Data Standards Body
c/o Data61
cdr-data61@csiro.au
22 March 2019

The Australian Competition and Consumer Commission
23 Marcus Clarke Street
GPO Box 3131
Canberra ACT 2601

Submitted electronically

Dear Commissioner Court

On behalf of the Consumer Data Right Interim Data Standards Body we would like to thank you and the ACCC for the opportunity to respond to your consultation paper on the matter of the economy-wide Consumer Data Right (**CDR**) for the Energy Sector. As you are no doubt aware Data61 is the interim technical adviser to the CDR's Data Standards Body (**DSB**). Mr Andrew Stevens was appointed by the Treasurer as Interim Data Standards Body Chair. Data61's dedicated Consumer Data Standards (**CDS**) team is overseen by Mr Warren Bradey and which provides technical advice to Mr Andrew Stevens. The DSB's Chair is also provided with industry and consumer advice by an Advisory Committee which comprises members from diverse industry and consumer groups, and government and regulatory observers.

The CDS team has been providing technical advice on the development of **API**[1] Standards, Information Security, and Consumer Experience (**CX**) guidelines for the CDR; to date this work has primarily focussed on the initial sector designated by the government. Our work over the last year has provided many learnings and insights into the practicalities of introducing an ability for consumers to have greater control over their data in the Australian context. The CDS team has established sound processes that will be further refined as the CDR continues to be implemented over multiple sectors.

At all times during the introduction of the CDR, the DSB has sought to maintain an open and transparent approach to the consultation and decision-making processes for the design of the technical standards, and provision of technical advice. The DSB team intends to continue this approach for the implementation in the Energy sector, and all subsequent sectors involved in the economy-wide CDR. This approach has included the use of Github to receive and publish all industry feedback on the standards development in an open and transparent manner, the holding of public workshops in Melbourne and Sydney, blog posts and the distribution of newsletters and email updates.

[1] **API** or Application Programming Interface. While there is no one distinct definition of an API, an API is essentially a piece of software that allows two applications to talk to each other; in the case of the CDR the applications in question belong to the accredited data recipient and the data holder. APIs are the standard mechanism for sharing information between software securely and efficiently. They enable interconnectivity between services, providing standardisable ways to access, interpret and present data on a server.

The DSB team has been operating to a set of open principles[2] that guide our work. These operating principles are fundamentally about ensuring our work directly supports the intended outcomes of the economy-wide CDR, as set out in the Farrell report and adopted by the government, which is to create value by improving the control, choice, convenience and confidence of consumers. This value is fundamentally created through innovation occurring inside a free market. The salient and over-arching principle is that our work is open and highly consultative. CDR standards are designed with extensive stakeholder engagement, and these standards are public and freely available.

The adoption of an economy-wide, interoperable approach is a key part of the strategic intent of the government for the CDR regime. The DSB has sought to facilitate this approach by establishing a common set of operating principles[3], to collaboratively establish technical standards for the exchange of consumer data that enables a general use case in order to provide value for consumers in the sector, and to connect the sector with Australia's new data market. This approach is clearly aligned with Treasury's implementation principles of being consumer focussed, encouraging competition, creating opportunity and being efficient and fair.

The DSB is ensuring that the simplest, most broadly applicable and most flexible standards as practical are being established. Potential future directions in terms of technologies and use-cases are also being considered in order to enable interoperability across sectors and support innovation for emerging business models, platforms and investment in Australia's new data market.

The DSB and CDS team looks forward to working with the ACCC, the OAIC, and the Treasury, in addition to all relevant industry, government and consumer stakeholders on continuing to introduce the economy-wide CDR. The establishment of sufficient baselines and standards for the technical operation of this right is paramount for the safety, security, and efficiency of consumer data, and ultimately for trust in Australia's new data market.

We have addressed the questions raised in the consultation paper below and would be happy to discuss them further and greater technical detail where that would be of assistance.

[2] See **Appendix A** for a list of the principles.

[3] Refer **Appendix A**

Question 1: Are there any other assessment criteria or relevant considerations which the ACCC should use to determine a preferred model for consumers to access their energy data under the CDR?

For all the data access models consideration should be given to the use of APIs; information security; the consumer experience (**CX**); and innovation. This consideration should be mindful of international, as well as national trends, standards and developments; as the intended outcome is a dynamic and flexible system able to anticipate and respond to change.

1. APIs

Under the CDR regime all Accredited Data Recipients (**ADRs**)[4] will need to be accredited by the ACCC and meet the CDR rules applied by the ACCC. As such all the data access model options proposed will require the ADRs to implement CDR APIs. This approach facilitates the standardised automatic transfer of data on a regular basis between computers (subject to explicit consumer consent) and enables more competitive access to new services than through other channels – such as via phone (which will not necessarily be de-activated under CDR).

Any designated gateways and/or data holders designated for each sector will similarly be required to implement CDR APIs to make them accessible by ADRs. As such any energy retailer would be expected to provide product data via CDR APIs (whether provided directly to customers or via a designated gateway). The implication is that it would be optimal for all participants to implement the same CDR standards, for all relevant datasets, in the event of the designation of any of the data access models and for the flexibility, to facilitate cross sector data transfers and to alter the data sets, should further decisions to expand the data and products applicable be made in the future by ACCC.

Version control of APIs is achieved through the standards published by the DSB, which are equally applicable to all data access models. Compliance with these standards will be maintained by the ACCC through ongoing accreditation, and the dynamic management of their directory.

2. Information Security

The pooling of personally identifiable information (**PII**) and consumption patterns as data at scale on one architecture / platform creates a highly attractive target for hackers; both foreign and domestic. Where new data sets of scale are established, appropriate and sufficient cyber security controls will be required.

[4] **ADR** Accredited Data Recipient. The CDR will apply to data holders who have information relevant to the designated sector – i.e. for banking, banks. Other participants can become accredited to receive information through the CDR system. A register of accredited participants will be maintained and accreditations can be revoked or suspended. Consumer data rules will be made about revocation and suspension of accreditations.

*Please note, this is NOT known as a '**honey pot**'.*[5] *A 'honey pot' is a detective control used for cyber security.*

The use of internationally recognised Information Security standards and protocols ensures that the data being transacted at the core of the system is designed in a commonly understood and safe way. Consistent use of these standards across the economy-wide CDR has additional benefits, such as a greater ability to detect malicious activity and other anomalies. The implementation of these standards for the transaction of CDR data is complementary to their implementation for the broader systems of the data recipients that store and analyse this data. Lowering standards for security in one sector by definition impacts all sectors in an economy-wide CDR.

Consequently it will be important to assess whether allowing different Information Security protocols to operate in the digital channel would weaken overall security where data is transferred between sectors. Consideration will need to be given as to whether adopting a lower standard in one sector would provide a back-door to access personally identifiable information (**PII**) in another sector.

3. Consumer Experience (CX)

If a data access model requires a consumer to interact with an entity that they have not previously had a relationship with, or a new way with an existing relationship, research will be required to ascertain the viability of this relationship and the level of trust held by the public / market in this entity.

A key criteria will be if consumers clearly understand what data they are being asked to approve for transfer; as is the perceived ease with which the consumer experiences this process, whilst maintaining appropriate security. Tipping the balance towards a simple and easy consumer experience may come at the cost of eroding consumer trust in the process (under all models); and consequently the entire CDR. Therefore finding the balance between adequate controls and ease of access will be paramount in order to support competition and consumer uptake of the CDR regime.

Similarly, if consumers are required to face multiple different consent processes and have variable consumer experiences where an industry specific approach is adopted this could adversely affect consumer trust and adoption in the both the broad CDR system.

[5] **Honey Pot** A system (e.g., a web server) or system resource (e.g., a file on a server) that is designed to be attractive to potential crackers and intruders, like honey is attractive to bears. Computer Security Resource Centre

OR

A specially configured server, also known as a decoy server, designed to attract and monitor intruders in a manner such that their actions do not affect production systems. Also known as "decoy server" ISACA

4. Innovation

As specified in the proposed legislation[6], consideration is to be applied to each new sector on the impact it may have on consumers and the market. The impact of designating one or more gateways should be considered for any impact this entity may create for the sector, and on the operation of the new economy-wide data market. This includes the capacity of this configuration of the sector to respond to and promote Treasury's implementation principles: being consumer focussed, encouraging competition, creating opportunity and being efficient and fair. This would include the capacity for a designated gateway to maintain the cadence of the iterative development of the CDR standards as the regime matures and reaches across sectors. An inability to maintain this cadence would impact the potential for innovation.

Question 2: Having regard to the assessment criteria, what are the advantages and disadvantages of each of the models?

In our view a key element of the CDR regime is to enable and facilitate competition by making consumer data easily accessible and transferrable to parties agreed to by consumers. To further support this capability CDR has never been considered to be the single mandated channel for provision of data (often because not all consumers will use a digital access channel). Similarly, it would provide a more open environment if, in the event that a gateway model was supported, that it not be mandatory and the regime allowed for participants to also offer direct access to accredited third parties and consumers.

Creating a centralised point of access (model 1 and 2) in any sector presents a series of potential disadvantages. High demand, and/or a degradation/loss of service could result in the central model being perceived as a single point of failure (**SPoF**); a SPoF that would consequently be more attractive to attackers (i.e. denial of service). The resulting impacts could affect consumers in the energy sector, as well as consumers accessing services from across sectors, such as in a mature economy-wide CDR data market of the future.

The use cases and designated data sets for both the energy sector, and across the data market, are encouraged to expand and mature over time and will require all participants (especially data holders / designated gateways) to be responsive and flexible as new standards and demands are placed on the system. Whilst centralising the current data may provide certain advantages and disadvantages, pooling data from multiple participants will require continuous updates and adjustments in order to provide a centralised portal and as such offer no discernible cost savings because of this on-going overhead.

[6] Treasury Law Amendment (Consumer Data Right) Bill 2018, s56AD considerations: the interests of consumers; the efficiency of relevant markets; the privacy or confidentiality of consumers' information; promoting competition; promoting data-driven innovation; any intellectual property in the information to be covered by the instrument; and the public interest.

There is an expectation that emerging technologies and business models will generate opportunities for additional CDR data designations and use cases to emerge and be supported. Consequently, consideration of the configuration of the market should be cognisant of the emerging potential for the CDR. This consideration should also be in alignment with Treasury's implementation principles (which feed into the CDS's operating principles).

Under the centralised data access models there may be an advantage in having a single aggregation point for data across the sector, however, the model will introduce a new party, being the gateway, who currently does not have an existing relationship with consumers, or accredited data recipients in other sectors. There is likely to be the need for substantial education to build trust in such a system. Additionally, this is likely to be an on-going need as consumers will continue to receive billing from the retailer, and maintain other interactions with them, whereas the centralised hub will only be the point of contact when consumers wish to transfer data to an accredited third party. This asynchronous and asymmetric approach to connecting with consumers may lack trust and serve as a point of confusion for consumers.

Question 3: What are the likely implementation/compliance costs for market participants (including accredited data recipients) under each of the models, including costs associated with IT system changes or data storage?

The consumer's right to share data makes it imperative that data access is maintained at the lowest possible cost-of-entry for the data recipient whilst being cost effective for the data holders.

A fragmentation of CDR implementation models across the economy will complicate data access implementation and therefore push up implementation costs, thus creating a structural impediment to the legislative right of the consumer under CDR.

A centralised data access model within Energy will also mean there will be a duplication of costs in building API's as eco-system participants (such as retailers) will need to provide API gateways both on demand for the designated gateway as well as for accredited data recipients. Therefore both the gateway and the participants will have to invest in duplicated API infrastructure.

Question 4: What additional requirements should the ACCC consider including in the CDR rules for the energy sector if the gateway model is adopted?

The ACCC may wish to consider whether the rules could allow other direct channels of connection beyond just the designated gateway. This would enable eco-system participants to introduce innovation by offering more data and disparate access to data (either designated and value-added / derived data) directly to consumers

beyond what is determined as available by the gateway manager and in a different timeframe.

Under a designated gateway data access model it would be necessary for ACCC to specify the extent of customer identity verification that is required of the accountable gateway manager and whether liability for errors would rest with the gateway manager or the data holder.

If a designated gateway is used in the energy sector will it be subject to the Mandatory Data Breach Notification laws? Who'd ensure, enforce and audit that the gateway has complied? Is this the role of the ACCC? A gateway model without mandatory breach notification could significantly undermine the confidence of the CDR.

As an alternative, consideration could be applied to the establishment of a CDR-wide 'designated gateway' that offers services which the market otherwise does not want to provide. Further research would be required to demonstrate the viability of such a platform.

Question 5: What emerging technologies do stakeholders believe will have an impact on the energy sector with respect to the CDR?

A key issue to be considered are the different digital / online experiences consumers currently have in other sectors. The ubiquity of these online experiences is likely to place pressure on the energy sector to adopt similar interfaces. For example, consumers currently have a high level of digital engagement in online retailing, superannuation and similar sectors, which is likely to place more pressure on the energy sector to increasingly provide online services; services that could (and in certain cases should) align with the CDR approach to accessing data on an economy-wide basis.

When also considering the emerging technical landscape in the energy sector, we are considering the impact of new energy monitoring devices[7], such as 'non-inductive load monitors' that are capable of identifying specific makes and models of electrical appliances inside a household. For example, one of these monitors would know what exact appliance you used, when you used it, and for how long; the accumulated profile of all the devices operating in a household provides both an explicit digital pattern of life and an ability to use algorithms that turn these profiles of behaviour into observations and insights on privately held opinions and emotions, such as ideologies and orientations.

[7] https://www.ecocentric.energy/

These emerging monitoring tools, coupled with increasingly IoT enabled devices means that there is an increasing potential for a highly granular surveillance of energy consumption patterns. This granularity has the potential to reveal sensitive information (beliefs, opinions, and desires), in a similar fashion to how seemingly innocuous 'likes' on Facebook revealed this sensitive information through Cambridge Analytica's analysis. Rich data sets, such as these, would require privacy and/or security controls and treatments in order to comply with relevant regulations. Privacy preserving technologies such as synthetic data sets would be required for this.

The data access model and energy sector rules should be flexible enough to harness this consumer data and provide assurance for its protection and utility. Systems and processes that are unable to expand to include this type of innovation present an opportunity cost.

Additionally, the current international standards for information security in the energy industry are evolving with the rate of technological adoption and increasing online threats. The reflection of these standards into the rules for emerging technologies would assist industry with compliance and harmonise requirements.

Question 6: What are the cost differences to participants of providing data once a day (to an AEMO repository) or on demand?

This question is relative to the use case in question. For current product comparison use cases, once a day may be sufficient; however limiting the architecture of the system to once a day presents an opportunity cost where future use cases could only be constructed in light of this constraint.

Question 7: What is the competitive impact, if any, of accessing data through AEMO rather than through a retailer?

Unlike with the flexibility provided in the legislation for the free-market operation of a designated gateway, imposing constraints where participants are required to use certain designated gateways could lead to unintended consequences.

Flow-on effects may also occur where potential degradations of service emanating from a single point of failure, or from a loss of synchronisation with the cadence of change for the CDR's standards. Either of these scenarios would impact the competitiveness of ADRs reliant on this data; in comparison to a distributed economy-wide CDR model.

Question 8: Are there any other issues that stakeholders wish to raise?

i) Innovation occurs close to the source

The intent and design of the economy-wide CDR architecture is to allow and support competition and innovation. In other words, we intend for allowing data holders and accredited data recipients to use the standards to provide greater value and features than are defined, specified or required. The DSB is completely supportive of innovation that results in the creation of value for consumers whilst satisfying the need for safety and trust in the system, which underpins Australia's emerging data market. As such it is critical to maximise flexibility and closeness / proximity to the source of the original data.

As has been seen in other jurisdictions, and in the establishment of the CDR in Australia, an emerging data services economy is forming to meet the demands of data holders and accredited data recipients. As this economy matures, products services and platforms will become commoditised, consequently reducing barriers to entry. Invoking multiple requirements for participants to adhere to, and potentially limiting their ability to trade, would increase friction and inefficiencies for both this economy and the larger data market that the consumer would interact with.

ii) Consent models and authentication

The consent model for managing a consumer's access to data would be complicated when using a designated gateway; as this gateway must be able to validate data recipient access requests as if the gateway were the original data holder. This new relationship between consumer and gateway would require new approaches to consent, authorisation and related security practices in the CDR. None of these are proven and will require research, as well as creating uncertainty for both design and implementation. Intensive amounts of consultation and negotiation may be required. This engagement would conceivably need to occur across sectors in order to account for this different approach.

iii) Advantages and disadvantages of creating precedents

Additionally, the decision to implement a designated gateway could be seen as a precedent for all sectors to implement designated gateways. The implementation of multiple gateways would be an inefficient investment and present a suboptimal outcome for performance and innovation across the national data market. If there is a requirement for a default designated gateway to offer services that the market is unwilling to offer, perhaps a proof of concept platform could be explored.

APPENDIX A: Consumer Data Standard Operating Principles

Principles
The following principles, classified as Outcome Principles and Technical Principles, are the basis for the development of the standards for the Consumer Data Right.

Outcome Principles
These principles articulate qualitative outcomes that the API definitions should seek to deliver.

Principle 1: APIs are secure
The API definitions will consider and incorporate the need for a high degree of security to protect customer data. This includes the risk of technical breach but also additional concerns of inadvertent data leakage through overly broad data payloads and scopes. The security of customer data is a first order outcome that the API standards must seek to deliver.

Principle 2: APIs use open standards
In order to promote widespread adoption, open standards that are robust and widely used in the industry will be used wherever possible.

Principle 3: APIs provide a good customer experience
The API definitions will consider and incorporate the customer experience implications. The APIs should support the creation of customer experiences that are simple and enticing to use.

Principle 4: APIs provide a good developer experience
To ensure that the entry hurdle for new developers is low the experience of the developers that are building clients using the APIs will be considered. The ability for a developer to easily understand and write code using the APIs in modern development environments should be facilitated by the API standards.

Technical Principles
These principles articulate specific technical outcomes that the API definitions should seek to deliver.

Principle 5: APIs are RESTful
The API standards will adhere to RESTful API concepts where possible and sensible to do so. In particular the concepts of statelessness and resource orientation will be followed.

Principle 6: APIs are implementation agnostic
The underlying implementation of the APIs should not be constrained or driven by the API definitions and standards. Conversely, the underlying implementation choices should not be visible or derivable to the client applications using the APIs.

Principle 7: APIs are simple
As complexity will increase implementation costs for both providers and clients as well as reduce the utility of the APIs, API definitions should seek to be as simple as possible but no simpler.

Principle 8: APIs are rich in capability
As the APIs are defined care should be taken to ensure that the data payloads defined represent rich data sets that can be used in many scenarios, including scenarios not necessarily front of mind during the design process.

Principle 9: APIs are performant
The API definitions should consider and incorporate performance implications during design ensuring that repeated calls are not necessary for simple use cases and that payload sizes do not introduce performance issues.

Principle 10: APIs are consistent
The API definitions across the full suite of APIs should be consistent with each other as much as possible. Where possible common data structures and patterns should be defined and reused.

Principle 11: APIs are version controlled and backwards compatible
As the API definitions evolve care will be taken to ensure the operation of existing clients are protected when breaking changes occur. Breaking changes will be protected by a well-defined version control model and by a policy of whereby previous versions are maintained for a period of time to allow for backwards compatibility.

Principle 12: APIs are extensible
The API definitions and standards should be built for extensibility. This extensibility should accommodate future APIs categories and industry sectors but it should also allow for extension by data providers to create unique, value add offerings to the ecosystem.