasonable, necessary and proportionate.