



30 October 2020

Consumer Data Right Division
Australian Competition and Consumer Commission
23 Marcus Clarke Street
CANBERRA ACT 2601

Lodged electronically: ACCC-CDR@acc.gov.au

Dear Sir/Madam

Consumer Data Right – Rules Expansion Amendments

Origin Energy appreciates the opportunity to provide input into the Australian Competition and Consumer Commission's (ACCC) Consumer Data Right (CDR) Rules Expansion Consultation Paper.

The proposed amendments represent a significant expansion of the CDR regime. We are concerned that the CDR Rules framework is now becoming increasingly complex with the focus of the CDR Rules expansion on the banking sector.

Running concurrent to this process is the ACCC's *Energy Rules framework* consultation to consider specific sectoral rules for CDR in energy or amendments to the Rules to accommodate the energy sector. We are concerned that the energy sector will be required to implement a considerably more complex framework as a result of these amendments without a robust assessment of whether the proposed level of functionality is required in the energy sector.

We believe there needs to be greater clarity on how these two processes interact and in particular how and when the expansion amendments are being considered in the *Energy Rules framework*.

These concerns have also been highlighted in the updated Privacy Impact Assessment (PIA). The PIA notes that the *“proposed amendments will introduce a number of new definitions, concepts and information flows, all at the same time. There are several inconsistencies and incomplete provisions in the proposed provisions..., which may make it difficult to understand the application and intention of those amendments”*¹. The PIA provides gap analysis and recommendations and Origin believes that the ACCC should adhere to addressing these recommendations prior to progressing these changes further.

We believe that it will be vital that the CDR Rules are simple but capture customer required functionalities so that the CDR scheme operates as intended. We have specific concerns regarding how the following elements of the expansion CDR Rules will operate:

1. Additional levels of accreditation to include a 'restricted' level of access to data;
2. The expansion of the outsourcing model to include Combined Accredited Persons (CAP);
3. The transfer of CDR data from one accredited data recipient (ADR) to another ADR and the tracking of data consent and information flows;
4. Disclosure to non-accredited persons such as accountants and lawyers;

¹ Maddocks, Update to the Privacy Impact Assessment – Consumer Data Right, 29 September 2020, P44

5. Ability to derive CDR 'insights' and the transfer of these insights to non-accredited parties; and
6. Additional functionalities for the consent process and whether CDR consumers will understand and engage in understanding why they are providing the consent.

These concerns are discussed further below.

1. Introducing new accreditation levels (Part 5 of the CDR Expansion Rules)

The current CDR Rules provide for one level of accreditation – this is at an 'unrestricted' level. This is considered the level of accreditation that ensures that ADRs have adequate system securities to request and hold CDR data. The ACCC is proposing to introduce new levels (tiers) of accreditation in the form of 'restricted' levels. The restricted level subcategories include²:

1. Limited data restriction – only certain data sets will be made available based on the relative risk of particular data sets;
2. Data enclave restriction – this requires a person accredited at the restricted level to have a relationship with an unrestricted ADR that has established a data 'enclave' (ie enclave provider); and
3. Affiliate restriction – a person accredited to the unrestricted level (sponsor) could certify to the Accreditor that it has a commercial relationship with the third party and is satisfied that it meets the relevant criteria.

We are concerned that a tiered accreditation will add unnecessary complexities with a requirement to segregate data sets to ensure that only the authorised data sets for the level of accreditation is provided to the accredited third party. The risks of data breaches increase with the system complexities to disaggregate data sets within data sets to provide only limited information to ADR 1, ADR 2, a non-accredited person or CAP Providers. The complexities with splitting data is evident with the energy billing data fields. There are considerable fields in relation to payments, tariffs, product information, concession or metering with a potential for these data fields to be provided to different entities.

Further, these sub-categories have the potential to introduce unnecessary reputational and operational risk to the CDR scheme. This in terms of the sophistication of entities that will be handling CDR data and complying with the CDR Rules. The potential for an entity to receive accreditation based on the 'association' or 'commercial relationship' with an existing ADR will not instil confidence in the market that they have appropriate system security and data control measures to operate. The ACCC would not have visibility to the robustness of systems and processes of these businesses and a data breach can have a significant negative impact on an industry.

We support the continuation of a standardised accreditation process as is in the current CDR Rules. A single tiered arrangement will provide for data security and efficiencies for accredited data recipients that operate across sectors as there is a single benchmark to satisfy in order to access to data. We do not view that allowing 'restricted' levels of accreditation will provide consumer confidence in the operation of the CDR scheme.

2. Combined Accredited Persons (CAP)

The CDR Rules propose that the current outsourcing arrangement will be expanded where an accredited outsourced service provider (CAP Provider) can collect CDR data from a data holder on

² ACCC, CDR Rules Expansion Amendments – Consultation Paper, September 2020, p13-19.

behalf of an ADR or CAP Principal (CAP Principal)³. That is, a CAP Provider would provide support functions (ie analyses of data) on behalf of a CAP Principal.

It is unclear to Origin whether the CAP Provider will have a consumer interface role of requesting consent or whether this will occur through the CAP Provider. Similarly, the information flows that will occur when there are changes to consent or authorisation on data sets and how this will be communicated through outsourced providers (ie CAP) to data holders.

The introduction of CAPs to the CDR framework adds a level of complexity to the management of data and we view that there are greater risks of information flow failures. We therefore believe that further use case scenarios should be worked through with industry prior to the Rules being extended to include them.

3. Transfer of CDR data from one ADR to another ADR

The proposed expanded CDR Rules will allow a consumer to consent to disclose CDR data from one ADR to another ADR in order to offer goods and services to consumers⁴. For example, one ADR may offer a product comparison service and recommend a product of another ADR.⁵ The proposed CDR Rules propose that appropriate consent must be in place with the respective ADRs prior to the disclosure of CDR data – this proposed consent process is supported.

A concerning aspect of this proposal is that it is not proposed that there be technical standards for the transfer of data between ADRs. Rather the format of the data transfer will be commercial agreements between the ADRs. This appears to go against the development of the scheme framework where there are standards and guidelines to direct the flow of information between ADRs and data holders. This format of data transfer will assist with the notification requirements for consumer dashboard obligations and to ensure that consumers are kept informed of the status of their data and who it has been transferred too. The non-standard could result in an ADR under reporting to a dashboard the level and content of data shared.

We note there will be a requirement that each ADR independently manage a consumer dashboard to notify the customer of the collection and transfer of CDR data. We question, from a customer experience point of view, how this will operate in practice. This is given one CDR consumer may have a minimum of three dashboards to navigate and manage – this is for ADR1, ADR2, data holders and any other party the CDR consumers provides consent to share data. We question whether the customer will become confused as to which dashboard is being used to manage consent and confusion if dashboard information is not timely updated between entities. This requires further consumer testing.

An added complexity for the energy sector with managing consents between ADRs is the presence of AEMO as the gateway. It is not clear to the energy sector whether the information flows for consent will be managed through the gateway or whether each of the ADRs will need a separate direct connection with a data holder. This is a complex issue that will need to be addressed in future energy framework consultations.

4. Disclosure to Trusted Advisors

The proposed CDR Rules will allow a consumer to nominate a trusted advisor, including non-accredited persons such as an accountant or lawyer to access CDR data. This is so the CDR consumer can receive professional services based on CDR data.

³ ACCC, CDR Rules Expansion Amendments – Consultation Paper, September 2020, p24

⁴ ACCC, CDR Rules Expansion Amendments – Consultation Paper, September 2020, p25

⁵ ACCC, CDR Rules Expansion Amendments – Consultation Paper, September 2020, p25

It is proposed that the format and scope of CDR data that an ADR could disclose to a trusted advisor will not be limited. We have concerns that without clear boundaries on requirements and obligations, it is possible that an ADR could become an intermediary that enables CDR to be transferred to other entities without being appropriately accredited to receive the data. It may become a 'loop hole' in the CDR scheme for an entity to receive data to provide a service. For example, a potential scenario could be that an ADR provides data to a financial broker for analysis without the financial broker having the systems in place to appropriately manage the data transferred. Under the general CDR model, the providing and analysis of data would require the entity to be accredited.

A further concern is once the data is transferred from an ADR to a non-accredited person, the CDR consumer protections will not apply as the data has been transferred out of the CDR eco-system. This raises the potential for data to be misused or consumers having limited abilities to pursue the entity if the data has been misused.

Given the potential risks and uncertainties with the use of the CDR data by non-accredited persons, we do not support the expansion of the CDR Rules to include them at this time. Further, consultation is required on the use case scenarios by non-accredited persons and ensure consumers rights in relation to the use of CDR data are protected.

5. Disclosure of CDR insights

The CDR Rules propose to permit ADRs to disclose an 'insight' directly derived from CDR data to any person, including non-accredited persons, with a customer's consent. We understand that an ADR could not disclose 'raw' CDR data as originally disclosed by the data holder to the ADR, but any derived nature of the data can be shared. Some examples of 'insights' include the outcome of product analysis (ie \$300 saving), verification of payments or expense verification⁶.

We believe the scope of directly derived data is too general for application in the CDR Rules framework. While we appreciate the CDR Rules is deliberately broad to cater for future scenarios of data innovation, there are 'grey' areas of how this would: 1) be interpreted by ADRs; and 2) whether consumers will understand the terminology for the release of certain data. For example, if an ADR receives payment history information from an energy customer based on monthly or quarterly billing and then collates the data to be a yearly history, is this considered a CDR insight? It is concerning that this could occur as the mere collation of the data to a yearly view could mean that it is transferred outside the protections of the CDR framework to a non-accredited person.

This is most likely to impact vulnerable customers who may not know or understand that the consent to transfer data insights may have a negative impact on them accessing a good or service. It is probable that an entity could use an 'insight' derived from energy data (ie customers payment history on an energy account) as part of a wider process to determine whether a customer is able to obtain additional financial credit. It is questionable whether a CDR consumer, at the time of providing the consent, would know that the insight data could be used in this manner.

We recommend removing the reference to CDR insights in the proposed CDR Rules. We appreciate in some industries derived data may be relevant from a CDR perspective, but the derived data concept (i.e., drawing the line between data capture and data not captured) would be difficult in the energy sector (and conducive to inconsistent application between ADRs) and subject to scrutiny and challenge by customers and the regulators (leading to inefficiencies). Limiting CDR data to well-defined data sets would provide the best level of clarity.

⁶ ACCC, CDR Rules Expansion Amendments – Consultation Paper, September 2020, p30

Should that recommendation not be accepted, a second-best option would be to tighten the scope of data 'insights' in a way that promotes innovation but carves out the risks that the CDR insights is used in a detrimental way to CDR consumers. This could include a requirement to explicitly explain the potential use of the data.

6. Consent

For the CDR scheme to achieve its' objectives, it must allow consumers to easily provide consent in an informed manner. More importantly, it must also provide customers with the confidence that their information will be protected and will only be used for the purpose and period consent was given.

The consent obligations and information flows will be paramount to the functioning of the scheme to ensure that data is not misused or incorrectly released. We urge the ACCC to work through use scenarios with regards to the proposed Rule amendments to ensure CDR consumers require additional consent functionalities and the consent requirements will not jeopardise the security of CDR data.

(1) CAP consent obligations

This level of complexity for the obtaining consent is going to be further exacerbated by the proposed introduction of Combined Accredited Person (CAP) and non-accredited parties as part of the consent process. This proposed outsourcing arrangement will allow CAP Providers to collect CDR data from a data holder on behalf of an ADR. However, it is unclear how the CAP Providers will be required to comply with the consent obligations and when it is considered that they are holding data. This needs to be addressed in the CDR Rules.

(2) Separate consents

The current CDR Rules have a combined concept of 'use and collection consent'. The ACCC is proposing to move away from this approach to allow separate consents for: 1) collection of CDR data; 2) consents to use CDR data; 3) direct marketing and 4) ability to disclose CDR data. This will allow greater flexibility for ADRs. For example, consent could be given to collect data for 7 days, consent to use data for 3 months, consent to direct marketing for 3 months and consent to disclose to a trusted advisor only once. Given the different levels of consent, the consumer could independently withdraw or amend consent at any time.

While it seems appropriate that these are separately categorised to allow customer choice for the collection and use of CDR data, we question whether the CDR consumer will understand the terms (ie collect, use or disclose) to which they have provided consent. It will be difficult to display on a screen all the information about the different data categories to which they are providing consent. The number of choices increases the risk that customers consent to data to which they did not understand they were consenting to be released or they provide consent for a longer period of time.

In relation to the energy sector, there are likely to be additional consent required for sensitive data sets such as if a CDR consumer is on a hardship plan, receiving a concession or on life support. It is proposed that the CDR consumer would need to explicitly provide consent to the release of this data given that DSB Consumer Experience (CX) research findings that some customers may not want this data shared. This adds another layer of complexity to the consent process.

Origin supports the ACCC undertaking further consultation on these proposed changes. This includes Consumer Experience testing with the DSB to test the functionality requirements and whether consumers understand the proposed policy direction with regards to consent.

(3) Amending consent

Under the current CDR Rules, in order to amend consent, consumers must create a new concurrent consent or remove an existing consent and replace it with a new one. The proposed CDR Rule will

extend functionality to allow adding or removing of uses, data types, accounts and the duration of the consent.

Where consumers amend consent, the proposed CDR Rules require the ADR to notify the data holder in order to invite the consumer to amend the corresponding authorisation. This allows consumers to amend their consents on an ADR's dashboard and allow ADRs to invite consumers to amend their consents.

It is unclear the time and the level of information that needs to be provided to the customer at the time of amending the consent. The timing will be important given that it is intended that the exchange of data occurs in a near real time manner and the level of information will determine the level of understanding to which they provided the consent. The flip side of this is that too many notifications will either disengage the CDR consumer from the process or confuse the customer as to the consent provided.

As the energy CDR framework is evolving, we are also questioning the consent flow and the obligations on data holders to register consent. We recognise that consent will be collected from the ADR at the time of a data request, however there is an ability for the customer to change the level of consent for the release of data at the authorisation level. Energy has the additional complexities with the existence of the gateway and information flows between all the entities will need to be worked through and documented.

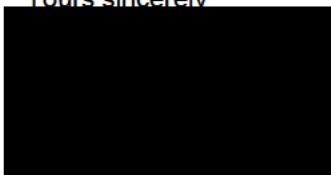
7. Timing for the commencement of the expansion CDR Rules

We are concerned with the proposed commencement of the enhanced CDR Rules in December 2020. It provides little time for addressing concerns raised as part of this consultation process and testing that the policy proposals will be operational efficient. There are a number of hurdles and potential costs that need to be reviewed prior to extending the CDR Rules.

Origin request the ACCC undertake further analyses of the implications of the CDR Rules and engage in further consumer experience testing prior to making these Rules. The greater the level of complexities to the implementation and management of the CDR scheme, the greater the privacy and compliance risks which will result in less entrants entering the market to offer services. This will be detrimental to both consumers and the operation of the CDR scheme.

If you have any questions regarding this submission, please contact [REDACTED] in the first instance on [REDACTED].

Yours sincerely



Sean Greenup
Group Manager Regulatory Policy