29 October 2020

Paul Franklin
Executive General Manager
Consumer Data Right
Australian Competition and Consumer Commission

**By email:** ACCC-CDR@accc.gov.au

EnergyAustralia Pty Ltd
ABN 99 086 014 968

Level 33
385 Bourke Street
Melbourne Victoria 3000

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

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

Dear Mr Franklin,

**Consumer Data Right Rules – Expansion amendments (PUBLIC VERSION)**

EnergyAustralia welcomes the opportunity to respond to the ACCC's consultation paper on the CDR Rules expansion amendments (Consultation Paper).

EnergyAustralia is one of Australia's largest energy companies with approximately 2.5 million electricity and gas accounts in NSW, Victoria, Queensland, South Australia, and the Australian Capital Territory. We also own and operate a multi-billion-dollar energy generation portfolio across Australia, including coal, gas, and wind assets with control of over 4,500MW of generation in the National Electricity Market (NEM).

The Consultation Paper and the Exposure Draft of the CDR Rules for 3rd amendment – 30 September 2020 (Proposed Rules) are a significant expansion of the current CDR Rules. We make the following general comments:

- The Proposed Rules contain amendments which are multi-dimensional and highly complex. In summary, they introduce, at the same time, three new models of tiered restricted accreditation (Restricted Accreditation), several types of consents, new non-accredited recipients of CDR data, expansions to eligibility via Secondary Users, and many other amendments.

  In our submission below we set out an example of how the new changes may overlap to demonstrate the complexity. We share the concerns outlined in Maddock's updated Privacy Impact Assessment on the CDR Rule expansion amendments (Updated PIA) that the complexity will be challenging for consumers to comprehend and for CDR participants to understand and comply with. If the ACCC were to pursue these amendments, we urge the ACCC to not introduce all the proposed amendments at the same time.
- The use cases which might support the proposed expansions to the CDR have a stronger basis in banking, compared to energy. We refer to use cases around disclosure to Trusted Advisors, where applications for banking accounts and mortgage products often require professional advisors, whereas the sale of energy typically does not.
- The energy sector has also not yet implemented the CDR. Current implementation dates are estimated to be set for H2 2022. EnergyAustralia raises concerns around requiring the energy sector to implement this expanded version of the CDR Rules in its first implementation unless there are substantial efficiencies in doing so.
- EnergyAustralia supports the recommendations in the Updated PIA. The drafting of the Proposed Rules requires more development before they are finalised by the ACCC. In this

submission, we outline the specific recommendations from the Updated PIA which we strongly agree with.

- The Updated PIA does not cover the full scope of the proposed changes[1], including material changes to introduce the concept of account privileges and Secondary Users. The ACCC should not proceed with progressing the changes until a PIA has been completed for those changes.

Our submission responds to the key topics in the Consultation Paper and is based on several overarching principles as set out below:

- **Strong consent frameworks are critical across the various proposed expansions.** Consent must be informed, unbundled and explicit. In particular, informed consent should place an emphasis on informing the consumer when data is disclosed to an accredited person with Restricted Accreditation or outside the CDR regime. Strong consent is particularly necessary where consents will be multiple (there are six different types of consent under the Proposed Rules), layered, and would be in place for potentially several Accredited Persons.

  We question the ability of customers to fully understand these multiple consents in tandem, and we also have concerns that customers may be compelled to accept consents to receive the CDR goods or services from the Accredited Person.

  Consent must also be current to ensure that the relevant account holder or customer is providing the consent.

- **Data security is paramount and must be maintained.** Restricted Accreditation via the three models (Limited Data, Enclave and Affiliate) will only be acceptable if sufficient data security is maintained. The proposed self-attestation and self-assurances of the Restricted Accreditation models are not sufficiently robust. To ensure comparable security baselines across all Accredited Persons and Accredited Data recipients (ADRs), auditing to the relevant Australian Standard is necessary.

- **Where two Accredited Persons are involved in providing an ADR service further measures can be introduced to bolster security measures.** The measures for Affiliate Restriction and Enclave Restriction should include establishing a regulated contract similar to what is in place for outsourced service providers, liability arrangements and incident management.

- **Ensuring that customers have transparency over disclosures of CDR data to non-accredited persons is key** to place the customer at the centre of these decisions, in addition to strong consent frameworks. These disclosures are to Trusted Advisors and disclosure of insights to any person - outside the CDR ecosystem. We also urge the ACCC to consider narrowing the scope of these expansions to avoid unintended effects as set out in our submission (see section 4).

If you have any questions in relation to this submission, please contact [redacted]

Yours sincerely,

Melinda Green
Head of Customer Value Management

[1] https://www.accc.gov.au/system/files/CDR%20-%20Update%202%20to%20privacy%20impact%20assessment.pdf p 4

**Submission**

## 1. High complexity of the CDR Rules amendments

The Proposed Rules contain amendments which together are multi-dimensional and highly complex, and which will be added to the current regime which is already highly complicated.

The complexity will be challenging for consumers and CDR participants, and will create a significant risk that customers will not understand what they are consenting to and what decisions they are making with respect to their CDR data.

Accredited Persons will find it very difficult to understand the full extent of their obligations as they deal with CDR data in different capacities (as Accredited Persons and ADRs) and under different disclosures (receiving it from Data Holders or other ADRs). As a result, there is a high likelihood that there may be unintentional non-compliance by Accredited Persons.

Both outcomes for consumers and ADRs will lead to mistrust in the CDR regime, and potentially unauthorised disclosure of CDR data. It is also not certain that the complexity is necessary or will be beneficial to customers and ADRs.

As noted in the covering letter, the Proposed Rules introduce, at the same time, three new models of tiered restricted accreditation (Restricted accreditation), several types of consents (where current consents cover only consent to collect and use CDR data), new non-accredited recipients of CDR data, expansions to eligibility via Secondary Users, and many other amendments such as arrangements for non-individual or business users and ability for a customer to amend consents.

To illustrate the complexity, we provide an example of how the amendments appear to overlap:

| **Example of how the amendments appear to overlap and associated complexity** | |
|---|---|
| **Step** | **Complexity** |
| a) A customer provides consent to a Data Enclave Accredited Person (A1) to collect their energy billing data from an Energy Retailer **(First consent)**. The Retailer obtains authentication and authorisation to do so. | Customers may already be confused between consent and authorisation. |
| b) A1 is operating under an Enclave Restriction (with a Combined Accredited Person (CAP) arrangement). A1 does not collect the data from the Retailer, rather the Enclave Provider (another Accredited Person) collects the data. | Two Accredited Persons are now involved, the customer may not understand where their data is held or who is handling their data.<br>The ADRs need to navigate the complexities of which ADR is meeting each obligation under the enclave, under the CDR Rules. |
| c) A1 seeks to disclose the billing data to A2 under an AP Disclosure. A1 obtains from the customer, a Disclosure Consent (**Second Consent**). A2 obtains a Collection and Use Consent **(Third Consent).** | Both consents relate to the same data. Customers are likely to be confused on what the difference is. |
| d) A2 is operating under a Limited Data Restriction (assuming billing data is a low/medium risk data set) but uses an Outsourced Service Provider to provide CDR services. | Throughout the data handoffs between CDR participants, different Restricted Accreditation models may apply (e.g. Enclave, Limited Data restrictions) – so slightly different information security measures may apply to the data. |
| e) A2 seeks to collect consent to disclose the billing data to the customer's accountant **(Fourth** | By this point, the customer has provided six consents linked to the same billing data to two Accredited Persons. |

| | | |
|---|---|---|
| | **Consent),** so that the accountant can provide budgeting assistance.<br><br>A2 also wishes to use the customer's data to conduct General Research to improve its own services and obtains consent to do so **(Fifth consent).**<br><br>And, lastly it also obtains consent to disclose Insights data about the customer to a third party non-accredited customer research firm **(Sixth Consent)** | The first four consents relate to billing data, and the last two relate to use of billing data to produce General Research or derived insights.<br><br>While the customer has provided consents to two ADRs, three ADRs have handled their data (due to the additional Enclave Provider) and one Outsourced Service Provider has also handled their data. |
| f) | The customer decides to add a Secondary User instruction to grant a Second User ability to share data. The Second User is authenticated by the Data Holder. | The Secondary User Instruction is another consent like function which the customer must provide.<br><br>A1 and A2 may now have further obligations in relation to this Secondary User – the extent to which might not be clear. |
| g) | The Customer withdraws their authorisation with the retailer and revokes their Secondary User instruction. | The Data Holder must communicate this to A1. But it is unclear how and if this cascades down to "downstream" ADRs like A2.<br><br>The customer is likely to be confused as to the treatment of their data by all CDR participants and non-CDR participants after their authorisation has been withdrawn. |

As above, we question the benefits of the proposed amendments but if the ACCC were to proceed with them, we urge the ACCC to not introduce all the proposed amendments at the same time in view of the apparent complexities. A staggered approach would allow the ACCC to assess the incremental effect of each change on the CDR regime in practice, before adding another level of change.

## 2. Restricted Accreditation for ADRs

### 2.1 General views across all three models

As noted in our cover letter, data security is paramount for customers and is fundamental to ensuring the integrity of the CDR regime and building consumer trust in the CDR. This will ultimately drive consumers' willingness to share their data under the regime.

Restricted Accreditation via the three models will only be acceptable if sufficient data security is maintained by all parties. The data security requirements in Schedule 2 already present a moderate approach to data security, there are higher and more prescriptive information security standards – including NIST maturity level 4. Any lowering of the security standards in Schedule 2 via partial application to Restricted as ADRs, means lowering the information security standards from this moderate starting point.

Consumer data is a honey pot. There are already countless examples of data privacy breaches and data misuse by data collectors and providers who push the boundaries. The recent ACCC's Digital Platforms Inquiry,[2] in relation to service providers like Google and Facebook, highlights the fine line between innovation and exploitation in this space. At a minimum, the CDR regime should effectively minimise the risk of data privacy breaches.

EnergyAustralia questions the robustness of the assessments (of compliance with Data security requirements under Schedule 2 of the CDR Rules) and attestations of compliance with those requirements, that will apply to Restricted ADRs (Restricted Level Attestation and Restricted Level Assessments).

[2] https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry

- Both are likely to be self-assured and self-attested; and
- Both are not subject to the ASAE 3150 standard but must be done in accordance with "any approved requirements".

In our view, to ensure comparable security baselines across all ADRs, external auditing to the relevant standard is necessary. As the Proposed Rules establish different frameworks of assessment (ASAE for Unrestricted ADRs and "any approved requirements" for Restricted ADRs), this consistent baseline will not be achieved.

**Measures to strengthen arrangements for Data Enclave and Affiliate Restrictions**

Separate from the auditing/attestation of data security, we also consider the CDR Rules could strengthen the arrangements regarding Data Enclave and Affiliate Restricted Accreditation. Specifically, to incentivise the Enclave Provider and Sponsor to take measures to ensure the security of the data handling by the Data Enclave Accredited Person and Affiliate:

- The Enclave Provider and Sponsor should also be liable for the breaches of the Data Enclave Accredited person and Affiliate irrespective of whether the Enclave Provider or Sponsor has acted in accordance with an arrangement in place with the restricted ADR.

  This liability requirement should be an additional requirement to the existing requirement of taking reasonable steps to ensure compliance by the Data Enclave Accredited person and Affiliate. We share the concerns in Updated PIA that reasonable steps could be taken to mean a condition in a contract that requires compliance with the CDR Rules which would be insufficient.

  Imposing the liability requirement will mean the Enclave Provider and Sponsor will take more thorough and comprehensive steps in their due diligence and compliance monitoring of Data Enclave Accredited Persons and Affiliates. It also has the second benefit of providing better enforceability for the ACCC across Enclave and Affiliate Restriction arrangements.

  To further strengthen the incentive, we propose that the arrangement/contract between the Enclave Provider and Sponsor and the Data Enclave Accredited Person and Affiliate, could be regulated in a similar way to how Outsourced Service Provider CDR arrangements/contracts are regulated.

  This regulated contract should address further outsourcing by the Enclave Provider and Sponsor. For instance, where the Provider/Sponsor is to collect CDR data under the contract, the provider must not further outsource that collection; the provider must not disclose any CDR data to another person, otherwise than under a further regulated contract; and if the provider does disclose such CDR data it must ensure that the other person complies with the requirements of the regulated contract.[3] Applying similar protections of Outsourced Service Providers to Enclave Providers and Sponsors appears proportionate and appropriate where they are effectively providing outsourced ADR services to Data Enclave Accredited persons and Affiliates.
- The CDR Rules should require that data breach incident management be in place to define responsibilities between the Restricted and Unrestricted ADRs under both the Enclave and Affiliate arrangements, and to require reporting on these incidents to the ACCC.

We also consider there are possibly alternative methods of Tiered accreditation which could be explored instead of the three models – which are agnostic on the types of data shared and type of relationship between the Unrestricted and Restricted ADR. EnergyAustralia supports an exploration of alternative options where adequate security measures (which reflect similar measures to those detailed in Schedule 2), and where the above dot points regarding liability and breach incident management, are also established.

Lastly, we also emphasise that a strong consent framework is key to extending the CDR via Restricted Accreditation under all three models. Information provided to the consumer before consent is obtained should clearly reflect that the relevant Accredited Person is only accredited to a Restricted Level and the effect of this, and the Enclave Provider's or Sponsor's role in handling the consumer's CDR data.

[3] CDR Rules, Rule 1.10(2)(b)(iv)-(vi)

### 2.2 Limited Data Restriction

A person with Limited Data Accreditation (Limited Data Accredited Person) will only be permitted to collect CDR data that has been assessed as lower risk compared to the complete set of data that can be collected by an Accredited Person with an unrestricted level of accreditation.

EnergyAustralia considers that allowing lower accreditation for lower risk data sets may have unintended effects in practice, particularly when applied across sectors and where banking and financial data will be included. Multiple items of low risk data can cumulatively present a high risk data set for a customer and it would be difficult for the ACCC to "future proof" the rules and identify these combinations so as to specifically exclude data points that may present this risk. This points to a weakness in the Limited Data Restriction model.

We also suggest the ACCC vigorously test the demand among potential ADRs for access to low risk data sets on a standalone basis. For the energy sector, the most popular use cases such as energy plan comparison, would require a mix of data sets which would likely include higher risk data sets (e.g. metering data) combined with other lower risk data sets from a customer's perspective such as Tailored Tariff Data (details of the energy plan a customer is on). The commercial attractiveness and viability of only holding low risk data is very unclear.

If the ACCC were to proceed with the Limited Data Restriction, EnergyAustralia will reserve its views on which energy sector data sets are specifically low, medium, and high risk. However, we encourage the ACCC to take a framework approach to considering these matters across sectors to promote consistency across the economy as the CDR is rolled out.

The ACCC should consider the following factors when undertaking its risk assessment as to which data is low, medium, and high risk, drawing from existing frameworks and concepts:

- CDR data which would also be "Sensitive data" under the *Privacy Act 1988*, including health information, should be high risk data and require an Unrestricted level of accreditation. Sensitive information has a higher level of privacy protection under Privacy Laws than other Personal Information, and similarly the CDR regime should reflect this approach by requiring a higher level of accreditation for sensitive information.
- Any information identified by family violence protections as "confidential information" - information that may be used to identify or locate an affected customer, including information about their whereabouts, contact details, or financial or personal circumstances, should be categorised as high risk data where it is associated with a person other than the account holder (i.e. in Secondary User contexts).[4]
- The initial PIA for the Consumer Data Right (March 2019) identified characteristics which make banking transaction data high risk. These characteristics could be used to identify other high risk information across other sectors, including[5]:
    - Data that contains behavioural information.
    - Information as to where a person has been and what actions they have taken, what their preferences are, and what their interactions have been with others.
    - Information about personal activities – such as in relation to health care.
    - The location or other characteristics of a person's home or the homes of relatives.
    - Financial status.
- From our experience in meeting our privacy obligations under the *Privacy Act 1988*, drivers licence number and date of birth are pieces of information which pose a high risk of misuse in terms of fraud and identity theft.

For the energy sector, high risk data includes:

[4] Energy Retail Code (Vic) rule 106(2)
[5] https://treasury.gov.au/sites/default/files/2019-03/p2019-t361555-pia-final.pdf, p 91

- metering data (usage data) – which falls under some of the categories above – by showing a customer's typical daily movements.
- Payment data could reveal behavioural information.
- The details of joint account holders or Secondary Users can reveal personal relationships and interactions with other people.
- Debt status - whether a customer is a hardship customer or receiving concessions can be used to insinuate financial capacity to pay.

We also note that some of the banking information flagged as low and medium risk may be higher risk, such as Account Identifiers (in Detailed Bank Account Data), Basic Customer Data, and Bank Payee Data. Again, these may assist in identity fraud and reveal relationships between customers and other persons.

### 2.3 Data Enclave Restriction

EnergyAustralia understands that the Data Enclave Restriction must be used in combination with a CAP arrangement. Accordingly, the Unrestricted Accredited Person will be the Enclave Provider, who will make Consumer Data Requests for CDR Data and hold the collected CDR Data on behalf of the Data Enclave Accredited Person. The Updated PIA also explains the Enclave Restriction allows access and use of CDR Data by leveraging the data environment of the Enclave Provider.

We understand that any use of the CDR Data by the Data Enclave Accredited Person will be within the environment of the Unrestricted Enclave Provider (i.e. their Information and Communication Technology infrastructure) which will have the necessary firewalls etc. The exact boundaries of this arrangement and data hand off points need to be clear for both the Data Enclave Restricted ADR and the Enclave Provider.

It also needs to be clear whether it is the Data Enclave Restricted ADR or the Unrestricted ADR who is interacting directly with the customer; and which party is ultimately responsible for handling the data throughout the data life cycle - from when the data is first obtained to when it becomes redundant. The Proposed Rules appear to make some clarifications, but the Updated PIA identifies a number of ambiguities.

We also suggest that the ACCC publish a guideline on these matters to assist ADRs seeking to use the Data Enclave Restriction, as these ADRs are unlikely to have the required regulatory and legal resources to navigate the full breadth and complexity of their obligations under the CDR Rules.

### 2.4 Affiliate Restriction

The Proposed Rules require the Sponsor of an Affiliate Restricted ADR to provide, on behalf of the Affiliate, the Restricted Level Assessment and Restricted Level Attestation. This appears to remove the engagement between the Affiliate Restricted ADR and the ACCC, which we consider should be maintained for the purposes of the ACCC "knowing" who is being accredited (even at a restricted level).

Please see our other comments set out under section 2.1 which apply to both Data Enclave and Affiliate Restrictions.

## 3. Disclosure of CDR data between Accredited Persons (AP Disclosure)

The Proposed Rules introduce the concept of AP Disclosures which can be used in conjunction with Affiliate Accredited Persons or on a separate basis as a data sharing mechanism.

AP Disclosure is linked to a specific and new type of Consumer Data Request. This type of Consumer Data Request allows for the transfer of data between an ADR (who holds the data) (A1) and an Accredited Person (who does not hold the data yet) (A2). Two consents must occur before AP Disclosure is permitted:

- An Accredited Person Disclosure Consent – where A1 (the ADR who has the data) obtains consent to allow it to disclose CDR data to A2.
- A Collection and Use Consent – where A2 (which does not have the data yet) must obtain from the customer their consent to collect the data (from A1) and to use the data.

Together, the two consents enable A1 to disclose CDR data to A2 in accordance with the Consumer Data Request. EnergyAustralia notes that the dual consent process provides a strong consent framework. However, we encourage the ACCC to consider the below issues:

(1) **Multiple consents will be confusing for customers** - The Proposed Rules define six types of consent, whereas previously there were effectively only two. These related to collection and use of data but they were combined. The new types of consents are now:

- Collection Consent
- Use Consent
- Disclosure Consent, which has four sub-types:
  - An AP Disclosure Consent (discussed above, which supports AP disclosures)
  - Trusted Advisor Disclosure Consents
  - Insight Disclosure Consent
  - Disclosure consent for the purposes of direct marketing.

Under the Proposed Rules, different and multiple consents can be in place with different Accredited Persons and across different data. We strongly agree with the Updated PIA that there is an issue of CDR Consumers not understanding (or not remembering or keeping track of) the consents they are providing.[6]

EnergyAustralia further notes:

- 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, and the period, to which the consent relates.
- As there may be multiple ADRs, a customer may not have a consolidated view of all their current consents in one centralised dashboard making it even more difficult to compare and differentiate between the consents.
- Customers are also unlikely to appreciate how each consent interacts with other consents where consents may relate to the same data disclosure.
- For example, with respect to AP Disclosure Consents – there are three different consents that may relate to the same data:
  - ADR 1 has obtained data from a Data Holder under an initial consent from the customer. The customer has also provided authorisation to the Data Holder.
  - The consumer then provides Disclosure Consent to ADR 1 to allow disclosure to ADR 2 (as required to enable AP Disclosure).
  - However, a different Collection and Use Consent must also be obtained by ADR 2 to receive the data, for the same data.

  All three consents are required by the Proposed Rules and relate to the same data. This crossover and interaction is unlikely to be clear to a customer unless at the time of consenting, it is explained how the other consents will relate to it – particularly for the last two where consents will occur in a short period of each other. Where these consents are on-going, it would be ideal that the customer is required to be periodically reminded of this by the appropriate party. It seems likely that A1 and A2 will often not be well-

[6] https://www.accc.gov.au/system/files/CDR%20-%20Update%202%20to%20privacy%20impact%20assessment.pdf, p 47

known brands and my only interact with the customer infrequently, so it is easy to foresee a scenario where a customer cannot recall them and is unable to source the right ADR dashboard at the point they wish to update/withdraw their consent.

- We are also concerned that Accredited Persons may present requests for consent in a way that customers feel compelled to accept in order to receive the CDR goods or services from the ADR (where the consent is not required to provide the CDR goods or service).

  Similar concerns around digital consent have been explored at length in the ACCC's Digital Platforms Inquiry,[7] in relation to service providers like Google and Facebook. That is, many digital platforms use standard-form click-wrap agreements with take-it-or-leave-it terms and bundled consents, which limit the ability of consumers to provide well-informed and freely given consent to digital platforms' collection, use and disclosure of their valuable data.

  While the CDR Rules are drafted to prevent these issues, ACCC monitoring of how Accredited Persons have implemented compliance with requirements around consent will be pertinent to ensure the Rules are adequate.

Any confusion by customers might be overcome with clear information requirements at the time of providing consent. However, we strongly urge the ACCC to arrange CX testing on the comprehension levels of customers when presented with multiple and layered consents, and whether extra information will solve for the issue of consents not being fully understood.

Additionally, while the customer may initially feel informed and comfortable with their consent/s, this could erode over time, especially if the customer is left with no record or easy way to access, view and update their consents with various ADRs who have cascading or other complex sharing arrangements with each other.

This CX testing should be performed before progressing any Proposed Rules relating to the consents and associated data sharing.

**(2) Authorisation and authentication -** It is unclear whether the Data Holder's authentication and authorisation function would also apply to the AP Disclosures between ADRs and Accredited Providers. Authorisation by the Data Holder appears to be redundant as they are not disclosing the data and the AP Disclosure Consent (obtained by A1) appears to operate in its place. However, we note that a*uthentication* would still serve as a necessary protection to the customer to ensure that the person who has requested all data sharing is the same customer of the Data Holder.

**(3) Disclosure, Collection and Use Consents must be current -** EnergyAustralia highlights that maintaining the currency of consents and ensuring the consent is provided by the same person – across disclosures from Data Holders to ADRs, and between ADRs is highly important and increasingly challenging where more CDR participants are involved. For example, the CDR regime should ensure that the same person has provided all relevant consents and is the current account holder. Specifically, that the same person has:

- engaged with ADR 2 and provided a Collection and Use consent,
- provided the Disclosure Consent to ADR1,
- provided the original Collection and Use consent to A1 (to cover disclosure of the CDR data to it from the Data Holder), and
- is the current account holder.

We would expect that authentication would play a role in confirming that the person providing consent is the current account holder. i.e. the ACCC must address scenarios where there are changes to the Account Holder after the initial authentication occurs and the need to limit any data sharing to the data generated while the person was the Account Holder. Changes to the Account Holder can occur frequently for energy accounts as they relate to

7 https://www.accc.gov.au/focus-areas/inquiries-ongoing/digital-platforms-inquiry

household bills or business expenses rather than a customer's financial affairs which are usually treated with more confidentiality by customers.

(4) **Disclosure of data where there is a risk of physical or financial harm or abuse -** The current CDR Rules provide that a Data Holder may refuse to disclose CDR data if the Data Holder considers this to be necessary to prevent physical or financial harm or abuse (Rule 3.5(1)). This same provision should explicitly apply to AP Disclosures.

(5) **All relevant CDR participants should have transparency over disclosures** - Data Holders should be notified of AP disclosures by the A1 to A2. This may occur through authentication initially, but it should also occur beyond authentication. This will be necessary to support complaint and dispute resolution across multiple recipients.

(6) **Dispute resolution -** As a further protection for customers, the handling of CDR data during AP Disclosures including transfer of data, should be subject to internal and external dispute resolution under the CDR Rules; with an explicit requirement covering how Accredited Persons will resolve which ADR should resolve a complaint.

(7) **Application of Data Standards -** We understand that the Proposed Rules do not specify the process for disclosing CDR Data under an AP disclosure. Accordingly, there are no requirements for the disclosure to be, for example, in accordance with the Data Standards. However, we understand that the transfer of data will need to be encrypted – which EnergyAustralia strongly supports. We request more information on what will and will not apply to the transfer of data from A1 to A2 before we can provide final views. If the ACCC were to make the Proposed Rules, the ACCC should publish clear guidelines for Accredited Persons and ADRs to clearly set out the requirements that apply to transfers of data under an AP disclosure.

## 4. Disclosure to non-accredited parties

The Consultation Paper outlines other extensions to the CDR Rules:

- Changes that will allow a CDR Consumer to consent to disclosure of their CDR Data, held by an ADR, to a Trusted Advisor who is not an Accredited Person (Trusted Advisor Disclosure (TA Disclosure)); and
- Changes that will allow a CDR Consumer to consent to disclosure of a "CDR insight", derived from their CDR Data by an Accredited Data Recipient, to any person (Insight Disclosure).

In contrast to AP Disclosures, disclosures to Trusted Advisors and disclosures of insight information can involve disclosure to non-accredited persons or non-CDR participants. This means that the protections that apply to CDR data do not apply to these disclosures which are essentially outside the CDR regime. The effects of this are two-fold:

- An Accredited Person does not need to comply with the CDR Rules or Data Standards in relation to such transfers of data to the recipient.
- The recipient does not need to comply with the CDR Rules or Data Standards including rules which restrict how that recipient holds and uses data. Importantly, the privacy protections in the Privacy Safeguards (PS) will not apply, including:
    - protection of data from misuse, interference, and loss etc (PS 12);
    - destroying redundant data or ensuring the redundant data is de-identified (PS 12) – which we consider is particularly important to consumers; and
    - notifications of disclosures by the recipient (Trusted Advisor or otherwise) to other parties (PS 10).

The data may be protected by the Privacy Act depending on whether the information is Personal Information and the recipient is an APP entity.

EnergyAustralia agrees with the ACCC's observations that there is a risk that ADRs could operate as conduits to transfer data to non-accredited data service providers. The ACCC will also have very limited visibility of these non-accredited recipients and their data security standards or maturity.

Redress under the Rules for consumers will also be restricted including no ability for the ACCC to take enforcement action under the CDR Rules, no external dispute resolution, and no direct right of action for CDR consumers. This is a concern. Consumers will be highly frustrated if they do not have any regulatory redress (which is possible if the Australian Privacy Principles do not apply to the data). There is also a significant risk that issues will only come to light at a much later date (after the customer has engaged with their ADR) if checks by the customer are infrequent. At this point it may be too late to prevent serious or widespread harm, or where a company is no longer in operation, it may be too late to hold them to account.

We also note that the CDR is in an embryonic stage, with a low number of registered ADRs. We expect that over time as more ADRs are accredited, the ACCC will obtain a better understanding of the compliance maturity of ADRs. The extent of any demand for TA Disclosures and Insight Disclosures among ADRs and Australian consumers is also very unclear and will remain so for some time.

**Customer comfort with on-sharing data and relevance across sectors**

EnergyAustralia strongly suggests the ACCC seek a deeper understanding of whether customers are comfortable with sharing their data between businesses generally. The data economy is still developing, and this is already presenting new challenges and is potentially disruptive to consumers and service providers.

According to the Office of Australian Information Commission's (OAIC) last Australian Community Attitudes to Privacy Survey' (ACAPS), eight in ten Australians (79%) are uncomfortable with businesses sharing their personal information with other businesses. Further, Australian's 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%).[8]

The above two misuses are highly applicable for TA Disclosures and Insight Disclosures, particularly if the consumer does not understand they have provided consent (which is foreseeable given the complexities of multiple consents, discussed above). CX testing should test customer comfort levels around ADRs on-sharing data to other businesses and sharing of CDR data outside the CDR regime.

From an ADR standpoint, these use cases also appear more relevant to banking. For example, TA Disclosures are clearly relevant to the banking sector where financial and mortgage products often require accountant and legal support. These linkages are less apparent for the energy and telecommunications sector, unless on an exception basis e.g. Power of Attorney. Accordingly, we suggest that the cross sectoral benefits related to TA Disclosures and Insight Disclosures need to be robustly assessed.

In view of the above considerations, the ACCC should take a conservative approach and not expand CDR data sharing to non-CDR participants at this time – until customer demand and the CDR regime is more mature.

While we consider the ACCC should not implement TA and Insight Disclosures at this time, if the ACCC were to proceed, the following safeguards should be established to mitigate against risks and consumer dissatisfaction around disclosure to non-accredited recipients.

[8] https://www.oaic.gov.au/assets/engage-with-us/research/acaps-2017/acaps-2017-report.pdf, p 14

**(1) Informed, unbundled and explicit consent**

In addition to the concerns around multiple consents being confusing (discussed above in section 3), we set out specific consent issues for TA and Insight Disclosures below.

Disclosure Consents for TA disclosures and Insight Disclosures should be separate from Collection and Use consents of CDR data. This is important to ensure a customer can separately decline consents that relate to distinct disclosures outside the CDR regime.

When asking for consent, the ADR should present the following:

- Where the recipient is non-accredited, this fact should be clearly disclosed along with an explanation that the data will be moving outside the CDR regime and the implications of this event i.e. Privacy safeguards will not apply, and specifically, that data may not be deleted or de-identified when it is redundant. This can be expressly included under Rule 4.11(3) which requires disclosures of other matters when seeking consent.

  EnergyAustralia considers this information to be fundamental to retaining trust in the CDR regime and that it might change the customer's decision on whether they provide consent.

- For TA Disclosures, information about the classes of Trusted Advisors and typical reasons for disclosure to them.

- For Insight Disclosures, a general description of the insight information possibly through a link to the ADR's CDR policy (This is required for Use Consents relating to General Research but not for Insight Disclosures).

**(2) For disclosure to Trusted Advisors, ensure that the *Trusted Advisor* is providing professional services to the customer** – Currently, the proposed rules require the *ADR* to provide a good or service directly to the customer to address the concern that the ADR will act only as a conduit to transferring data to a non-accredited business.

Our recommendation is directed at a different concern. We propose to limit disclosures to Trusted Advisors who are themselves providing or intend to provide professional services (e.g. accountancy services where the TA is an accountant). This limitation will assist in mitigating the risk of non-accredited parties avoiding accreditation by obtaining CDR data via a TA Disclosure but then using the data in the same way an ADR would.

**(3) Nomination of Trusted Advisor –** The customer is best placed to determine whether they are comfortable for CDR data to be disclosed to a Trusted Advisor. To place the customer at the centre of this decision, the CDR Rules should require that the customer nominate/select the Trusted Advisor.

**(4) Customer must have transparency over each disclosure** – Given that disclosures may be to non-accredited parties, a high threshold of transparency should apply.

We support that the ADR be required to pre-notify the customer before disclosure of Insights or TA disclosures can take place, via their dashboard and seek from the customer a reconfirmation that they agree to the disclosure. This will help to safeguard against the sharing of discriminatory insights or insights that are incorrect (due to poor analytics or being based on incomplete data), and disclosures of CDR data which appear excessive to the Trusted Advisor's needs.

If inclusion of pre-notification in the dashboard is not possible, in the alternative, copies of disclosed data and insights should be required to be provided by the ADR to consumers, upon request. The Proposed Rules already contemplate the keeping and maintenance of records of disclosures to Trusted Advisors and a copy of each insight disclosed (under Rule 9.2 (eb) and (ec)). We do not consider this obligation to be an onerous additional burden. Although this would provide a lower level of protection to customers compared to pre-

notification, this would at least provide some transparency to customers and allow them to withdraw their consent for future disclosures.

## 5. Permitting use of CDR data for research

Where an ADR seeks to collect and use CDR data for the purpose of providing a CDR good or service, the Proposed Rules will allow ADRs to also seek the consumer's consent to use that same data for the purposes of "general research".

The definition of "general research" is broad –

> "general research, in relation to an accredited data recipient, means research by the accredited data recipient that does not relate to the provision of goods or services to any particular CDR consumer".

We understand that the drafting of research "not relating to the provision of goods or services to any particular CDR consumer", is intended to allow an ADR to expand its use of data to general product development or business improvement. However, the current wording could capture research that is unrelated to the ADR's core business or research that a customer would not reasonably expect their CDR data to be used for.

There are risks around businesses using this "General Research" consent in a way that was not intended, particularly in ways that support sales of other services. i.e. an ADR could conduct research on essentially any customer attribute/propensity and disclose this data to another business for a fee.

## 6. Secondary Users

EnergyAustralia supports the broadening of persons who can share CDR data with Accredited Persons. We also fully support the Secondary User mechanism and consider this a better solution compared to the Joint Account Holder arrangements. The Secondary User mechanism appears to be a flexible way to allow additional persons to share CDR data relating to an account, while retaining appropriate authorisations by the Account Holder.

The definition of "account privileges" may need to be reviewed for the energy sector which we will comment on in the ACCC's consultation on the draft energy CDR Rules. However, we wish to highlight the key consideration when considering Secondary Users – which is around ensuring that any risk of family violence is mitigated to the greatest extent possible, while also ensuring that customers who are at risk of family violence (Affected Customers) can still have access to the CDR.

Under the *Energy Retail Code* (Victoria) (Rule 106G), a retailer must not disclose or provide access to confidential information about an Affected Customer[9] to any other person (including a person who is or has been a joint account holder) without the consent of the Affected Customer. Confidential information refers to any information that may be used to identify or locate an Affected Customer, including information about their whereabouts, contact details, or financial or personal circumstances.

In the context of the CDR for the energy sector, this includes information about a customer and potentially metering data which could show when an Affected Customer is likely to be at home. It is also important to note that the family violence risk could apply both when the Affected Customer is the account holder and the perpetrator is the Secondary User and vice versa – but the risks appear to be higher when the Affected Customer is the account holder. This is because where the Affected Customer is the Secondary User they can choose not to share data on the account, even when a Secondary User instruction is in place (however, this does not cover situations where the Affected Customer might be coerced into sharing data).

The following measures could assist in addressing family violence risk related to Secondary User arrangements, and could be deployed individually or in combination:

[9] Affected Customer means any *customer*, including a former *customer*, who is or was a *small customer* and who may be affected by *family violence*

- Where an account is flagged as being linked to family violence risk *and* where there are additional account holders, the CDR Rules should recognise that the Data Holder can refuse to disclose CDR data and refuse to provide authorisation services. Where Data Holders have previously disclosed data and an account is subsequently flagged, a Data Holder should be able to withdraw CDR services. Rule 16.12.1 already provides that a Data Holder may refuse disclosure if necessary, to prevent physical or financial harm or abuse, but the ACCC should ensure this applies to the account flagged with family violence risk.
- Where there is a Secondary User, the contact details other than name (i.e. phone number and address) should not be disclosable to an ADR. That is, the disclosed information for Secondary User arrangements should relate to account information and not personal information about the Secondary User. The exception is metering data which relates to an account, and which could reveal the typical hours and days of the week that the Secondary User is at the premises; and so, this measure is not a full solution.
- On all transactions relating to a Secondary User instruction, a Data Holder should be able to receive and send directions to the Affected Customer's preferred method of communication (a safe method of communication). This is to safeguard against an Affected Customer being unable to openly take action due to their perpetrator being present. E.g. an Affected Customer should be able to withdraw a Secondary User instruction via their preferred method of communication.
- It is also highly important that authentication would also need to occur via the preferred method of communication.
- A reminder notification to both an account holder and Secondary User, to remind them that a Secondary User instruction is in place, should be sent periodically. Like Rule 4.20 which requires an ongoing notification requirement by ADRs in relation to certain consents, this reminder could be sent every 90 days since the instruction was put in place.
- A Secondary User should be able to decline or cancel the Secondary User instruction via their consumer dashboard provided by the ADR.

Separately, the Rules should clarify if the Secondary User instruction will apply to disclosures by an ADR (A1) (and not Data Holder) to Accredited Providers (A2) and non-accredited parties.