Business Council of Australia

SUBMISSION

Submission to the ACCC on the Consumer Data Right draft rules consultation

May 2019

Business Council of Australia ABN 75 008 483 216

ABOUT THIS SUBMISSION

The Business Council welcomes the opportunity to comment on the Australian Competition and Consumer Commission's *Competition and Consumer (Consumer Data) Rules 2019 (Exposure Draft).* This submission provides a consolidated response from Business Council member companies to the Exposure Draft.

BACKGROUND

- The ACCC is consulting on its draft consumer data right rules for the banking sector, with the energy sector and other sectors to follow.
- The successful implementation of the Consumer Data Right (CDR) framework overall will require consumers to trust that their data will be safe, secure and put to good use should they exercise their rights under the scheme.
- For trust to be maintained, all parties - regulators, industry (data holders and Accredited Data Recipients), and any designated gateways - need to clearly understand their obligations, be fully prepared in terms of systems and processes, and demonstrate they can work together to protect consumers' privacy.
- The CDR framework legislation was introduced to Parliament in February, but with the Federal Election being held on 18 May, the Treasury Laws Amendment (Consumer Data Right) Bill 2019 has lapsed. The final form of the rules is dependent on the passage of the framework legislation through parliament.

ISSUES

1. General concerns

- The framework is complicated and needs to be more user-friendly and easier to apply to reduce the risk of unintended breaches occurring. There is a concern about the need for stakeholders to cross-reference multiple documents to understand how the entire CDR framework will work in practice.
- CDR implementation timelines should be reconsidered if there is any doubt about the preparedness of industry or government regulators to implement the CDR policy initiative – including due to clarity of requirements, and preparedness of systems and process.
- There is concern that this consultation – which is considering the general rules and the banking specific rules (in the Schedule) – is predominantly considering the framing of the general rules in the context of the banking sector and is not sufficiently considering other sectors to which they will also apply. Future sectoral consultations should not only include the draft Schedule for that sector but also the application of the general rules to that sector. Otherwise, there could be flaws in the CDR regime to the detriment of businesses and consumers in each sector (see below for concerns with regard to the energy sector).

- Some crucial aspects of the CDR regime have been deferred to the ACCC to address in the Rules that would be better addressed in the Bill, for example, privacy and data definition – notwithstanding that the Bill was amended to ensure that there was regulatory rigour around the ACCC's consultation requirements to address stakeholder concerns.

2. Sectoral concerns

- While the initial focus on the banking sector is understood, there is concern from companies outside the banking sector about whether there will be a similar level of focus and engagement on issues in their sectors when the time comes to extend the implementation of the CDR.

- For instance, it is not clear whether the banking rules will be extended to the energy and telecommunication sectors through a schedule, or through separate rules and consultation. If the intention is that this exposure draft will be extended to other sectors with the addition of a schedule, members are concerned that:
  - There will be insufficient consultation and rule setting to address energy and telecommunication sector matters. The banking sector rules are specific to banking's economy wide model, and there is insufficient analysis of the appropriateness of these rules in different sectors. This is important particularly where the ACCC is still considering what data access model is appropriate for the energy sector and will therefore have impacts on the relevancy of general rules.
  - Regulatory Guide 165 under Part 6 (relating to internal dispute resolution) is referenced in the 'general rules', but this is not something that is required in other sectors such as energy. Reference to ASIC's Regulatory Guide 165 should either be included in the relevant industry specific schedule or alternatively, the general rules should require data holders and accredited data recipients to meet more general requirements (such as *AS/NZS 10002:2014 Guidelines for complaint management in organizations*).
  - The layering and frequency of express consent is potentially too onerous for the energy sector and could be burdensome for customers.
  - Other decisions made under the banking rules that may raise key questions for the energy sector and which will need further exploration include: Will there be restrictions on whether an energy retailer can be an Accredited Data Recipient? Will customers will be able to request data directly from data holders in the energy sector (especially if a centralised model is chosen)?

- There are a number of instances in the general rules that refer to 'compliance with the data standards'.
  - Compliance with technical standards was always positioned and expected to encompass the Application Programming Interface (API) and security requirements for CDR participant interactions. To-date these have focused only on the banking experience and consultation with businesses outside the banking sector ceased in December 2018.

3. Privacy

- Instead of the privacy requirements being duplicated in the rules (which might lead to inconsistent application), the privacy requirements should be in the Bill and harmonised with centralised privacy requirements.

- The 'general rules' should be consulted on more broadly, and be accompanied by a Privacy Impact Assessment (PIA) to explain why the ACCC consider departures from existing Privacy Act requirements is necessary

- One suggested approach to addressing interaction with existing privacy laws would involve the Australian Privacy Principles (APPs) being 'turned off' and replaced with the Privacy Safeguards. If the current approach is to be retained then there should be clear direction in the Rules regarding the transition from the Privacy Safeguards to APPs. There should also be a recognition that many data holders may choose to be accredited data recipients, and distinctions between safeguards and APP application between the two participants will increasingly become redundant.

- Some requirements of businesses under the general rules are more onerous than current requirements under the Privacy Laws, and it is not clear why this is the case.
  - For example, under the Australian Privacy Principles a body must take reasonable steps to correct information if a consumer requests it – but such requests can be refused. If the request is refused and an individual then requests a record or appended statement to be attached to their information then this must be done within 30 days.
  - Under the draft Rules, this appended statement must be done within 10 days. There is no explanation or information as to why a 10-day period was deemed appropriate or necessary.

- There is concern that the 24-hour timeframe for informing the ACCC for refusal of access to CDR data is onerous and impractical. For example, what happens if the refusal occurs outside business hours or on the weekend? There is no explanation or information as to why 24 hours was deemed the appropriate period. A longer timeframe may be warranted, consistent with other privacy laws.

4. Concerns with specific rules

Concerns in relation to specific aspects of the Exposure Draft:

- The approach to joint account consents in the draft Rules significantly differs from the previous approach, adds technical complexity and may lead to customer frustration. Joint accounts should therefore be excluded from Phase 1 to allow the technical issues to be considered and for further consideration of user experience and appropriate customer education with respect to joint accounts.

- Regarding the rules governing the outsourcing of data by an Accredited Data Recipient outsource to a non-accredited service provider: to reduce privacy and security risks, when a customer wishes to have CDR data directed to a non-accredited person, such as a lawyer or accountant, it is recommended that the ADR or data holder should provide the data to the customer for them to pass on, rather than provide the data directly to the non-accredited person.

- The adoption of a customised Security Management framework does not include a mechanism for monitoring or updating the framework to address new security threats. A possible solution is the adoption of an industry-accepted framework for Security Management in consultation with each relevant sector.

- In relation to Draft rule 1.8(1), the reference to CDR data should be limited to clarify that the CDR data of that particular consumer is intended to be caught. In banking, the reference to 'another person' is also unduly broad and should be limited. It gives rise to uncertainty around the status of the 'other person' under additional requirements (e.g. the consumer dashboard obligations under Subdivision 1.4.3 of the rules).
  - However in the energy sector, questions remain around how the CDR regime will be applied and whether CDR data will be generated at a household/entity level or an individual/account holder level. The potential impacts of the term 'another person' for energy cannot be fully understood until more information is available, particularly where persons may be an 'authorised representative' on the account (e.g. a spouse or roommate who also generates CDR energy data).

- The Exposure Draft does not appear to include a framework for reciprocal obligations, as envisaged by the Open Banking Review. Reciprocity is important to promote innovation and to maximise the benefits of the CDR regime for consumers. The inclusion of reciprocity in Phase 1 is generally supported, even if it is in a limited form.
  - the Accreditation process at rule 5.2 of the Rules requires persons applying for accreditation to self-indicate 'whether it is or expects to be the data holder of any CDR data that is specified in a designation instrument.' It is recommended that the Accreditor be required to make reasonable enquires as to the data that a prospective data recipient holds at the time of accreditation to determine whether reciprocal obligations apply.

5. Areas requiring more clarity

Concerns in relation to a lack of clarity in the rules:

- Under draft rule 3.5, it is not clear whether a refusal to disclose CDR data due to fraud would amount to a refusal under the rules. For some companies in the banking sector a 24-hour notification in these instances could create a significant burden.
- Draft rule 7.6 outlines what needs to be updated in the consumer dashboard following a CDR data disclosure. In its current form it is unclear how much detail must be provided regarding disclosure (i.e. does it need to state every API call)?
- It Is not clear whether cross-sector access is intended to apply (i.e. banking can access energy data, and vice versa), and at what stage this would apply, noting the privacy implications could be significant.
- It appears accreditation is done on an individual level. If an individual loses accreditation, would that mean the business that employs the individual loses accreditation, or can there be a replacement accredited individual?
- In relation to the ACCC's intended approach to disclosure to non-accredited recipients, more clarity is needed to understand what amounts to 'derived data' and what amounts to 'materially enhanced data'.

- The Exposure Draft is silent on hosting of CDR in a cloud or shared environment. This is a concern to some companies, whose usage of cloud solutions is being closely monitored by the Australian Prudential Regulation Authority (APRA).
- The Exposure Draft is silent on the legal authority needed for authorisation in particular circumstances (e.g. powers of attorney, payroll and multi-party ownership).
- The Exposure Draft does not provide information on the instances where a fee can be imposed in relation to a CDR request.
- Consumer testing is important for the customer experience, but is not addressed in the Exposure Draft, with the only reference being that the data standards must be subject to such consumer testing as the Data Standards Chair considers appropriate (Rule 8.11(3)).
  - The ACCC is able to make rules about the data standards body, including how it must consult. ACCC Rules in this area would help to ensure appropriate governance and stakeholder engagement.

BUSINESS COUNCIL OF AUSTRALIA
42/120 Collins Street Melbourne 3000 T 03 8664 2664 F 03 8664 2666 www.bca.com.au