AUSTRALIAN ENERGY COUNCIL

Bruce Cooper
General Manager, Consumer Data Right Branch
Australian Competition & Consumer Commission

Lodged by email: ACCC-CDR@accc.gov.au

10 May 2019

Consumer Data Right Draft Rules Consultation – Exposure Draft CDR Rules

The Australian Energy Council ('AEC') welcomes the opportunity to make a submission to the ACCC on the *Competition and Consumer (Consumer Data) Rules 2019 Exposure Draft* ('CDR Draft Rules').

The AEC is the industry body representing 23 electricity and downstream natural gas businesses operating in the competitive wholesale and retail energy markets. These businesses collectively generate the overwhelming majority of electricity in Australia and sell gas and electricity to over 10 million homes and businesses.

The AEC continues to support introducing a Consumer Data Right ('CDR') into the energy sector and wider economy. We consider it has the potential to enhance competition in the retail market and provide better outcomes for consumers. But, this potential will only be realised if the CDR Draft Rules are tailored around the unique characteristics of each sector.

The AEC is concerned then that the CDR Draft Rules, purported by the ACCC to merely relate to banking, appear to have been drafted in a manner that would enable the rules to be implemented more generally, with specific industry provisions limited to those in the Schedules. It would be unacceptable for the application of these Draft Rules to be applied to the energy sector without extensive consultation first taking place. To avoid this outcome, we encourage the ACCC to rename the Exposure Draft as the *Competition and Consumer (Consumer Data - Banking) Rules 2019*.

The AEC would be comfortable with the banking rules, once determined, acting as a starting point for developing the rules for the energy sector. Where appropriate – and only after robust and extensive consultation – the provisions should be aligned to avoid process duplication between sectors.

Proceeding to implement these rules without first identifying their specific impacts on the energy market risks exposing energy consumers and businesses to unintended consequences and thereby undermining the effectiveness of the CDR regime.

With this concern front of mind, this submission intends to provide high-level comments on the CDR Draft Rules for banking, and highlights some difficulties that might emerge if implemented into the energy sector in its current state.

Consultation Issues

Structure of CDR Exposure Draft

The CDR Draft Rules appear intended to operate through two sections. The first section, covering Part 1 to Part 9, reads as a general set of rules that would apply to all sectors. The second section, known as the Schedules, appears to provide sector-specific applications of the general rules.

Level 14, 50 Market Street
Melbourne 3000
GPO Box 1823 Melbourne Victoria 3001

P +61 3 9205 3100
E info@energycouncil.com.au
W energycouncil.com.au

ABN 98 052 416 083

We strongly suggest the ACCC clarify this issue formally or in writing prior to continuing with this process.

The general rules are built upon consultation with the banking sector, namely the Productivity Commission report and Open Banking review. Consultation with the energy sector (and other sectors) has been less extensive, and remains ongoing. The AEC is concerned then that any general set of rules determined at this time could not properly take into account the different impacts on each sector.

Technical Issues

Notwithstanding the above concerns, the AEC wishes to make a number of comments regarding the current drafting of the CDR banking rules, in particular how they might need amendment prior to being considered in the future energy rules.

Disclosure to Non-Accredited Parties
Under rule 7.5, the ACCC states it is considering whether to authorise disclosure of customer data to a person that is not accredited (such as a customer's accountant or lawyer) if the customer gives consent. This possibility, if realised, raises a number of security and privacy concerns that the ACCC should take into account. For example:

- What privacy provisions will non-accredited persons be subject to?
- How will the ACCC address the potential power imbalance between the accredited party, non-accredited person and the consumer to the extent that it impacts on customer consent?
- If the non-accredited person is the customer's lawyer, how will the ACCC regulate, if at all, requests from other legal persons to access that data?

24-Hour Requirement Rule (Rules 3.5 and 4.7)
Rules 3.5(2) and 4.7(2) require the data holder to inform the Commission of its reasons for refusing to fulfill a CDR request within 24 hours. The AEC seeks clarification as to why the ACCC has chosen to enforce a 24 hour time limit on data holders. An obligation of this nature would be onerous, for questionable public benefit. It is likely that many data holders will approve consumer data requests through an automated system rather than employ someone to individually assess each claim with human judgment. This is necessary to ensure the CDR operates efficiently while also minimising compliance costs. It also means though that, if a request is rejected, it may be impractical for the data holder to respond within 24 hours. Data holders will require time to identify that a request has been rejected and then perform information-gathering exercises to determine why. Such an exercise is time-consuming on its own, yet will be near impossible to do within 24 hours if the refusal occurred outside business hours (such as the weekend or late at night). With this in mind, the AEC believes it would be more appropriate for this rule to be removed and data holders instead be audited on whether a refusal is valid (similar to the framework that governs explicit informed consent). Alternatively, a less prescriptive time frame should be adopted.

The AEC is also concerned that the grounds for rejecting a request are too narrow, which may cause unintended consequences. For example, a situation may emerge where data holders opt to err on the side of caution and approve all technically valid consumer data requests to avoid breaching the rules.

Privacy Provisions
Part 7 of the CDR Draft Rules outlines rules relating to privacy safeguards while Schedule 1 provides 'steps for privacy safeguard 12', which is contained in section 56EO(1) of the enabling legislation. Both these

provisions impose onerous obligations on data holders to protect the security of customer data. For example, the information security controls listed in rule 2.2 of Schedule 1 require a data holder to invest in expansive software protections including encryption services, firewalls, security patching and application whitelisting. This is in addition to staff undergoing police checks and being subject to security training every year.

While this level of protection might be necessary for the banking sector, where customer data is particularly sensitive, it is less apparent why such onerous requirements are needed to protect a customer's energy information. Such information is already protected under the NERL, which regulates how retailers are to manage customer data as well as giving customers the right to request access to their personal data. These provisions have worked effectively since being introduced so it is unclear why further, burdensome regulations are necessary. Imposing such requirements on retailers is only going to raise compliance costs, potentially increasing prices for consumers unnecessarily.

Consumer Responsibilities for Data

Part 3 lays out rules that gives a consumer the power to make a consumer data request directly to the data holder. These rules highlight the difficulty in determining rules that might apply to the energy sector prior to determining the data delivery model. If the energy sector's preferred data model – the gateway model – is selected, issues around authentication will emerge, namely:

- Will data holders be required to become an accredited data recipient so they can legally approve a consumer data request?
- Is AEMO responsible for authentication of the customer and, if so, will the customer operate through AEMO directly?

The ACCC should further clarify what responsibilities, if any, data holders have after approving a request to ensure the customer maintains their data in a way that protects their privacy and security. If there is a data breach, it is unclear what mechanisms are in place to trace that breach and prevent the data from further misuse.

The AEC are committed to working with the Government and the ACCC to implement a CDR that empowers consumers and improves their experience in the energy market.

Any questions about this submission should be addressed to Rhys Thomas, by email to [redacted] or by telephone on [redacted].

Yours sincerely,

Ben Barnes
Director Retail Policy
Australian Energy Council