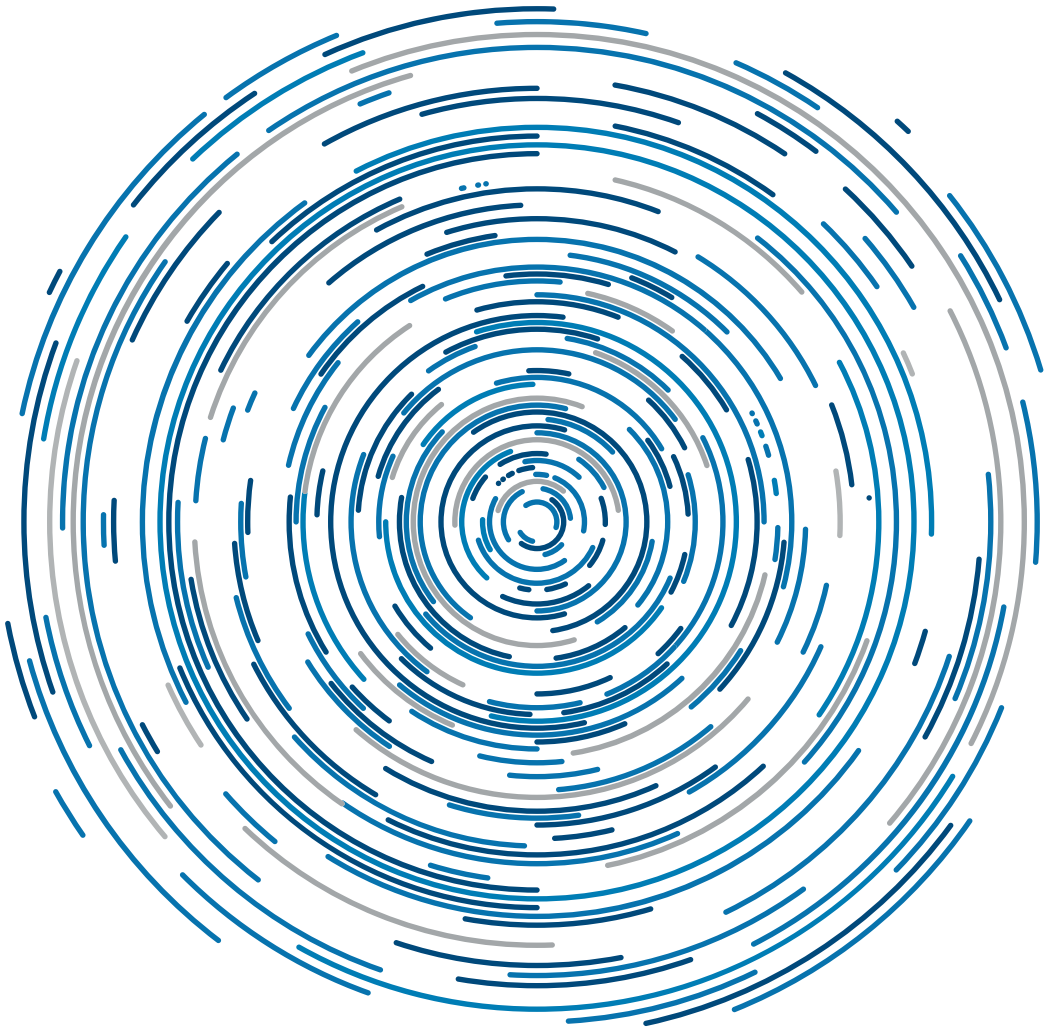
Deloitte.



Shaping the Future

Consumer Data Right

Deloitte Submission on the Draft Consumer Data Right Bill

7 September 2018

Introduction

On 15 August 2018 the Treasury released the Treasury Laws Amendment (Consumer Data Right) Bill 2018 (the CDR Bill or the Bill). The CDR Bill is part of the regulatory framework to encourage greater competition in in the Australian economy, starting with the banking sector from July 2019.

You have invited comments on this draft bill. Deloitte is pleased to provide our observations in this submission. Overall we believe that open data has the potential to enhance the Australian economy. We support the legislative framework set out in the CDR Bill and the guardrails that have been put in place in the CDR Bill to support privacy, confidentiality and information security. Our response has been based on the intent of the legislation and practical issues that organisations may encounter in complying with the open data requirements. We have not sought to provide a detailed commentary on the legal drafting of the Bill.

The Treasury's Consumer Data Right publication[1] and the Farrell Report[2] both outlined four key principles for establishing data sharing and a consumer data right in Australia:

- It should be ***consumer focussed***. It should be for the consumer, be about the consumer, and be seen from the consumer's perspective.
- It should ***encourage competition***. It should seek to increase competition for products and services available to consumers so that consumers can make better choices.
- It should ***create opportunities***. It should provide a framework from which new ideas and business can emerge and grow, establishing a vibrant and creative data sector that supports better services enhanced by personalised data.
- It should be ***efficient and fair***. It should be implemented with security and privacy in mind, so that it is sustainable and fair, without being more complex or costly than needed.

We support the ***consumer focus*** of the CDR Bill including, in principle, the extension of the definition of a CDR consumer to include business entities. In the spirit of consumer focus, differences in the Rules and Standards applied to different sectors should be minimised to enhance consumer understanding, and ultimately usage, of data sharing.

We support the intention of the CDR Bill to enhance and ***encourage competition*** by giving consumers the right to access data about them and their transactions that is currently held by businesses, and by ensuring that product information is available, accessible and comparable.

The Australian Consumer and Competition Commission (ACCC) has noted that competition provides incentives to improve economic efficiency to:

- produce goods and services at least cost (technical or productive efficiency);
- allocate resources to their highest valued use (allocative efficiency); and
- innovate to create new products and production processes (dynamic efficiency).[3]

Finding the balance between achieving a sound, stable system and encouraging competition and innovation is a continuing challenge and an evolving challenge in sectors being disrupted by technological change.

[1] The Australian Government, the Treasury, Consumer Data Right, 9 May 2018

[2] The Australian Government, the Treasury, Open Banking: Customers choice convenience confidence, December 2017 (Farrell Report), pages v and 8-10

[3] Australian Competition and Consumer Commission, 'Reinvigorating Australia's Competition Policy: ACCC Submission to the Competition Policy Review', 2014.

Over the last decade the financial services sector's regulatory focus has been on enhancing prudential and consumer protection rules. The CDR Bill brings an important focus on competition, which we believe is a cornerstone to the regulatory framework supporting the financial services sector.

The CDR Bill intentionally establishes a framework for the implementation of a consumer data right in many sectors of the economy. As a result many of the details on the application of the consumer data right to a particular sector will be set out by the ACCC in the consumer data rules and in the standards which apply to each specific sector.

We support the intention of the CDR Bill to enhance and ***create opportunities*** and ***encourage innovation***. The obligations in the CDR Bill on data holders and the process for accrediting data recipients should help achieve this. However, we note that this will require careful consideration of the treatment and definition of 'directly or indirectly derived' CDR data to ensure that innovative service offerings from both incumbent and new competitors are not compromised.

It will also require consideration of the application of reciprocity requirements, including on initial application of the consumer data right to a sector to avoid creating a competitive disadvantage for either new entrants or incumbents.

We also support the focus on ***security and privacy*** to help ensure that the open data arrangements engender consumer confidence. Privacy and confidentiality will be critical to consumer acceptance and unlocking the economic benefits from encouraging competition.

To ensure that the data sharing arrangements are ***efficient and fair*** it will be important to ensure that the CDR data arrangements consider other existing data related legislative regimes and frameworks.

The comments in our submission are mainly intended to clarify aspects of the implementation of open data in Australia and its interaction with other legislation. However, it is important to acknowledge that the implementation of open data is not without risks.

The increase in:

- the amount of consumer data that is shared; and
- the number of counter-parties with which this data is shared;

where the consumer data is:

- sourced from systems that were not necessarily built with consumer data sharing in mind; and
- shared via a new regulatory environment which introduces new obligations on data holders and authorised data recipients;

with

- the first sector in which open data is implemented being one with high risk information;

together create a risk of unintended, and potentially unanticipated, adverse consequences.

Our response to the CDR Bill includes comments on:

1. The regulatory framework for the CDR
2. The definition of CDR data including derived data and the data standards that would apply to CDR data
3. The framework for establishing CDR Rules
4. The accreditation process for data recipients
5. The privacy provisions of the CDR Bill and their interaction with the Australian Privacy Principles
6. The interaction of the CDR Bill with other financial services legislation including financial crime legislation and conduct legislation
7. The application of the CDR Bill to other sectors of the economy, particularly energy, telecommunications, and consistency with data sharing initiatives in the public sector

The Regulatory Framework

Object of the Bill (Section 56AA)

Section 56AA sets out the object of the CDR Bill:

> *The object of this Part is:*
>
> *(a) to enable consumers in certain sectors of the Australian economy to require information relating to themselves in those sectors to be disclosed:*
>
> *(i) to themselves; or*
>
> *(ii) to others in those sectors that they trust; and*
>
> *(b) to enable any person to access any information in those sectors that does not relate to any identifiable, or reasonably identifiable, consumers; and*
>
> *(c) as a result of paragraphs (a) and (b), to create more choice and competition within those sectors.*

While we do not disagree with the intent of the object set out for the CDR Bill, we believe that the wording of this section could be more focused and specific. There should be two primary objectives of the CDR Bill:

1. to create more choice and competition in the Australian economy[4]; and
2. to enhance the right of an individual or entity to access and control their data.

The mechanism to achieve these objectives is enabling consumers, both individuals and other entities, to require certain information relating to them and their interactions to be disclosed, at their request, to accredited third parties.

This section includes a reference to disclosure of this information to "others in those sectors that they trust." (Subsection 56AA(a)(ii)). However, the CDR Bill is only intending to enable consumers to require organisations to share data relating to the consumer with 'accredited third parties'. As a result, we recommend that the object of the CDR Bill should be modified to specifically refer to sharing CDR data with 'accredited third parties' and remove the reference to "others in those sectors that they trust".

This section also refers to enabling "any person to access any information in those sectors that does not relate to any identifiable, or reasonably identifiable, consumers." (Subsection 56AA(b))

We believe that this clause is too broad to be effective and potentially presents a risk to commercial interests. The reference to 'any information' could include, inter alia, intellectual property included in pricing algorithms, customer segmentation analytics, customer portfolio characteristics, or information about market share.

A means for compensating holders fairly for 'value-added' data or 'derived' data needs to be in place before open banking commences. As it stands, it is incumbent on the data recipient to compensate the data holder or CDR consumer where a property right is involved, but it is not clear what the mechanism would be to ensure holders are able to receive a 'fair' price. In addition, it does not appear that the draft CDR Bill includes a basis for determining compensation for derived data that does not have a property right in it, for example a database.

However, a corollary is that in certain sectors consumers may unknowingly provide information with consents buried in lengthy terms and conditions that consumers have not read.

[4] This is particularly important in the context of open banking as greater competition in banking and financial services impacts competition in the economy more broadly.

Designation of a Sector (Section56AD)

We support the inclusion in Section 56AD of a specific requirement for the Minister to consider consumer impact, market efficiency, privacy, competition, innovation, regulatory impact and other relevant matters before designating a sector.

We have previously noted that "regulation, and the compliance burden that accompanies it, comes at a cost. An unduly onerous regulatory or supervisory system risks adding unnecessary costs and restricting innovation throughout the economy. … Good regulation must carefully consider this balance. Specifically, it should be demonstrably welfare enhancing. Overall, **a regulation should only be enacted if its benefits outweigh its costs**."[5] This same principle applies to the designation of an industry sector for application of the Consumer Data Right.

Determining the **regulatory** impact of designating a sector is important. This is acknowledged in the Explanatory Memorandum: *"While the CDR is intended to enhance competition, that should not occur at the expense of significant regulatory burden or disruption unless the **broadly defined benefits** of designation outweigh the **regulatory** impact."*[6] [Emphasis added]

As a matter of principle, broadly defined benefits should be weighed against broadly defined costs, not just the regulatory burden component of costs. Thus, a Regulatory Impact Assessment (RIA) should seek to provide answers to questions such as:

- how much is consumer switching between providers likely to increase if consumers are provided with access to their data, but their ability and willingness to make decisions based on this information is not improved?
- how much will competition with large incumbents (as distinct from between large incumbents) increase if the large incumbents invest in superior capability to analyse the data and, hence innovate, while still benefiting from scale economies (including funding costs)?
- will the regulator and standards body have sufficient capability and capacity to meet demand in a timely manner, e.g. for accreditation?
- will the additional regulatory burden applied to accredited data recipients outweigh the benefits of receiving data?

We note that in the case of banking, the government's decision to implement data sharing occurred prior to the consultation undertaken as part of the preparation of the Open Banking report. We question whether, in the case of banking, consideration of the matters noted in Section 56AD will be effective given the short timeframe for implementation. A RIA is unlikely to provide definitive answers, but it could highlight areas where costs are significant and where there would be benefit in considering offsetting measures. However, there is likely to be a longer timeframe for other designated sectors and greater benefit from a RIA.

Section 56AD could be further strengthened by explicitly including a consideration of the costs and benefits associated with a designating a sector, acknowledging that these may differ from one sector to the next.

In considering 'other relevant matters' the approach should be directed at:

- embedding the **principle** of a less interventionist approach, where regulators only address well-defined problems;
- seeking to **align** Australian regulations with international standards, unless there is a strong rationale to do otherwise;

[5] Deloitte Access Economics, Shaping the Future: Deloitte submission to the Interim Report of the Financial System Inquiry, 26 August 2014

[6] The Australian Government, the Treasury, Exposure Draft Explanatory Materials, 2018, paragraph 1.34, page 10

- encouraging the **design** of less prescriptive regulation;
- ensuring that there are appropriate and effective **enforcement** mechanisms consistent with an emphasis on outcome-based regulation;
- ensuring that a **culture** consistent with an emphasis on outcome-based regulation is maintained within each of the regulators;
- boosting the **accountability** of regulators; and
- encouraging **regulated entities** to actively explore better ways of meeting the objectives of regulation.

Consultation (Section 56AD(2) and (3))

Under Section 56AD the Minister ***must*** consult the Commission (Section 56AD (2)) and the Information Commissioner (Section 56AD(3)) before issuing an instrument under subsection 56AC(2).

However Section 56AE implies that consultation of the Commission and Information Commissioner is optional when it states '***If*** the Commission is consulted under subsection 56AD(2)…" (Section 56AE(1) emphasis added) and '***If*** the Information Commissioner is consulted under subsection 56AD(3)' (Section 56AE(2) emphasis added).

We recommend that the language used in these sections be reviewed to avoid ambiguity about the Minister's obligation to consult the Commission and the Information Commissioner when designating a sector.

Implementation

The challenge in the Australian financial system has not been in the design of principles; it has been in their implementation. While overarching principles have been well specified in legislation, they must also be translated into practice at the detailed operational level.[7]

It will be important that the principles outlined in the CDR Bill are supported by Rules and Standards that are appropriate to each designated industry sector and which support the policy objectives of enhancing competition and choice.

Even more vital is the need to ensure the accountability of regulators and ensure an outcomes-based culture within which regulations are enacted and enforced.

The CDR Bill provides the Commission with the ability to make consumer data rules for specific industry sectors (section 56BA) and introduces criminal (subsections 56BM(1) and 56CG(1)) and civil offences (subsections 56BM(2) and 56CG(2)).

In addition, the Information Commissioner has a range of civil penalties for breaches of the privacy safeguards.

The CDR will or will potentially apply to a broad range of sectors. A key to achieving effective enforcement of the CDR requirements will be the quality of accountability standards in the regulatory bodies. The quality of the administration of regulation will crucially depend upon the experience and skills of regulators themselves.

To support the accountability of regulators, the CDR Bill could explicitly include an obligation for the regulators to report to the Minister on the effectiveness of their enforcement of the requirements set out in the CDR legislation, Rules and Standards.

Consideration could also be given to undertaking an independent review of regulators' performance on CDR prior to designating additional sectors.

[7] Deloitte Access Economics (2014) op. cit.

CDR data

Meaning of CDR data (Section 56AF(1) and (2))

The Farrell Report outlined various categories of data:[8]

Shared	Not shared
Customer-provided data (excluding identity verification) - data holders should be obliged to share all information that has been provided to them by the customer (or a former customer), subject to resolution of issues with identity verification.	**Customer-provided identity verification data** – to be reconsidered by the ACCC once consideration of proposed reforms to AML laws have been finalised and concerns on liability have been resolved.
Transaction data - data holders should be obliged to share all transaction data in a form that facilitates its transfer and use.	**Value-added customer data** - data that results from material enhancement by the application of insights, analysis or transformation by the data holder should not be included in the scope of Open Banking.
Product data – banks will be required to publicly disclose information on their products and services where they are under existing obligations to publicly disclose this information.	**Aggregated data sets** - Aggregated data sets should not be included in the scope of Open Banking. Inclusion should be considered once the broader CDR is operational.

Source: Farrell Report (2017), Chapter 3, The Scope of Open Banking; Deloitte analysis

The Farrell Report recommended ***excluding*** 'value-added customer data' as it was concerned that imposing an obligation to share value-added customer data could breach intellectual property rights, or interfere with existing commercial arrangements.[9]

By contrast subsections 56AF(1) and (2) refer to both data 'specified' in an instrument designating a sector and data 'directly or indirectly derived' from other CDR data.

In the briefing sessions the Treasury representatives has noted that the concepts of 'directly or indirectly derived' data and 'value-added customer data' represent a spectrum. The Treasury representatives also noted concern that a narrow interpretation of 'value-added customer data' could include, in the case of the banking sector, account balance information. This would result in this information not being shared as CDR data in contrast to the intention of the open banking policy.

A number of potential use cases for CDR data rely on the ability to 'directly or indirectly' derive insights from customer transaction data. In banking these include personal financial management, account aggregation, spend analysis, and the creation of tailored recommendations as well as traditional credit analysis and reporting.

The Farrell Report also noted that including 'value-added customer data' in the scope of open banking would reduce incentives to invest in data analytics and transformation.[10]

Similar issues potentially arise in other sectors where insights which have been 'directly or indirectly' derived from customer transaction data are part of organisations' customer value propositions.

While acknowledging that it will be important for specific data to be specified in the instrument designating a sector as one to which CDR will apply, we recommend that the definition of CDR data be modified to better reflect the intent of the CDR.

[8] Farrell Report (2017),op. cit., Chapter 3, The Scope of Open Banking, pages 33-40

[9] Farrell Report (2017),op. cit., Recommendation 3.3, page 38

[10] Farrell Report (2017),op. cit., page 38

For example, the definition of CDR data could explicitly refer to:

- customer data; and
- transaction or usage data;

and could explicitly exclude:

- data 'directly or indirectly' derived from customer and transaction CDR data.

This would allow the Rules and Standards to define for a specific sector what is included in each of these categories.

CDR data definition – product data (Section 56AF)

The Farrell Report noted a distinction between ***customer related data*** (including customer-provided data, transaction data, value-added customer data, and aggregated data sets based on customer data) and ***product data*** which does not relate to a customer.[11]

The explanatory memorandum notes that certain CDR data that does not relate to a CDR consumer, such as general product information, could also be transferred to a non-accredited entity.[12]

This reference in the explanatory memorandum seems to conflate the ***provision*** of information, such as product information which entities are required to make available to any third party, with the ***transfer*** of CDR data which relates to CDR consumers.

Given the differing requirements for data recipient accreditation, and the different privacy and confidentiality obligations related to consumer information, we recommend that when identifying the data to which the CDR Bill applies, a clear distinction be made between customer-related data and product data.

Inclusion of legal entities in the definition of CDR consumer (Section 56AF(4))

The Treasury has stated that the intention of the CDR legislation is to ensure that the definition of Consumer Data Rights is broad and extends beyond the traditional definition of a consumer to include small, medium and large business enterprises.

Acknowledging that the CDR is a broad right, a consequence of the CDR Bill's definition of a CDR consumer is that it blends individual privacy with confidentiality for legal entities. For example, "*Privacy*" is a consideration for the Minister's power to designate sectors, "*whether the consumers be individuals or other persons such as businesses*" (Subsection 56AD(1)(a)(iii)).

Consideration should be given to including separately within the definition of CDR consumer, reference to natural persons and business enterprises, including corporations, partnerships and trusts.

Moreover, this would allow greater distinction of the obligations around privacy (applying to individuals) and confidentiality (applying to business enterprises). It will also enable greater clarity to be provided in the CDR Bill or in the Rules, on who may request access to CDR data related to a business enterprise.

Definition of a CDR Consumer (Section 56AF(4))

In establishing the definition of a CDR consumer (which impacts the associated data in scope) legislators need to be conscious of the many different roles that parties can hold in relation to an account.

[11] Farrell Report (2017), op. cit., Chapter 3, The Scope of Open Banking, pages 33-40
[12] Exposure Draft Explanatory Materials, paragraph 1.48, page 13

In banking, for example, in addition to account holders, other roles individuals can hold in relation to an account include (but are not limited to) joint account holders, account users (e.g. for a credit card), authorised signatories, trustees, guardians, attorneys and beneficiaries. These roles and the individuals in these roles may also change over time.

It will be important that the Rules designating a sector provide clarity on which consumers are eligible CDR consumers as a result of their account ownership or their usage or transactions associated with an account.

Definition of a CDR Consumer (Section 56AF(4))

The definition of a CDR consumer refers to 'a person to whom the CDR data ***relates***…' (Subsection 56AF(4) emphasis added)

The term 'relates' is a similar term to that adopted in the GDPR definition of personal data. The use of the term 'relates' instead of the term 'about' in reference to an identifiable or reasonably identifiable individual, is intended to broaden the scope of protected data, so that it includes metadata.[13]

To further clarify the definition of personal information the Consumer Data Rules could provide examples, akin to the GDPR, of types of data that are classified as personal information.[14]

Data holders, accredited data recipients and derived data (Sections 56AG(1) and 56AG(3)(c))

The particular CDR data held by an accredited data recipient includes 'any other data from which it was directly or indirectly derived' by the accredited data recipient (Subsection 56AG(3)(c)).

However the direct or indirect derivation of particular data from CDR data is an action that defines a person or entity as a data holder (Subsection 56AG(1)(ii)).

We recommend that the CDR Bill provide greater clarity on what constitutes directly or indirectly derived CDR data and the impact the process of directly or indirectly deriving CDR data has on a person or entities classification as a data holder or a data recipient.

Meaning of accredited data recipient (Section 56AG(3)(d))

The CDR Bill notes that a person is an accredited data recipient of particular CDR data if, inter alia, the person is ***not*** a data holder of the CDR data (Subsection 56AG(3)(d)).

However, the Exposure Draft Explanatory Materials notes that accredited data recipients are ***entities holding CDR data*** as a result of that CDR data being disclosed to them at the direction of a CDR consumer under the consumer data rules.[15]

It would appear that the CDR Bill intends that a person or entity will not be an accredited data recipient of ***particular*** CDR data if that person or entity is already a data holder of that ***particular*** CDR data. This is not clear when the CDR Bill is read in conjunction with the Explanatory Materials.

Geographical application (Section 56AH)

The CDR Bill applies to CDR data generated or collected outside of Australia, if the data is generated or collected by ***or on behalf of*** an Australian citizen or permanent resident or an Australian registered corporate entity specified in an instrument designating a sector (subsection 56AH(1) emphasis added).[16]

---

[13] Exposure Draft Explanatory Materials, paragraph 1.52, page13
[14] For example, the definition of 'personal data' under the GDPR clearly states that it extends to location data: Article 4(1).
[15] Exposure Draft Explanatory Materials, paragraph 1.42, page 12
[16] Exposure Draft Explanatory Materials, paragraph 1.55, page 14

It is possible that a foreign entity acting 'on behalf of' an Australian citizen or permanent resident or an Australian registered corporate entity could collect or generate CDR data, including directly or indirectly 'derived' data.

It is not clear how the Commission would enforce the CDR Bill in relation to action taken by a foreign entity 'on behalf of' an Australian citizen or permanent resident or an Australian registered corporate entity.

Consideration should also be given to how the Commission would enforce the CDR Bill in relation to such actions taken by a foreign entity, where the requirements of the CDR Bill conflict with applicable foreign law.

Data Standards (Section 56FE)

Section 56FE sets out various matters which need to be considered or included in the data standards established under the CDR Bill, including the format, disclosure, and security of CDR data.

These data standards will be subject to the consumer data rules. 'Privacy Safeguard 11 – security of CDR data' does not prescribe the steps that need to be taken to protect the data, but relies on the Consumer Data Rules and Data Standards.

To ensure secure data flows between data holders and accredited data recipients, and continued security standards of recipients, it will be important that the consumer data rules and data standards set out stringent data protection and security safeguards that extend to people, process, and technology.

Consideration should be given to ensuring that the data standards also include appropriate standards for the service levels associated with the sharing and transfer of data.

Reciprocity

The Farrell Report noted, in the context of banking, that *"it would seem unfair if banks were required to provide their customers' data to data recipients such as FinTechs or non-bank credit providers, but those data recipients were not required to reciprocate in any way, merely because they were not banks and therefore did not hold 'banking' data."*[17]

The Explanatory Memorandum defines the principle of reciprocity as: *"When in possession of a consumer's CDR data, an accredited entity can also be directed by a consumer to provide that data to other CDR participants."*[18]

The Farrell Report recommended that:

> *Entities participating in Open Banking as data recipients should be obliged to comply with a customer's direction to share any data provided to them under Open Banking, plus any data held by them that is transaction data or that is the equivalent of transaction data.*[19]

The definition of reciprocity in the Explanatory Memorandum only refers to an entity sharing data they have received. It does not refer to providing 'equivalent data'.

While acknowledging the potential for sector creep, the Farrell Report recommended that:

> *as part of the accreditation process for data recipients that do not primarily operate in the banking sector, such as data recipients from the technology sector, the competition regulator*

[17] Farrell Report (2017), op. cit., page 43

[18] Exposure Draft Explanatory Materials, paragraph 1.46, page 12

[19] Farrell Report (2017), op. cit., Recommendation 3.9 page 44

should determine what constitutes equivalent data for the purposes of participating in Open Banking.[20]

The introduction of data sharing is intended to encourage greater competition. This competition could come from new entrants from outside a designated sector, including from organisations operating in the technology sector.

We recommend that the CDR Bill provide greater clarity on the obligation of CDR participants to provide 'equivalent' data.

[20] Farrell Report (2017), op. cit., page 44

CDR Rules

Consumer Data Rules (Section 56BA)

The ACCC will be responsible for defining rules across sectors, data classes, and CDR participants (Customers, Holders and Recipients). These rules may deal with, inter alia, disclosure of CDR data.

In general we support the discretion given to the Commission to make different rules for different sectors, classes of CDR data and classes of persons.

In exercising its discretion the Commission should be guided by the primary objective of creating more choice and competition in the Australian economy.

To support consumer awareness and understanding of the operation of open data in the Australian economy, the Commission should minimise the extent to which different rules are applied in different sectors and limit differences to those necessary to give effect to the application of CDR data sharing in that sector. Consideration should be given to making these restrictions more explicit in this section.

Matters dealt with by the Consumer Data Rules (Section 56BB)

Some entities have expressed concern that a Data Holder may not provide CDR data in a timely manner. Other entities have expressed concern that a Data Holder may create a cumbersome and onerous customer experience as part of the identity verification or the data selection process. Concerns have also been expressed that the current response times for data sharing in some sectors (e.g. electricity) are significantly slower than those which apply, or are expected to apply, to the banking sector. Significant differences in response times for sharing data risk undermining public confidence in data sharing.

Section 56BB of the CDR Bill could explicitly state that the consumer data rules may deal with the timeframes within which sharing of CDR data is expected to occur.

Disclosure, use, accuracy, storage, security or deletion of CDR data for which there are CDR consumers (Section 56BC)

Section 56BC sets out a number of matters which may be included in the consumer data rules for a designated sector. We support the matters that have been noted in this section, noting that the categories of matters which may be included in the consumer data rules in this section is non-exhaustive.

Consideration could be given to explicitly including in this section an obligation on CDR data holders to maintain a registry of requests to share CDR data, including evidence that the request was processed and, potentially, the period within which the request was processed. It is possible that this is contemplated in Section 56BG.

Disclosure, use, accuracy, storage, security or deletion of CDR data for which there are no CDR consumers (Section 56BD)

Data for which there are no CDR consumers is likely to include aggregated data sets and potentially value-added data or derived data.

Section 56BD potentially requires a data holder to disclose this CDR data to parties making a valid request. It includes the power for the Commission to determine the 'amount of a fee' that can be charged for disclosing this data.

We believe that this section presents a potential risk to commercial interests. This could include intellectual property included in pricing algorithms, customer segmentation analytics, customer portfolio characteristics, or information about market share.

It is not clear why it is appropriate for the Commission to determine the 'amount of a fee' that can be charged for disclosing this data.

If the requirement for the Commission to determine the 'amount of a fee' that can be charged for disclosing this data is not changed, a means for compensating holders fairly for 'value-added' data or 'derived' data needs to be in place before open banking commences.

As it stands, it is incumbent on the data recipient to compensate the data holder where a property right is involved, but it is not clear what the mechanism would be to ensure data holders are able to receive a 'fair' price.

Rules for a designated sector (Section 56BN)

We support the inclusion in Section 56BN of specific requirements for the Minister to consider the matters referred to in subsection 56AD(1) – viz. consumer impact, market efficiency, privacy, competition, innovation, regulatory impact and other relevant matters – when making consumer data rules for a sector.

Section 56BN could be further strengthened by explicitly including a consideration of the costs and benefits associated with the rules applied to a designated sector, acknowledging that these may differ from one sector to the next.

CDR Data Recipient Accreditation

Accreditation (Section 56BF)

The ACCC will be responsible for defining rules for accrediting data recipients.

In general we support the discretion given to the Commission to make a risk-based determination of different levels of accreditation.

To support consumer awareness and understanding of the operation of open data in the Australian economy, the Commission should minimise the extent to which an entity operating in different designated sectors receives different levels of accreditation.

Accreditation Process (Section 56CE)

The open data regime has the potential to attract new competitors to a sector. This could include new entities, such as neobanks in the case of banking, or existing entities intending to compete in the sector, such as technology providers or retailers.

Section 56CE outlines that the Data Recipient Accreditor may "accredit a person if the person satisfies the criteria specified in the consumer data rules for accreditation."

It will be important that the rules for each sector clearly set out the accreditation process for non-traditional entities operating in each sector, and that the accreditation process for these entities supports the objective of the CDR Bill of creating more choice and competition in the Australian economy.

Where the implementation timetable for a sector is staggered, consideration should be given to accrediting an entity as a Data Recipient before they are required to comply with the obligations as a Data Holder.

If this was not done, there is a risk that the first-mover advantage provided to the organisations to which the CDR obligations initially apply would have the unintended consequence of creating a competitive disadvantage for either new entrants or incumbents.

Non-accredited data recipients (Section 56CG)

The CDR Bill allows a consumer to request that CDR data about them be shared with them directly. They can then choose to share this with an accredited data recipient.

However, the Explanatory Memorandum acknowledges that in some circumstances a CDR consumer may wish to share their data to a third party outside of the CDR system (i.e. a non-accredited data recipient).

It is possible that a market may arise where rather than just 'sharing' data a consumer wishes to realise value from their data by selling their data to a third party. The sale of their CDR data by a consumer would be consistent with the objective of enabling consumers "*to harvest the value of their data*."[21]

Non-accredited data recipients may include, for example, accountants, financial advisers or credit assistance providers. They could also include marketing firms. In some circumstances, the distinction between an accredited data recipient and a non-accredited data recipient may be unclear, particularly for non-financially literate consumers.

The CDR Bill introduces an offence of a person representing (holding out) that they are an accredited data recipient. (Section 56CG)

[21] Exposure Draft Explanatory Materials, paragraph 1.33, page10

We recommend that the CDR Bill clarify the nature of allowable actions for non-accredited data recipients.

The CDR Bill should be reviewed to assess how the provisions of the Bill would operate in an environment in which a CDR consumer wished to sell their data to a third party irrespective of whether that third party was an accredited data recipient.

Register of Accredited Data Recipients (Section 56CK)

Public access to the Register of Accredited Data Recipients is likely to be an important component of building public trust and confidence in data sharing.

Section 56CK requires the Accreditation Register to "establish and maintain" an electronic "Register of Accredited Data Recipients." (Section 56CK(1) and (2))

However, the "publication or availability of all or part of the register, or of specified information in the register" is subject to the requirements outlined in the consumer data rules for a specific sector. (Section 56CK(4)(c)).

Given the importance of building public trust and confidence in data sharing, the requirements of the consumer data rules for a specific sector should not be able to restrict publication or availability of all or part of the Register of Accredited Data Recipients.

Privacy

Interaction of CDR Bill with Privacy Act

In the briefing sessions on the CDR Bill, Treasury noted that they were considering three options in relation to the interaction of the CDR Bill with the *Privacy Act 1988* (the Privacy Act):

1. The Privacy Safeguards in the CDR Bill would operate in parallel with the Australian Privacy Principles (APPs) and the Privacy Act
2. The Privacy Safeguards in the CDR Bill would replace the APPs and the Privacy Act for a designated sector
3. The Privacy Safeguards in the CDR Bill would apply to data recipients but the APPs and the Privacy Act would continue to apply to data holders in a designated sector.

These options differ from those set out in the explanatory memorandum which proposed that "the Privacy Act and the APPs will continue to apply to data holders under the CDR (as defined by section 56AG)".[22]

The explanatory memorandum appears to propose option 3 whereby for *"accredited data recipients (as defined by section 56AG), the privacy safeguards will substitute for the APPs so that if an action is inconsistent with the privacy safeguards, it will not be "required or authorised by law" by virtue of the APPs"*.[23]

The replacement of APPs with Privacy Safeguards in designated sectors (Option 2) or the differential application of APPs and Privacy Safeguards to different CDR participants, risks creating confusion for individuals and organisations and undermining consumer confidence in data sharing.

We would support the implementation of the first of the options considered by Treasury under which the Privacy Safeguards in the CDR Bill would operate in parallel with the APPs and the Privacy Act. This is also important given the APPs apply to individuals but the CDR Bill applies to both individuals and entities.

Under this option the principle of *Lex Specialis* would apply so that a law governing a specific subject matter (*lex specialis*) would override a law governing only general matters (*lex generalis*). Where a Privacy Safeguard was more restrictive and specific, it would take precedence over an equivalent or general requirement in an APP. However, the APPs, and individual's privacy rights, would not be retracted, or made exempt (see exempt issue below).

The APPs reflect individual rights to privacy, and should not be "switched off". Although many of the Privacy Safeguards replicate the APPs, there are differences between them. Importantly, the APP right to access has not been replicated as a privacy safeguard. Moreover, the "switch off" of privacy principles is unlike the relationship between the Payment Services Directive 2 and the General Data Protection Regulation.

Privacy and the Consumer Data Rules (Sections 56EC, 56EF and 56EG)

Section 56BB notes a number of matters to which consumer data rules may apply. This includes, inter alia, matters related to privacy such as disclosure and use of CDR data. Other important rules and requirements for the Privacy Safeguards which would need to be drawn out in the Consumer Data Rules include clarifying what constitutes 'valid consent', and the right to access (rather than it being a Privacy Safeguard).

[22] Exposure Draft Explanatory Materials, paragraph 1.168, page 33
[23] Exposure Draft Explanatory Materials, paragraph 1.169, page 33

Issues that will need to be considered in the Consumer Data Rules include:

- Restrictions on the handling of CDR data which is designated as sensitive information
- Time qualifications for responding to solicited and unsolicited receipt for CDR data under Sections 56EF and 56EG
- Permissible uses and disclosures, and how an accredited data recipient may use CDR data for secondary, linked or compatible purposes[24]
- The rights and protections of other individuals before access, use, disclosure, or deletion of CDR data related to an identifiable or reasonably identifiable individual occurs.

The rights and protections of other individuals should be recognised in the CDR Bill before access, use, disclosure, or deletion of CDR data related to an identifiable or reasonably identifiable individual occurs.

This is important where multiple identified individuals are contained in a data set. It is important that the rights and protections of all relevant individuals are maintained, not just the rights of identified CDR consumers.

Privacy safeguard 1 - Open and transparent management of CDR data (Section 56ED)

It is beneficial that the CDR Bill mirrors APP 1 by extending open and transparent behaviours to the way CDR data is managed. An exception is that an accredited data recipient does not need to include in its CDR policy information about how it collects CDR data, only how it is held. (Subsection 56ED (5)(a)).

The inclusion in an accredited data recipient's CDR policy of information about how CDR data is collected could allow CDR consumers to better understand how accredited data recipients collect CDR consumers' personal information from designated data holders.

Privacy safeguard 6 - Use or disclosure of CDR data (Section 56EI)

Section 56EI allows the disclosure of CDR data where that disclosure is required or authorised under Australian law in addition to where the disclosure is required or authorised under the consumer data rules.

The Explanatory Memorandum states: *"It is not the intention that the CDR privacy safeguards restrict the ability of data holders to disclose CDR data outside of the CDR system where the disclosure is required or authorised under law, including under the Privacy Act"*.[25]

While implicitly recognising that certain uses and disclosures of personal information under the Privacy Act would be permissible, Section 56EI specifically does NOT allow the disclosure of CDR data where that disclosure is authorised under the APPs (subsection 56EI(1)(b)(i)).

We believe that this exception is appropriate given that the APPs permit broad uses and disclosures of personal information, including for direct marketing and secondary related purposes. The permitted uses and disclosures of personal information under the APPs are broader than the permitted uses of CDR data under the CDR Bill.

This section also appropriately allows the Office of the Australian Information Commissioner (OAIC) to make legally binding rules and guidelines applicable to specific types of CDR data sets where lawfully permitted under the Privacy Act outside of the APPs.

[24] The Farrell Report included the concept of a secondary purpose for the use of data that a customer 'would reasonably have expected their information to be used for' (Farrell Report (2017), op. cit., page 56

[25] Exposure Draft Explanatory Materials, paragraph 1.198, page 38

Privacy safeguard 8 - Cross-border disclosure of CDR data (Section 56EK)

Section 56EK requires CDR participants to only disclose CDR data to a non-Australian entity if that non-Australian entity is an accredited Data Recipient or meets conditions specified in the consumer data rules.

Some of the entities to which the CDR Bill will apply will have non-Australian subsidiaries as part of their group structure.

We recommend that the CDR Bill clarify the extent to which each legal entity controlled by an Australian-based entity is required to separately be accredited as a CDR participant.

This question of separate accreditation as CDR participants would also apply to other Australian-based entities controlled by an Australian-based entity.

Privacy safeguard 10 - Quality of CDR data (Section 56EM)

One of the potential challenges a Data Recipient will face is identifying and rectifying inconsistencies and errors detected within data received, particularly where it has been received from multiple Data Holders.

As a CDR participant, a Data Recipient 'must take reasonable steps to ensure that the CDR data is, having regards to the purpose for which it is held, accurate, up-to-date and complete' when the data is used (subsection 56EM(1)).

We recommend that the Rules and Standards for each sector provide clarification of the responsibilities of a Data Recipient for:

- matching, merging and de-duplicating data received from different Data Holders
- identifying and rectifying inconsistencies and errors within CDR data received
- ensuring that the CDR data received is appropriate for its intended use.

As a CDR participant, a Data Holder 'must take reasonable steps to ensure that the CDR data is, having regards to the purpose for which it is held, accurate, up-to-date and complete' when the data is disclosed (subsection 56EM(1)).

If a Data Holder later 'would reasonably be expected to be aware that some or all of the CDR data was incorrect because, having regard to the purpose for which it was held, it was inaccurate, out of date, incomplete or irrelevant' the Data Holder is required to advise the CDR consumer. (subsection 56EM(2)).

Customer-related data is likely to include a point in time at which it was received or last validated. Transaction or usage data is likely to include a time period to which it relates. As a result it is not clear why the CDR Bill would require that the CDR data is 'up-to-date' or to make a subjective assessment of whether data is 'out of date'.

We recommend that the references to 'up-to-date' and 'out of date' be removed and that instead a Data Holder should be required to disclose the time period applicable to the CDR data which is shared.

In addition Subsection 56EM(1) requires CDR participants, which includes both Data Holders and Data Recipients, to take reasonable steps to ensure CDR data is accurate, up-to-date and complete '…having regards to the purpose for which [CDR data] is ***held***…' (emphasis added). However the actions of certain Data Recipients may not involve 'holding' CDR data, but only 'receiving' or 'using' the CDR data.

We recommend that the language in subsection 56EM(1) be reviewed to ensure it adequately captures all of the potential actions of CDR participants including 'receiving' and 'using' CDR data as well as 'holding' CDR data.

Privacy Safeguard 12 - Correction of CDR data (Section 56EO)

An organisation must respond to a request from a CDR consumer to correct CDR data by taking such steps as are specified in the Consumer Data Rules. One of the permitted responses by a Data Holder is giving notice to a CDR consumer of why a correction is 'unnecessary or inappropriate' (subsection 56EO(2)(b)).

We recommend that the CDR Bill provide clarity on what 'unnecessary' and 'inappropriate' mean.

In addition we recommend that Section 56EO include a time frame within which a data holder is required to respond to a request from a CDR consumer to correct data, and a time frame for notifying other parties of the correction.

Compliance with Privacy Safeguards (Section 56EP)

Under the Privacy Act the OAIC is responsible for the development of legally binding guidelines and rules.[26] Although it includes privacy safeguards, Section 56EP does not provide the OAIC with the authority to develop rules or legislative binding guidance in relation to the consumer data right.

We recommend that the CDR Bill provide the OAIC with the authority to develop rules or legislative binding guidance in relation to the Consumer Data Right. This will be particularly important if the Privacy Safeguards in the CDR Bill replace the APPs and the Privacy Act for a designated sector.

Penalties (Section 56ET)

The penalty rates for breach of the Privacy Safeguards (1000 to 2000 penalty units) are lower than penalties applicable under the Australian Privacy Principles, given there is no increased maximum amount for serious and repeated offences (5 times the 2000 penalty limit).[27] This detracts from the importance of the Privacy Safeguards, which are intended to provide higher protections than the APPs.

We recommend that the penalty regime for breaches of Privacy Safeguards under the CDR Bill and for breaches of APPs under the Privacy Act be aligned.

Exemptions (Section 56GD)

The Commission may exempt a person or a class of persons or a data set or class of data from all of the specified provisions of the CDR regime under Section 56GD. The explanatory memorandum notes that the purpose of this section is to "*ensure that the CDR system does not operate in an unintended or perverse way in exceptional circumstances. They provide the ACCC with scope to ensure that the CDR system works in the best way possible for consumers and designated industry.*"[28]

The exemption appears to be too broad, particularly as it applies to Privacy Safeguards. It is not clear why the Commission would require this power. And if this power is required, to the extent to which it applies to the Privacy Safeguards it would appear to be more appropriate that this exemption power be exercised by the OAIC.

We recommend that the wording of this section be reviewed.

---

[26] Refer https://www.oaic.gov.au/agencies-and-organisations/legally-binding-guidelines-and-rules/

[27] Privacy Act, Section 80W.

[28] Exposure Draft Explanatory Materials, paragraph 1.263, page 47

Interaction of CDR Bill with other financial services legislation

Financial Crime – Identity Verification

One of the matters that is not included in the CDR Bill is the sharing of information about the outcomes of identity verification.

The *Anti-Money Laundering and Counter-Terrorism Financing Act 2006* (AML/CTF Act) allows entities required to report under AML/CTF Act to apply a risk-based approach to identifying, mitigating and managing financial crime risk. In essence, this requires a tiered approach to the identification and verification of both customer identity and commercial profiles.

The Farrell Report highlighted the possibility of amendments to the AML/CTF Act to facilitate the sharing of standard Know-Your-Customer (KYC) information, principally the minimum identification and verification standards of specified entity types in Part 4 of the AML/CTF Rules Instrument 2007 (No.1).

The Farrell Report noted that "*granting customers the right to instruct their bank to share the result of an identity verification assessment performed on them could improve efficiencies in the system".* However, it cautioned that *"obtaining access to the supporting documents provided by an individual as part of an identity verification is one of the most common methods of identity theft."*[29]

However, while minimum KYC standards are formally defined and therefore commoditised in terms of data definition and sharing, the majority of AML/CTF legislative obligations are 'risk-based'. This in turn leads to broad and differing standards of data to be collected by individual financial institutions to manage their assessment of the risk and enable the operation of appropriate controls to mitigate and manage that risk. Under this risk-based approach, there is significant market divergence in terms of defining and collecting required data on customers.

In its submission to the Farrell Report, the Australian Energy Council noted the importance of identity verification in the application of open data to other sectors. Its submission stated that:

> *One of the obstacles to third party access is the difficulty of verifying the customer's identity and their consent to the disclosure. As Energy Consumers Australia (ECA) has pointed out, arrangements for third party access are made more problematic by different market participants adopting different verification and consent requirements.*[30]

The Farrell Report recommended that *"If directed by the customer to do so, data holders should be obliged to share the outcome of an identity verification assessment performed on the customer, provided the anti-money laundering laws are amended to allow data recipients to rely on that outcome"*.[31]

We are aware that there are pending reforms proposed for the AML/CTF Act. The alignment of the AML/CTF Act to the open banking legislative framework will be important to achieve the objectives of open data without compromising identity verification.

In Deloitte's view, the CDR must be flexible enough to allow sharing of customer data beyond stated minimum standards if the open banking regime is to provide the requisite flexibility to meet the fluid and risk-based obligations imposed on impacted entities under the AML/CTF Act. Failure to adopt this flexibility on customer data will, in our view, limit the utility of the open banking regime by obligating impacted entities to significantly duplicate collection and verification of information on customers seeking the flexibility of open banking.

---

[29] Farrell Report (2017), op. cit., page 38

[30] Australian Energy Council, Open Banking and the implementation of the Consumer Data Right: Implications for energy sector, 23 March 2018. See also: https://treasury.gov.au/consultation/c2018-t247313/ :

[31] Farrell Report (2017), op. cit., Recommendation 3.4, page 39

We recommend that the government implement a legislative model that allows a recipient to rely on another entity's identity verification (subject to safeguards) in conjunction with the CDR Bill. This would enhance the confidence of consumers and potential third parties in the identity of the parties with which they are interacting in an open data environment.

Financial Crime – Suspicious Matter Reporting

Currently reporting entities under the AML/CTF Act are required to submit a Suspicious Matter Report (SMR) to AUSTRAC if, at any time while dealing with a customer, the entity forms a suspicion on a matter that may be related to an offence, tax evasion or proceeds of crime.

The sharing of customer transaction data between entities under open banking has the potential to result in a significant increase in the amount of data acquired or held in relation to a particular customer, both by individual entities that take advantage of open banking data sharing, and across the platform. In these circumstances a matter may only become suspicious, and therefore reportable, when considering the combined data about a customer.

However, the SMR reporting obligation could become challenging for reporting entities in the context of the CDR Rules and Standards. These enable a customer to specify a limited purpose for which a data recipient can use customer transaction information that has been shared with it. This conceivably creates the potential for a conflict between complying with the CDR legislation and Rules and complying with reporting and risk management obligations under the AML/CTF Act.

In addition, SMRs are subject to the legal restrictions on 'tipping off', whereby reporting entities are prohibited from disclosing outside of the organisation certain information about a SMR. Concerns by reporting entities under the AML/CTF Act about potentially breaching this obligation could be a constraint to the sharing of some customer information.

The CDR Bill includes a section stating that in the event of an inconsistency between the privacy safeguards and the consumer data rules, those safeguards prevail (Section 56EC).

The CDR Bill could also include a section stating that in the event of an inconsistency between the CDR Bill and other legislation applying to the sector, the other legislation applying to the sector should prevail.

Consideration could also be given to amending the AML/CTF Act to clarify how it should operate in relation to third-party data about a customer which has been shared under CDR legislation with an entity required to report under AML/CTF Act.

Conduct

Credit licensees must comply with the responsible lending conduct obligations. These are set out in Regulatory Guide 209 Credit Licensing: Responsible Lending Conduct (RG209), Chapter 3 of the *National Consumer Credit Protection Act 2009* (the National Credit Act) and the consumer protection provisions in the *Australian Securities and Investments Commission Act 2001* (Part 2, Division 2).

The responsible lending obligations apply when[32]:

(a) if you are a credit assistance provider—you:
  (i) suggest that the consumer apply, or assist the consumer to apply, for a particular credit contract or consumer lease;
  (ii) suggest that the consumer apply, or assist the consumer to apply, for an increase to the credit limit on an existing credit contract; or
  (iii) suggest that the consumer remains in an existing credit contract or consumer lease; or
(b) if you are a credit provider or lessor—you:

[32] RG209.5

(i) enter into a credit contract or consumer lease with the consumer;
(ii) increase the credit limit on an existing credit contract or
(iii) make an unconditional representation to a consumer that you consider that they are eligible to enter into a credit contract or consumer lease with you, or that the credit limit of an existing credit contract with you will be able to be increased.

The responsible lending obligations do not just apply to new credit contracts:

> *"…the obligations also apply when you are considering whether to increase a credit limit under an existing credit contract (if you are a credit provider) or when you are providing credit assistance in relation to an existing credit contract or consumer lease by suggesting that the consumer remains in the contract, suggesting that the consumer applies for an increased credit limit, or assisting the consumer to apply for an increased credit limit. If credit assistance is provided, the responsible lending obligations must be complied with even if the consumer does not subsequently enter into the credit contract or consumer lease."*[33]

Under RG209 credit licensees – credit assistance providers and credit providers – must not enter into a credit contract with a consumer, suggest a credit contract to a consumer or assist a consumer to apply for a credit contract if the credit contract is unsuitable for the consumer. Credit providers are required to make a final assessment about whether the credit contract is ***'not unsuitable'*** for the consumer.[34]

Credit licensees are also required to have appropriate systems and processes to identify whether a proposed credit contract or consumer lease is likely to cause ***substantial hardship*** to a consumer.[35]

The sharing of customer transaction data between entities under open banking has the potential to result in a significant increase in the amount of data acquired or held in relation to a particular customer.

As a result of the information about a customer that has been shared by a third party, a credit licensee may:

- where a credit facility was originally assessed as 'not unsuitable' for a customer, form a view based on the additional information received, and subsequent to the initial assessment, that a credit facility is no longer 'not unsuitable' for a customer (ie that it is in fact unsuitable)
- where a customer was not assessed as being in 'substantial hardship', form a view based on the additional information received, and subsequent to the initial assessment, that a person with a credit facility is subject to 'substantial hardship'.

In addition, the CDR Rules and Standards for a sector may enable a customer to specify a limited purpose for which a data recipient can use customer transaction information that has been shared with it. This conceivably creates the potential for a conflict between complying with the CDR legislation and rules and complying with the Credit Act.

Consideration could also be given to amending the National Credit Act to clarify how it should operate in relation to information shared as a result of the CDR legislation.

[33] Regulatory Guide 209, Credit Licensing: Responsible Lending Conduct (RG209), RG209.6
[34] RG209.2
[35] RG209.102

Application of CDR Bill to non-financial services sectors

Application to energy sector

In February 2018, the Department of Environment and Energy on released a draft report prepared for the Council of Australian Governments (COAG) Energy Council *Facilitating access to consumer electricity data* (the HoustonKemp Report).[36]

The purpose of the HoustonKemp Report was to examine how, and make recommendations for, streamlining the process, and facilitating timely access to consumers' electricity consumption data by authorised third party service providers. The HoustonKemp Report referred to this as a consumers' electricity data access framework for authorised third parties (electricity data access framework). This report did not address access to consumer data relating to other energy sources such as gas.

The HoustonKemp Report proposed that the Australian Electricity Market Operator (AEMO) develop its preferred accreditation framework for the electricity sector, with the ACCC certifying it to be consistent with the legislative framework (i.e. the CDR Bill) and subsequent rules framework to provide consistency across sectors.

The Energy Council has also noted that it supports the development of a Consumer Data Right in the energy sector.

We recommend that the CDR Bill clarify how the ACCC and other regulators, such as AMEO, would work together.

It will also be important that the definitions of CDR consumers, CDR data, data holders and accredited data recipients enable the application of the CDR Bill to the energy sector and address matters such as:

- the identity of a contracted customer
- users of energy services where these differ from the contracted customer
- the application of the CDR Bill to data holders which are entities owned or controlled by a state government
- the application of the CDR Bill to data recipients which are entities owned or controlled by a state government, such as price comparison websites
- the interaction of the CDR Bill with existing regulatory frameworks such as the National Energy Retail Rules (NERR).

Application to telecommunication sector

The explanatory memorandum notes that the Government has committed that the telecommunication sector (along with the energy sector) will be subject to the CDR.[37]

We recommend that the CDR Bill clarify how the ACCC and other regulators would work together. For the telecommunications sector this would include the Australian Communications and Media Authority (ACMA), the Telecommunications Industry Ombudsman (TIO), and the Commonwealth Ombudsman.

[36] HoustonKemp, Facilitating access to consumer electricity data: A draft report for the Department of Environment and Energy, February 2018. See also: http://www.coagenergycouncil.gov.au/publications/call-submissions-facilitating-access-consumer-energy-data
[37] Exposure Draft Explanatory Materials, paragraph 1.14, page 5

It will be important that the definitions of CDR consumers, CDR data, data holders and accredited data recipients enable the application of the CDR Bill to the telecommunication sector and address matters such as:

- what data will be included in CDR data, including the extent of any derived data or aggregated data, particularly in an environment where there are a significant number of entities whose business model is based on value derived from consumer data
- the interaction of the CDR Bill with existing regulatory frameworks such as the Telecommunications Interception and Access Amendment (Data Retention) legislation
- the application of the CDR Bill to data holders around the identity of an account holder or service owner where multiple parties are involved in service provision (wholesaler / retailer providers)
- owners of telecommunication services where these differ from the account holder
- the application of the CDR Bill to consumers who have granted full authority or limited authority to another person or a third party
- the application of the CDR Bill to data holders which are entities owned or controlled by a state government
- the application of the CDR Bill to data holders who are foreign entities involved in the provision of service in support of global roaming when consumers are travelling internationally
- the application of the CDR Bill to data recipients which are entities owned or controlled by a state government, such as price comparison websites

Application to Public Sector

In its response to the Productivity Commission's *Data Availability and Use Inquiry* (PC Inquiry report), in addition to introducing a Consumer Data Right which is the subject of the CDR Bill, the Australian government committed to:[38]

- Establishing a **National Data Commissioner** (NDC) to implement and oversee an efficient data sharing and release framework
- Introducing legislation to improve the sharing, use and reuse of public sector data

In July 2017, the Department of the Prime Minister and Cabinet released an issues paper for consultation *New Australian Government: Data Sharing and Release Legislation* (Issues Paper).

The purpose of the issues paper was to seek feedback on initiatives to promote greater use and sharing of public data and the proposed Data Sharing and Release Bill (DS&R Bill).

The Issues paper has noted that the NDC will work closely with the OAIC in relation to privacy considerations. However the CDR Bill does not discuss the relationship that the ACCC would have with the NDC in the operation of data sharing and the Consumer Data Right.

We recommend that the CDR Bill clarify how the ACCC and other regulators, such as the NDC, would work together. This will be particularly important where public sector entities are providing products and services in sectors which have been designated under the CDR legislation.

[38] Australian Government, Issues paper: New Australian Government Data Sharing and Release Legislation, July 2018. See also: https://www.pmc.gov.au/resource-centre/public-data/issues-paper-data-sharing-release-legislation

Application to State entities

In December 2015 the Commonwealth released the *Public Sector Data Management Report*.[39] This was followed in July 2016 by the *Public Sector Data Management: Implementation Report*.[40] Consultations are currently in train on the application of the report to the Australian Public Service (APS).

The CDR Bill does not appear to extend to public sector entities including state public sector entities, however public sector entities operate as data holders and potential data recipients in sectors that could be designated under the CDR Bill.

To help build citizen and consumer confidence in data sharing, we recommend that the CDR Bill review the alignment between the CDR and public sector data management of principles and policies for data rights, data sharing and privacy.

[39] The Australian Government, Department of the Prime Minister and Cabinet, Public Sector Data Management, July 2015. See also: https://www.pmc.gov.au/sites/default/files/publications/public_sector_data_mgt_project.pdf

[40] The Australian Government, Department of the Prime Minister and Cabinet, Public Sector Data Management: Implementation Report, July 2016. See also: https://www.pmc.gov.au/sites/default/files/publications/Implementation-Public-Sector-Data-Management-Report_0.pdf

Contact us

John O'Mahoney
Partner, Deloitte Access Economics
+61 2 9322 7877
joomahony@deloitte.com.au

Paul Wiebusch
Partner, Financial Services
+61 3 9671 7080
pwiebusch@deloitte.com.au

Simon Pelletier
Partner, Strategy
+61 2 8260 4184
sipelletier@deloitte.com.au

Michael Thomas
Director, Deloitte Access Economics
+61 2 9322 7145
michaelthomas@deloitte.com.au

Melissa Ferrer
Partner, Data
+61 2 9322 7844
meferrer@deloitte.com.au

Jonathan Benson
Director, Data
+61 3 9671 8576
jobenson@deloitte.com.au

Tommy Viljoen
Partner, Privacy
+61 2 9322 7713
tfviljoen@deloitte.com.au

Ilana Singer
Manager, Privacy
+61 3 9671 5475
isinger@deloitte.com.au

Alex Lord
Partner, Conduct
+61 3 9671 6339
allord@deloitte.com.au

Paul Rehder
National Leader, Banking
+61 3 9671 8058
prehder@deloitte.com.au

Michael Rath
National Leader, Energy & Resources
+61 3 9671 6465
mrath@deloitte.com.au

Kimberley Chang
National Leader, Telecommunications
+61 2 9322 3233
kimbchang@deloitte.com.au

Ellen Derrick
National Leader, Public Sector
+61 2 6263 7069
ederrick@deloitte.com.au

Deloitte.