30 July 2021

EnergyAustralia Pty Ltd
ABN 99 086 014 968

Level 19
Two Melbourne Quarter
697 Collins Street
Docklands Victoria 3008

Phone +61 3 8628 1000
Facsimile +61 3 8628 1050

enq@energyaustralia.com.au
energyaustralia.com.au

Ministers
Consumer Data Right Division
Treasury
Langton Cres
PARKES ACT 2600

Lodged electronically: data@treasury.gov.au

Dear Ministers,

Consumer Data Right Rules amendments - Version 3

EnergyAustralia is one of Australia's largest energy companies with around 2.3 million electricity and gas accounts in NSW, Victoria, Queensland, South Australia, and the Australian Capital Territory. EnergyAustralia owns, contracts, and operates a diversified energy generation portfolio that includes coal, gas, battery storage, demand response, solar, and wind assets. Combined, these assets comprise 4,500MW of generation capacity.

EnergyAustralia welcomes the opportunity to make this submission to the Draft Consumer Data Right Rules amendments – Version 3 (Draft Rules).

With regard to the consultation process, we suggest that Treasury would have benefited from providing more detail on the policy intent of the proposed changes in its consultation materials when the Draft Rules were released. While the Exposure Draft Explanatory Materials were concise and easy to read, they lacked detail around why Treasury had adopted certain design details. For instance, it was difficult to understand the reasons why Affiliates could not collect CDR data from Data Holders directly. It was also difficult to gauge the focus areas which Treasury was interested in. We suggest providing more detail and questions for stakeholders in another document to supplement the Exposure Draft Explanatory Material in future consultations and releasing this information as soon as possible.

Our comments on the substance of the Draft Rules are below.

Increasing pathways to participation

We understand that the broad intent behind the new pathways is to:

- lower barriers to greater uptake of the CDR by participants and consumers, and
- ensure customers trust the security and integrity of the CDR.

It will be important to test with the ADR community whether the particular pathway models (Affiliate, CDR Representative etc.) are viable options for participation. Our comments focus on the second part of the intent - maintaining trust in the security and integrity of the CDR.

Affiliate model

In relation to the Affiliate model (the sponsored level of accreditation), all ADR obligations will apply to the Affiliate except that the conditions of accreditation will be adjusted to allow for self-assessment against Schedule 2 (information security requirements) and an attestation statement. ASAE 3150 will also not apply.

We note that ISO 27001 is the industry standard for information security, and ASAE 3150 is already a simplified version of it and so we do not consider that it should be removed. It is also unclear why ASAE 3150 is a cost barrier, when ADRs are likely to be taking credit card payment for their services and would be Payment Card Industry Data Security Standard (PCI DSS) compliant which is a higher standard than ASAE 3150.

Regarding self-assessment/attestation, we consider this is a sub-optimal control for ensuring Schedule 2 is complied with. If Treasury chooses to use self-assessment and does not apply ASAE 3150, we strongly suggest that that self-assessment be reinforced with auditing or the possibility of audit in the first 12 months or if issues arise later.

CDR Representatives and unaccredited collecting Outsourced Service Providers

In relation to the CDR Representatives and unaccredited collecting Outsourced Service Providers (OSPs), we consider the following issues are key:

- **Transparency to the customer on who they are dealing with and who to raise complaints with**. This should apply across the Affiliate and CDR Representative pathways so that the customer knows more than one business is involved and another business is involved in the "back end" in supplying their CDR service.

  This is particularly the case for the CDR Representative model where from the point of view of a consumer they only deal with the CDR Representative (as if it were an ADR) and they may not be aware of the Principal's involvement. Draft Rule 4.3B)(i) provides some transparency by requiring information on the "fact that the person is a CDR Representative, and that the CDR data will be collected by its CDR Principal". However, it could be further strengthened by an additional requirement to explain what this means in terms of the CDR Representative being non-accredited, and to specify who a customer should raise complaints with.

  In the same way, information regarding Affiliates under 4.11(3)(i) should be improved to explain what it means. i.e. Affiliates are an ADR with self-auditing of information security.

  We also suggest an addition to Rule 8.11(1) to require the Data Standards Chair to establish another data standard on the terminology that must be used when providing information on CDR Representatives and Affiliates. This will help to ensure the information is clear to customers and there is some level of consistency in messaging across providers.

  In addition, we note that Data Holders will not have visibility over who the data has been disclosed to. A Data holder may have only directly dealt with the Sponsor/Principal and so when directing customer complaints, it will only direct the customer to the Sponsor/Principal ADR.

- **Greater risks around ongoing consent** – There are greater risks of the consumer not recalling who they are dealing with when more than one business is involved in providing their CDR service. Where a consent to disclose data to the Affiliate or CDR Representative is ongoing, ongoing notification under Rule 4.20 to remind the customer that their consent is still operating will be key, with a reminder that the person is an Affiliate or CDR Representative.

- **Limited ability for direct Regulator enforcement** – We recognise that the CDR Representative and Outsourced Service Provider models contemplate parties managing risk and compliance through commercial contracts.

  The energy sector's experience with managing Third Party compliance with energy sector regulation via contracts illustrates the challenges of Third Party compliance management. There are several examples where it has not been effective in protecting customers. Recently, on 29 June 2021, Simply Energy paid penalties totalling $2.5 million after the Essential Services Commission of Victoria issued 125 penalty notices. The penalty notices related to two Third Party Sales agents undertaking deliberate fraud to transfer 525 gas and electricity

accounts at 264 properties without any contact to obtain explicit informed consent to enter an energy plan contract.[1] In practice, managing compliance through contracts may not be effective.

The CDR Representative model has only a few obligations which can be enforced directly by the ACCC against the Principal (not CDR Representative), and it appears the OSP has none. The ACCC should have a strong mechanism to monitor how successful these commercial contracts are in achieving compliance with CDR obligations.

Rule 2.3 of Part 2 Schedule 1 requires Accredited Persons to notify the ACCC when they become a CDR Principal including details of the CDR representative and any information necessary to evaluate the CDR representative. We would suggest a specific reference to being able to request information about CDR arrangements and the contracts themselves, and a power to audit and review Third Party management.

Trusted Advisor Disclosure and Insights Disclosure

The Draft Rules extend the CDR regime to sharing CDR data outside the regime to non-accredited persons:

- Draft Rule 1.10A provides that a CDR consumer can consent to an ADR disclosing a consumer's CDR data to a nominated Trusted Advisor (Trusted Advisor Disclosure).
- Schedule 3 amends the CDR Rules to allow a consumer to consent to an ADR sharing "CDR insights" using their CDR data to any person, provided the disclosure is for one of the specified purposes in the CDR Rules (Insight Disclosure).

Trusted Advisor and Insight Disclosures need more information at time of consent

EnergyAustralia acknowledges that disclosing CDR data to Trusted Advisors and other businesses may promote new or existing services with a convenience benefit.

We still however question whether customers would be comfortable with ADRs sharing their data to other businesses generally. The data economy is developing, and this is already presenting new challenges to consumers and service providers. According to the Office of Australian Information Commission's last Australian Community Attitudes to Privacy Survey' (ACAPS), 79% of Australians are uncomfortable with businesses sharing their personal information with other businesses. Further, Australians consider a misuse of information to be a situation in which:

- an organisation that they haven't dealt with gets hold of their personal information (87%); or
- they supply their information to an organisation for a specific purpose and the organisation uses it for another purpose (86%).[2]

In view of the above, strong informed consent to disclosures of data outside the CDR regime will be critical to maintaining trust in the regime. Similar to our discussion above on the new pathways to CDR participation, the CDR Rules should require specific information about Trusted Advisor Disclosures at the time of obtaining the customer's consent. We ask that Draft Rule 4.11(3) include a clear explanation at the time the customer provides their consent which explains that their CDR data will be disclosed to Trusted Advisors who are not Accredited Persons.

For both Trusted Advisor and Insight Disclosure consents, the information provided at the time of consent should also make it very clear that the protections in the CDR Rules will no longer apply to how their data will be used. This is partly in place for CDR Insights (Rule 8.11(1A)) but should be extended to Trusted Advisors. Further, it should also be specifically explained that:

[1] Simply Energy penalty notices 2021 (explicit informed consent) | Essential Services Commission
[2] https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2017/acaps-2017-report.pdf , p 14

- Trusted Advisors are under no obligation to delete or de-identify data when it becomes redundant as required under the CDR Rules, and other legislation such as the Privacy Act does not substitute for this requirement.
- Data leaving the CDR regime may not be protected by the Privacy Act, where that data is not Personal Information, or the Trusted Advisor is not an Australian Privacy Principles Entity.

EnergyAustralia believes it will also be of high importance to consumers that the Rules or CX experience data standards ensure consents are presented in a way so they do not feel compelled to accept them in order to receive the goods or services from the ADR. Similar concerns around digital consent have been explored at length in the ACCC's Digital Platforms Inquiry,[3] in relation to service providers like Google and Facebook that use standard-form click-wrap agreements with take-it-or-leave-it terms and bundled consents. This is again only partly addressed in the Rules for Trusted Advisors. For Trusted Advisors, the Draft Rules provide an Accredited Person must not make nominating a Trusted Adviser or giving a Trusted Advisor Disclosure consent, a condition for supply of goods or services. This should be extended to Insight Disclosure Consents.

Even with the above improvements to information provided at the time of consent, we still have concerns that the multiple different types of consent under the Draft Rules will be confusing for customers.[4] The Draft Rules will add an additional two consent types to the existing four. The last Privacy Impact Assessment made various recommendations about the complexity of the previous proposed CDR Rules, and we recommend that the next assessment should shed further light on this issue. There is a real risk that consumers will not appreciate the subtle differences between the consent types, and will not be able to identify the data, the ADR or other recipient, and the period, to which the consent relates.

Trusted Advisors and Recipients of Insight Disclosures may have weak data security

Some classes of Trusted Advisor might not have strong data security**.** The Exposure Draft Explanatory Materials states that:

> "Trusted advisers do not attract the regulatory obligations that apply to ADRs under the CDR regime. However, these rules recognise that as members of a professional class, they are subject to existing professional or regulatory oversight, including obligations consistent with safeguarding consumer data (e.g. fiduciary or other duties to act in the best interests of their clients)".

This statement appears to address intentional misuse of consumer data in conflict with the best interests of the customer. However, we see another key risk as relating to unintentional data breaches where the data security of a business is deficient. While the larger players in the Trusted Advisor categories would have very sophisticated data security systems and processes, we note that many financial counselling agencies/advisors/planners and mortgage brokers can be very small businesses that would lack the resources to provide strong data security environments. Overall there is an increased risk to data security in allowing disclosure to all Trusted Advisors without a consideration of their data security maturity.

Additional feedback regarding CDR insights

We would like to have a clearer understanding of the likely value of the use cases and customer benefits that would flow from Insight Disclosures.

Our overall concern is that some businesses may eventually collect data via the CDR on a regular basis for a large number of customers. This comment also applies to Trusted Advisors. We encourage Treasury to consider if existing regulations are sufficient to ensure that customer data is not data

3 https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry
4 Previous sub p 8.

mined for insights, on-sold or treated in other ways (possibly without disclosure) that consumers are unlikely to find acceptable.

At first glance, the Draft Rules appear to offer a narrower version of previous iterations of Insight Disclosure - by linking the CDR data to "specified purposes". Rule 1.10A(3) defines an Insight Disclosure consent as a consent given by a CDR consumer for an ADR to disclose particular CDR data (the CDR insight) for a specified purpose. Specified purposes are: to identify the consumer or to verify the consumer's account balance, income, or expenses.

In operation, it is difficult to appreciate the effect of adding the specified purposes. The specified purposes only seem to limit the type of CDR data that can be disclosed. i.e. the ADR can only disclose CDR data to verify an account balance etc.

Our main concern is that once the ADR discloses the CDR data to the recipient, there is no limit on how the recipient can use the CDR data or further disclose that data (subject to Privacy Act or other regulation outside the CDR regime). This could be a very broad expansion and our concern is that it could be used in ways that are not presently contemplated by Treasury and Government. This could include ways of using data to target vulnerable customers.

Unlike disclosures to non-accredited Trusted Advisors (who must act in the customer's best interest), Insight Disclosures could disclose CDR data to any person or any business which may not have similar regulatory obligations. We provide an example below to illustrate the risks this may present.

For example, a Customer could consent to allow an ADR to provide their account balance amount and expense data to Business X (an advertising company) every day for 12 months. The Customer provides their consent because they are comfortable with providing data to a marketing company and have in previous contracts with other businesses.

Under Rule 4.11(3), when the customer is asked to give consent to the ADR, the customer is provided an explanation that their account balance will be disclosed and that will allow Business X to verify the customer's account balance; and likewise, that their expenses will also be disclosed to verify their expenses. There is no need for the ADR to inform the customer of how Business X will use the CDR data. Nor is there an extra requirement for Business X to inform the customer of how it will use the CDR data.

Business X obtains the customer's daily account balance and their expenses and the businesses charging the expenses. Business X is able to ascertain when the customer is paid and that one of their expenses is paid to an online betting business. Business X then offers services to the online betting business to send it notifications at times when advertising to the customer for their betting services will be optimised (but not the underlying reason why or the data).

While the above is a very specific example, it is not inconceivable. The Consumer Policy Research Centre's latest report on Joint accounts & the Consumer Data Right noted "it is anticipated that the business models of CDR data recipients will utilise behavioural marketing techniques to obtain customers, such as personalised advertising of value propositions based on existing data profiles…". The CPRC's report also notes an example of transactions to online betting accounts being used by recipients to assess a customer as a high-risk borrower.[5]

We ask Treasury to consider the breadth of the provisions around Insight Disclosures and what use cases may be enabled. One possible way to de-risk undesirable use cases and provide greater transparency/oversight to the customer is to only permit consents to *one off* Insight disclosures, and not permit ongoing disclosure. This would at least assist to mitigate the risk that customers will

[5] Consumer Data Right Report 2: Joint accounts & the Consumer Data Right - PERSPECTIVES FROM COMMUNITY ORGANISATIONS & CONSUMER ADVOCACY - CPRC , p 39

forget and leave ongoing data disclosure arrangements in place. We also contend that many of the use cases that would require identifying the customer or verifying the customer's account balance etc relate to assisting with a customer's application or the on-boarding of a customer for a product (which would be a one-off use case and not require ongoing data disclosure).

If you have any questions in relation to this submission, please contact me (Selena.liu@energyaustralia.com.au or 03 9060 0761)

Selena Liu
Regulatory Affairs Lead