



AGL Energy Limited

T 02 9921 2999

F 02 9921 2552

agl.com.au

ABN: 74 115 061 375

Level 24, 200 George St

Sydney NSW 2000

Locked Bag 1837

St Leonards NSW 2065

Australian Competition and Consumer Commission

Consumer Data Right Division

29 October 2020

Consumer Data Right – rules expansion amendments consultation paper

AGL welcomes the opportunity to comment on the Australian Competition & Consumer Commission's (ACCC) Consumer Data Right (CDR) Rules Expansion Amendments Consultation Paper released on 30 September 2020 (CDR Rules amendments).

AGL supports the development and implementation of the CDR regime across the Australian economy, recognising the benefits that it can deliver consumers. The CDR regime is a significant and wide-reaching reform program that will be underpinned by consumer trust and comprehension in its operation. We note that the ACCC recognise the importance of consumer trust in data with ACCC Chair Rod Sims stating recently "you've got to have consumer trust in data. Once consumers start to mistrust it, we'll stop getting the benefits".¹

The CDR regime is meant to be founded on concepts of strong authentication, consumer control, trust and understanding to ensure consumers remain fully informed and at the centre of all transactions. The proposed CDR Rules amendments shift that foundation towards easier access and freer flows of consumers' data between businesses. We strongly encourage the ACCC to carry out analysis on consumer impacts and risks before proceeding with amending the CDR Rules.

We are concerned that the proposed CDR Rules amendments focus more on trying to lower costs to businesses without undertaking a fulsome assessment on how this is likely to impact consumers operating in a safe, transparent, and clear CDR regime. CDR is still only in its infancy for the banking sector and still being developed for the energy sector, and therefore consumer engagement and impacts remain relatively unknown and the ACCC proposal need to be carefully considered in this context.

In particular, AGL is concerned the proposed changes to the consumer engagement and consents process, including allowing greater data access by third parties (both accredited and non-accredited), and changes to the privacy safeguards and protections engrained within the CDR legislation, most notably that accreditation should act as the license for accessing CDR data, has not be subject to a rigorous customer

¹ Rod Simms at National Press Club on 22 October 2020



impact assessment. Further, these changes have not assessed how or whether they will promote greater consumer trust.

The Privacy Impact Assessment Update 2 (**PIA 2**) provides clear learnings to the ACCC's proposed CDR Rules amendments that should encourage a pause, and proper and greater consideration of consumer impacts be undertaken, most notably:

1. The complexity of the proposed CDR Rules amendments, introducing several new definitions, concepts and information flows all at the same time as well as inconsistencies and incomplete provisions within the amendments.
2. Lack of clarity around collection, use, holding and disclosure of CDR data with proposed new information flows.
3. Lack of clear information – specifically on how CDR consumers will understand the consents they are providing and how risks associated to 'information overload' will be managed.

These are three risks out of a total of 39 that remain unaddressed by the proposed CDR Rules amendments. There is no clear cost-benefit or customer impact analysis for these proposed changes, and therefore it is difficult to understand where the benefits for consumers are or whether the proposed reductions in industry costs outweigh any commensurate consumer confusion, costs and lower trust in the CDR regime

AGL's position is not against amending the CDR Rules to improve data flows, but rather to raise concerns about the rapid pace in which the ACCC is seeking to make these changes without adequate analysis or evidence to show that it will be consumers who benefit. Further, we do not believe the ACCC has adequately addressed concerns raised in the PIA 2 or provided detailed analysis of how consumers will be protected, and risks against them and data breaches or data misuse will be minimised.

There are elements of the proposed Rules amendments that we consider represent low risks for consumers and can be advanced in these amendments, including the principle of broadening to secondary-users, access for broader set of CDR consumers (including non-individuals) and principles around disclosures and helping consumers be informed.

If you have any questions, please contact Kat Burela on [REDACTED] or at [REDACTED].

Regards

Elizabeth Molyneux

General Manager Energy Markets Regulation



Executive Summary

The following submission details AGL's response to the proposed CDR Rules amendments. AGL has previously provided views on many of the topics raised in the CDR Rules amendments consultation paper and we urge the ACCC to consider this response in connection with those previous submissions. These can be accessed through the following links:

- Participation of non-accredited parties [and permitted disclosures](#) – February 2020
- Use of CDR Logos and withdrawal [of consents](#) – May 2020
- [General CDR Rules](#) (including transparency and CDR ecosystem) - May 2019
- Energy [rules framework \(including risks associated with tiering data\)](#)- August 2020

At the centre of the proposed CDR Rules amendments are a focus on improving data flows for businesses, without clear analysis and evidence on the consideration of a seamless and clear experience for consumers from the proposed changes. The ACCC refers to the Open Banking report, a report developed before the structure, mechanisms and strong privacy safeguards had been contemplated as the rationale with proceeding with the proposed changes. While the Open Banking recommendations show a possible way forward for the future of the CDR regime from an industry perspective, it should not come at the cost of robust evidence-based considerations of consumer impacts.

We note the proposed CDR Rules amendment consultation paper essentially offers limited actual evidence or experience of a consumer providing consents (including to multiple Accredited Data Recipients (**ADR**)), and yet introduces new use consents, collection consents and four types of disclosure consents. Wire frameworks of how each consent will operate should not be considered in isolation of one another, there must be a real consideration of how a consumer using the CDR framework will utilise services from an ADR and the likelihood of all the information disclosures and terms and conditions being considered across multiple differing consents including insights, research, non-accredited parties etc.

In the Privacy Impact Assessment Update 2 (**PIA 2**)², Maddocks has raised a number of questions and gaps that present risks to consumers under these proposed CDR Rules amendments. These consumer risks arise from the desire to provide a benefit to accredited parties regarding ease to access and transfer of data. Further, these consumer risks are not adequately addressed or considered by the ACCC in the consultation paper. For example, in relation to the **limited data restriction** model, the ACCC simply notes that the model does not consider the cumulative risks of data.

The proposed CDR Rules amendments consultation paper does not provide any advice on the need to move forward with such significant changes without being able to properly assess the initial implementation of the minimum viable product (**MVP**) for the banking sector. While we support timely regulatory change, we do not consider this should come at the expense of evidence-based consideration of the potential risks to consumers. For example, we do not believe there has been a meaningful analysis of consumer comprehension for the proposed expansions of all the new consents requirements (e.g. to non-accredited parties, tiered accreditation processes, data **transfers** between accredited persons, insights and research

² [Privacy Impact Assessment Update](#)



transfers). While the data standards body (DSB) has conducted research into the consents process, the real evidence will come from assessing the way consumers engage and comprehend the CDR system in a live environment. This is a concern that is echoed within the PIA update by Maddocks.³

Finally, the proposed CDR Rules amendments consultation paper refers to the Open Banking report as a binding series of steps for CDR progression that must be implemented as soon as possible. We believe the recommendations should not be implemented without the ACCC undertaking an evidence-based approach that ensure consumer expectations, outcomes and protections are at the centre of any expansion decisions.

³ [Privacy Impact Assessment Update](#), p.47, raises concerns about consumers not understanding consents that they are providing and will experience 'information overload'. Strongly encourage DSB consumer research on this to happen before finalising rule changes given the significance of these changes.



Accreditation and barriers to entry

Currently, businesses wanting to access CDR data must become accredited at the 'unrestricted level'. In the recent Fintech/Regtech Senate Committee review⁴, some stakeholders stated that the current accreditation requirements acted as a barrier to entry. In response to these concerns, the ACCC has proposed three new models for restricted accreditation.

1. Restricted level: **Limited data restriction**
2. Restricted level: **Data enclave restriction**
3. Restricted level: **Affiliate restriction**

We recognise the benefits of lowering barriers to entry and encourage this to be done in a way that is consistent with the founding principles of the CDR regime, which is to ensure consumer control and protection of CDR data. However, we do not believe that the mechanics and potential consumer impacts of each of the three models have been appropriately discussed in the proposed CDR Rules amendments consultation paper.

While the **Data enclave restriction** model, at a high level, appears to best embody the founding principles of the CDR regime of consumer protection, the mechanics of its operation on a provider basis has not been given sufficient attention or review. For example, it is unclear how consumers' data in an enclave arrangement would be protected from any screen recording software. When introducing these types of expansions to the CDR regime, the ACCC must have mind to fringe examples and/or nefarious uses that may negatively impact the consumer experience, to ensure that all adequate mitigations are put in place. Another important consideration is whether the screen presented data is obfuscated or tokenised such that the value of screen scraping would be negligible to the screen scraping actor and may lead to significant customer detriment on how this information is used to provide services.

Again, at a high level, the **Affiliate restriction** model appears to provide access to data while minimising accreditation costs for participants, however, it also relies on commercial arrangements and liabilities through contracts for any breaches or misuses of data, rather than on any initial confirmation by decision-makers of the appropriateness of the business to receive data. This will mean that there will not be detailed regulatory oversight before being able to access data, and instead relying on audit and reporting obligations to identify any consumer impacts or issues. We question whether this is in the consumers' interest. This model would be better suited for consideration when the current CDR framework has matured and there is greater consumer confidence and awareness of CDR.

We do not support the **Limited data restriction** model and provide further detail on this below.

Tiered accreditation will deliver benefits to both participants and consumers if developed with a consumer protection framework front-of-mind. Therefore, a slow expansion based on the Combined Accredited

⁴ See Parliament of Australia, [Financial Technology and Regulatory Technology](#) 2019-20.



Person (CAP) arrangements that have already been introduced into the ACCC CDR Rules, would likely present the lowest risks to the CDR regime.

Limited data restriction

The **Limited data restriction** model does not adequately consider the risks of data sets being combined, particularly as the CDR regime expands.

In our submission to the Energy Rules Framework, we provided significant information to the ACCC regarding risks of tiering data and classing some datasets as 'more sensitive'.³ We encourage the ACCC to consider this previous submission in relation to the **Limited data restriction** model, at a high level our comments relate to:

- Sensitivities related to data sets that do not immediately reveal a specific financial or medical fact about a customer but may nevertheless be considered sensitive, we provided an example of metering data insights.
- Interdependencies of data sets may allow the viewer to reverse engineer data and infer sensitive information; we provided the example of a customer's health status.
- Consumer education campaigns that need to start at a whole-of-system approach. Tiering data can impact the quality and effectiveness of services available to consumers and must be carefully considered by the ACCC in how these impacts are made clear to consumers.⁵
- Differences in CDR products and services due to a smaller subset of data. Specifically, CDR is intended to deliver consumer benefits relating to innovation and improved products/services, it is unclear how consumers will understand that some providers will only have access to a smaller subset data and therefore a full suite of analysis, services and products may not be available to them.

Both the Office of the Australian Information Commissioner (**OAIC**) and the **PIA 2**, raise concerns around the combination of data sets as a risk to consumer data.

- Maddocks notes in the PIA 2 that the **Limited data restriction** model focuses on cyber-security expert advice but does not consider the inherent sensitivity of individual consumers and the risks of exposure/mismanagement of their data. They state "we note that any banking transaction data is likely to be inherently sensitive and could potentially still expose CDR Consumers to risk it is mishandled, even if there are little security risks in relation to that CDR Data."⁶
- The OAIC recently raised concerns regarding the potential approach of 'lower tiers of accreditation for 'less sensitive' CDR data. The OAIC stating that "as CDR is rolled out across the economy and data sets can be combined, richer and more granular insights may be derived about individual consumers, meaning the overall privacy risks for consumers may increase".⁷ The OAIC recommends that the ACCC gather and consider evidence of handling sector-specific data as part of the exploration in to whether a lower tier of accreditation to CDR energy data is appropriate.⁸

⁵ See [AGL Hub – Submission to ACCC Energy Rules Framework](#) 28 August 2020, p.15.

⁶ See [Privacy Impact Assessment Update](#), p.79.

⁷ See [Office of Australian Information Commissioner submission](#) to the ACCC energy Rules Framework consultation, p.11-12.

⁸ *ibid*



We also refer to the recent consultation on DSB Decision Proposal 114 – Account Payloads. Under the energy designation instrument, concession information and hardship information are captured data types, these two are not interchangeable concepts.⁹ In our response to Proposal 114, we noted the inherent risks of exposure of highly sensitive information embedded in this data (e.g. that it is not uncommon for concession type definitions to embed within it a medical classification). What this means is there is a risk of this field being used to derive a customer’s medical condition. Merely adding in an additional step for consents does not guarantee the consumer will comprehend the different inferences (and therefore the impacts) that could be made at each level.

This is just one of many examples that the ACCC must consider and is compounded by the way each new subsequent sector has its data tiered (e.g. will energy concession information combined with banking information increase the risks of these data sets).

The proposed ‘bucketing’ of data on sensitivity grading does address what the ACCC recognises as the cumulative risks of CDR data. Until thorough consumer research is undertaken, and broader considerations of future designated sectors and data cumulation is considered, we urge the ACCC not to implement the **Limited data restriction** model while the CDR regime is in an infantile state.

Increasing ways for data to flow

The ACCC also contemplates how accredited persons can work together and how to improve data flows for positive customer outcomes. The three key topics here are:

1. The transfer of CDR data between accredited persons
2. Non-accredited parties' access to CDR data
3. Disclosure of CDR insights

These three categories are aimed at enabling CDR data to flow across a range of CDR and non-CDR participants, with the hope that these flows will result in positive customer outcomes. However, we encourage the ACCC to consider these three categories of data flow from a consumer-first perspective, being mindful of the strong privacy safeguards and protections enshrined within the CDR legislation to ensure a simple, clear and effective CDR regime for customers.

Transfer of CDR data between accredited persons

The ACCC is proposing the Rules allow for transfer of CDR data between accredited parties to facilitate an efficient data supply chain. This would most likely be based on commercial arrangements between accredited parties. From our reading of the proposed CDR Rules amendments:

- ADR's would be able to charge customers a fee for this service.
- ADR's can only seek customer consent for the transfer of data if they reasonably believe the customer may benefit from the good or service.

⁹ See [github consultation on proposal 114](#)



- The transfer of data between ADRs in this arrangement would not be prescribed by the data standards body / technical standards. The ACCC states that this can be done in line with commercial arrangements.

Our key comments on the above approach by the ACCC are set out below and we encourage further consideration and research before determining a final position:

- What rules will be in place to ensure that customers being charged a fee are made aware of this in a clear and transparent way during the consents process as the CDR legislation and designation instruments are clear on fee charging only in relation to specific data sets allowable under the designation instrument.
- What assessment of risks has been undertaken in regards to the transfer of data between ADRs in this arrangement (e.g. is there an enhanced risk of data exposure if ADRs choose to share CDR data in a way outside of the CDR API's, such as by email).
- If the ACCC establishes any disclosure statement requirements (e.g. that a fee will be charged for services), how will the ACCC ensure this message is clear and accessible for all kinds of consumers to minimise detriment?¹⁰
- Finally, it appears that this proposal of transfer of data between accredited persons is being introduced on an assumption that write access will be introduced into the CDR regime.

The final report for the Future Directions of the Consumer Data Right by Treasury is yet to be released and as such stakeholders are unaware of what (if any) recommendations are made regarding 'write access'. The proposal to allow ADR's to offer to transfer CDR data to another for the purposes of providing a recommended product will still then require action (e.g. contact such as email or phone) by the receiving accredited person.

Non-accredited parties' access to CDR data

We have previously provided comment to the ACCC and Treasury on the ability for non-accredited parties to access CDR data.¹¹ We do not consider that any of the information provided in this current consultation has provided an adequate response to our concerns which are:

- The Treasury CDR legislation acknowledges the importance of strong privacy safeguards.
- The explanatory memorandum of the CDR legislation placed significant weight on the importance of accreditation for the purposes of receiving data **calling it a licence to receive data through a disclosure made in accordance with the CDR Rules.**
- The explanatory memorandum notes that there is a limitation on the ACCC's rule making power, and that the ACCC can only write rules which mandate disclosure of CDR.

The proposed CDR Rules amendments do not have an obligation for non-accredited recipients to delete the data they receive, and as such consumers will not be afforded the same level of protection for the same sets of data. We consider this is counter to the strong privacy safeguards and importance of accreditation

¹⁰ [Privacy Impact Assessment Update](#)

¹¹ AGL Hub, [submission to CDR Rules for intermediaries and third parties](#), 2 February 2020, p.3.



established under the CDR. This proposal will mean that customers are not only expected to understand their new rights under the CDR regime, but then further to comprehend that CDR data shared under the regime to non-accredited recipients are not protected in the same way. This is an unnecessary confusion/perversion of the CDR system, as accountants and lawyers can become accredited if they so choose.

Further, we believe that such an approach will likely create consent fatigue, particularly when coupled with a range of other recommendations proposed under these amendments (see our earlier comments in the Executive Summary).

We do not believe that any professional classes should be able to access CDR data from ADRs and these should not be described in the Rules. Professional classes requiring CDR data can either become accredited, or request that consumers provide their CDR data directly themselves while making it clear that they are not afforded the same protections.

Disclosure of CDR insights

Should the ACCC proceed with making these rules, we agree that disclosures of CDR data to trusted advisors by ADRs be limited to situations where the ADR is providing a good or service directly to the consumer and strong measures put in place to ensure that ADRs do not act as mere data conduits to perverse the course of the CDR legislation and intention, including the strong privacy and consumer protections inbuilt to the regime.

While we strongly encourage the ACCC should make rules to restrict CDR insight disclosures to exclude raw CDR data, we note that there is a risk that CDR insights may be even more invasive than the raw CDR data. This concern is also raised by Maddocks in PIA 2 and does not appear to be appropriately addressed in these proposed amendments.¹² We also agree with Maddocks observations of potential risks relating to disclosures and encourage greater consideration by the ACCC to ensure that consent is free and fully informed on these matters.¹³

There may be value and business use cases available for disclosure of CDR insights, but as we have previously stated these must come from a customer-centric perspective given the purpose and nature of the CDR regime. At this stage, we do not consider there is sufficient detail in the ACCC Rules, or evidence that supports the proposed approach as being one that centres on more positive consumer outcomes – for all consumers and their individual circumstances.

Extending CDR to more consumers

The ACCC note that the Open-Banking review envisaged that all consumers (not limited by age, or business size) would be able to access CDR data. The proposed CDR Rules amendments would allow a broader range of consumers to access CDR data. While we agree with the intention of making CDR data more accessible to

¹² See [Privacy Impact Assessment Update](#)

¹³ Ibid



a range of consumers – it is important to ensure that these proposals are fit-for-purpose across a range of sectors and use cases that is based on explicit informed consent. We provide our comments on this below.

Non-individuals

The ACCC propose that businesses should be able to nominate individuals who are able to share CDR data. This would not be a blanket authority but based on an ‘opt-in’ model by the business. It would require a data holder to allow non-individual consumers to nominate individuals as ‘nominated representatives’ who can share CDR data and manage data sharing on their behalf. Businesses could nominate more than one representative for the purposes of CDR data management and consents. We support the extension of the rules to this category of consumers.

The ACCC state that in the event of one nominated representative having their access revoked, other nominated representatives would still be able to retain access and the consents will remain valid. If there was only one nominated representative, and their access was revoked (e.g. due to ending their employment) would this result in all consents and arrangements with ADRs being revoked? Greater clarity on the continuity of these types of arrangements is important.

Business partnerships

It is not clear from the proposed Rules amendments consultation paper how dashboards would be managed for business partnership arrangements. For example, would these be two separate dashboards for each partner?

Secondary users

The ACCC state that secondary users would be defined as those having relevant account privileges within sector-specific schedules of the Rules (e.g. that the banking wording is not necessarily how it will apply in energy). In this scenario, the account holder would approve a ‘secondary user instruction’ for a secondary user, to share CDR data relating to the account with accredited persons. Secondary users would then receive a dashboard (consistent with the approach for joint account holders).

The ACCC specifically state that current privileges that relate to secondary users (e.g. card holders) should not be automatically extended in the CDR context. Instead, the expectation is that the account holder will have to create a new CDR-specific ‘secondary user instruction’ – in other words, a CDR specific authorisation for people who are not the account holder’.

We agree with the ACCC’s proposal to establish a new CDR specific ‘secondary user instruction’ for the purposes of sharing CDR data. Both cross-sectorally, and even within industries (such as energy), businesses’ approach and management of authorised representatives on accounts can vary significantly. To ensure a fair and consistent approach across the economy, a CDR specific authorisation is the most appropriate and cost-effective way to allow secondary users to participate in the CDR.

Facilitating improved consumer experiences



Sharing data on joint accounts

The ACCC is proposing rules to allow data holders to refuse the disclosure of CDR data on a joint account or to update a dashboard if they consider it necessary to prevent physical or financial harm. This will allow vulnerable consumers to share CDR data on a joint account as if they account was held in their name alone.

We strongly support this proposal as it will allow retailers to put in measures to protect the most vulnerable consumers such as those that are impacted by family violence. AGL has a strong family violence supports program for customers, including flagging accounts of potentially impacted customers to ensure that additional safety measures are placed to prevent any nefarious or unlawful account information access.

Amending consents

Customer choice

Currently customers can amend a CDR consent either by having a new concurrent one or by removing the existing consent and replacing it with a new one. The proposed CDR Rules amendments seek to increase functionality that allows different attributes including adding or removing uses, data types, accounts, durations, etc. Further, the ACCC states this will not be prescriptive, and that ADRs will be able to choose which functionality they will provide to customers. If the consumer experience is not to be consistent across ADRs then there should be express provisions regarding transparency of what options are and are not available to consumers based on the ADRs service choices.

We also encourage the ACCC to allow data holders the ability to see/access consent amendment information to ensure data breaches do not occur once consents are amended. This is consistent with Maddocks position in the PIA Update where they state that CDR consumers should be able to see amendments to ADR dashboard reflected on DH dashboard to include their experience and access to information/control.¹⁴

ADR service

The ACCC also propose amending the rules to allow the ADR to invite the consumer to amend consents where the amendment would:

- 1) better enable the accredited person to provide the requested good/service
- 2) enable the accredited person to provide modified goods or services agreed to by the customer.

These limitations are proposed to ensure accredited persons are not 'spamming' consumers.

We believe the ACCC's proposed guardrails for preventing consumer overload is so broad that they are almost redundant in their application. If the ACCC wish to pursue this option, then it should be subject to further consumer testing before finalising rule changes. We encourage instead a time and/or content limitation on the consents amendments that can occur (e.g. that an ADR can only ask once every 3 months

¹⁴ See [Privacy Impact Assessment Update](#)



and can only ask for [up to 3] amendments). Information overload is a key driver for consumer disengagement and therefore must be appropriately managed within the Rules.

Separate consents

The ACCC proposed Rules amendments states that a consumer may have the following consents with an accredited person:

- Consent to collect for 24 hours;
- Consent to use for 3 months;
- Consent to direct marketing for 3 months;
- Consent to disclose to a trusted advisor on a single-occasion.

Given they are different consents, the consumer could independently withdraw or amend each consent. We agree that consumers should have greater flexibility in consent amendment and withdrawal. On this basis we also agree that combined consents should be excluded from the Rules.

Further, while we strongly disagree that disclosures should be allowed to 'trusted advisors' that are not accredited, should the ACCC pursue this then disclosure consent should only be allowed after an original consent is in place. The disclaimer information should be prescribed within the data standards to ensure a clear, consistent and consumer accessible packet of information on the risks of disclosing outside of the CDR system are in place.

Point in time redundancy

The ACCC note that under the current Rules, customers will experience different outcomes if they withdraw consents depending on how their consents have been established (e.g. with a single data holder, multiple data holders and joint accounts).

AGL believes different outcomes may create confusion for consumers and therefore we do not support a consistent CDR education and consumer awareness campaign informing consumers of their rights and protections (such as deletion and de-identification). Rather, we encourage further consumer research and consultation with stakeholders on the mechanics of point-in-time redundancies to ensure that consumers will understand that a revocation of their consent for one part of their data will not provide for the data collected to-date to be deleted. Any education and awareness campaign should be informed by this consumer research.

Other matters

AGL provides the feedback on the following matters raised in the proposed Rules amendments consultation paper:

- **Using the CDR Logo** - We support the ACCC's proposal to suspend or revoke ADR accreditation if they do not comply with the data standards for CDR logo use. As we have previously noted, the CDR logo will be an important tool for businesses and government to establish trust and recognition in the broader economy.¹⁵

¹⁵ See our previous submission to the ACCC on the [AGL Hub](#).



- **Permitting use of CDR data for research** – as with our comments above regarding the purpose of the CDR regime, we do not support expanding CDR data access outside of accredited recipients. We encourage the ACCC to consider how those wanting to conduct research can gain access and consents through the established accreditation model to ensure that it is appropriately managed and protected. recommend that those seeking to use CDR data for research should require accreditation as with any other party seeking to access CDR data.