Australian Government
The Treasury

Consumer Data Right

Operational Enhancements

Consumer Data Right rules design paper

August 2023

Table of Contents

Purpose of this design paper

This design paper seeks stakeholder feedback to support the development of changes to the *Competition and Consumer (Consumer Data Right) Rules 2020* (the CDR Rules) to ensure they are fit-for-purpose and support the policy aims of the Consumer Data Right (the CDR).

The design paper draws on a range of sources, including submissions received in response to previous consultations about possible amendments to the CDR Rules, and submissions received in response to the 2022 CDR Rules maintenance consultation process. The design paper is separated into three parts:

- proposed changes to the rules of general application
- proposed changes to the energy-specific rules
- issues for future consideration.

No changes to the other sector-specific rules are proposed.

The role of the CDR Rules

The CDR Rules consist of rules of general application, which have been developed to apply universally across all sectors of the economy, and sector-specific schedules (for example, the banking sector rules are set out in Schedule 3). The rules of general application are separated into nine parts.

Part 1 includes a simplified outline and overview of the rules and defines key terms. It also sets out:

- key concepts (such as the criteria for assessing fitness and propriety to receive data as an accredited person, who is an eligible CDR consumer, what is voluntary and required product and consumer data, the types of consent that may be given by CDR consumers, and the characteristics of sponsorship, outsourcing and CDR representative arrangements)
- general provisions relating to data holders and accredited persons, including dashboard requirements and requirements for de-identifying and deleting data.

Part 2 sets out requirements for the disclosure of product data by a data holder in response to a valid request. Product data relates to the characteristics of products offered by data holders. It does not relate to individual CDR consumers.

Part 3 sets out requirements for the disclosure of consumer data in response to a request made directly by that consumer. This Part is not currently operational.

Part 4 sets out requirements for the disclosure of data about a CDR consumer in response to a request made on behalf of the consumer by an accredited person. This Part contains a range of requirements in relation to the processes for seeking consents and authorisations from CDR consumers. Part 4A sets out modifications to these requirements in the context of CDR data relating to joint accounts.

Part 5 specifies the criteria that need to be met for an entity to become an accredited person; ongoing obligations of accredited persons, including in relation to internal and external dispute resolution processes; rules relating to the Register of Accredited Persons; and the powers and responsibilities of the Australian Competition and Consumer Commission (the ACCC) as the Data Recipient Accreditor.

Part 6 sets out requirements on data holders for internal and external dispute resolution processes.

Part 7 sets out rules relating to the CDR's privacy safeguards, which are contained in the *Competition and Consumer Act 2010* (the Act). This Part sets out a range of obligations in respect of the management of CDR data and the processes that must be used by entities participating in the CDR in order to ensure the integrity and security of CDR data.

Part 8 sets out rules relating to data standards. These cover matters including the functions and procedures of the Data Standards Advisory Committee, processes for making data standards, and types of standards that must be made.

Part 9 includes the record keeping and reporting obligations placed on data holders and accredited persons, and the powers of the Australian Information Commissioner and the ACCC to request documents and conduct audits.

Treasury is responsible for advising the Minister, who has the authority to make and amend the CDR Rules, on amendments to maintain and expand the regime.

Data Standards

The data standards are developed and maintained by the Data Standards Body (the DSB) in the Treasury and made by the Data Standards Chair in accordance with the CDR Rules. The data standards for consumer experience, security profile and application programming interface (API) definitions are published on the Consumer Data Standards website.

The Consumer Experience Guidelines (CX Guidelines) provide best practice recommendations and optional implementation examples for key rules data standards. They include annotated wireframes, open-source assets, prototypes, and a checklist outlining key requirements. The CX Guidelines assist CDR implementation in the banking and energy sectors.

The data standards are publicly consulted on using GitHub. Change requests to the data standards and CX Guidelines can also be raised on the standards maintenance site.

Consultation on this design paper

Treasury seeks feedback on the proposed policy approach and consultation questions set out in this paper by **6 October 2023**. Feedback can be provided via email to CDRRules@treasury.gov.au.

Treasury has engaged a supplier to conduct a Privacy Impact Assessment (PIA) considering the privacy risks of making the changes to the CDR Rules for the proposed operational enhancements. Treasury welcomes feedback on any privacy issues or risks that should be addressed in the PIA.

Feedback provided in response to this paper will be used to develop exposure draft amendments and will inform Treasury's advice to the Minister. Stakeholders will have a further opportunity to provide feedback on draft rules and data standards at a later stage.

Issues for Feedback – Rules of general application

1. Secondary users

Giving and withdrawing secondary user instructions

Data holders must provide account holders with the ability to allow a secondary user of an account to initiate sharing of CDR data from the account (known as a 'secondary user instruction'). They must also allow account holders to withdraw that instruction in order to cease all CDR data sharing from that account on behalf of the secondary user.[1]

However, the CDR Rules do not currently require data holders to provide functionality allowing account holders to *give* secondary user instructions online (although functionality to *withdraw* secondary user instructions must be available online).[2]

Blocking secondary user data sharing to a particular accredited person

Where an account holder has given a secondary user instruction in relation to an account, they must also be able to indicate they no longer approve of data from that account being shared on behalf of the secondary user with a particular accredited person.[3] This indication permanently 'blocks' account data from being shared by the secondary user with that accredited person, but still allows the secondary user to initiate data sharing with other accredited persons.

Treasury has received feedback from both data holders and ADRs which raised concerns in relation to the secondary user blocking requirement, including:

- the requirement for data holders to offer blocking functionality in relation to a particular accredited person does not reflect the reality of how data sharing arrangements are structured. If an account holder indicates that secondary user data sharing with a particular accredited person should stop, this usually means the data holder must stop sharing data with all the accredited person's CDR representatives, affiliates, brands and/or software products. This outcome may be inconsistent with the intention of the account holder.
    - It may also not be clear to the account holder which accredited person they need to block to stop data sharing with the relevant CDR representative/affiliate, brand and/or software products.
- the rules do not require data holders to provide functionality that allows this indication to be reversed, raising the possibility that an account holder could inadvertently permanently block data on behalf of a secondary user with a particular accredited person.
- it is possible an account holder would choose to block secondary user data sharing without informing the secondary user, raising complexities in terms of how notifications to the secondary user should be managed.
- the blocking requirements in relation to secondary users are not consistent with the requirements for data holders in relation to joint accounts, which require

[1] CDR Rules 2020, r 1.7 (definitions of 'secondary user' and 'secondary user instruction') and 1.13(1)(e).
[2] CDR Rules 2020, r 1.15(5)(b)(ii).
[3] CDR Rules 2020, rr 1.15(5)(b)(i) and 4.6A(a)(ii).

data holders to allow account holders to manage approvals in relation to authorisations, rather than in relation to accredited persons.[4]

Various alternatives to the current requirement (that data holders must allow an account holder to block data sharing initiated by a secondary user in relation to a particular accredited person) have been put forward by stakeholders. Nevertheless, the majority of submissions received to date suggest it should be replaced with a requirement to allow an account holder to block data sharing initiated by a secondary user in relation to a particular authorisation.

In the meantime, the DSB and the ACCC have published a knowledge article in relation to these issues.[5]

Proposed approach

Treasury is considering the following changes to the CDR Rules to address the issues raised by stakeholders:

- amendments to require data holders to provide an online secondary user instruction management service that includes giving, not just withdrawing, secondary user instructions.
- amendments to require data holders to provide online functionality that allows account holders to block secondary user data sharing by indicating they wish the sharing of CDR data by a secondary user to be stopped in relation to a particular authorisation, rather than a particular accredited person, and to also allow account holders to withdraw such indications.
  - It may also be desirable for data holders to be required to notify an account holder who gives such an indication that the secondary user could give a new authorisation to share CDR data with the same recipient. If the account holder preferred, it would be open to them to withdraw the secondary user instruction altogether, to prevent any sharing of CDR data from the account on behalf of that particular secondary user. Treasury welcomes feedback on whether this notification would be beneficial.

Treasury is also seeking feedback on any supporting amendments required to facilitate appropriate dashboard functionality and notifications. For example, rule amendments and/or new data standards may be required to clarify:

- how data holders should notify secondary users of actions taken by the account holder that affect their ability to request data to be shared in relation to an account.
- where an account holder has indicated they would like to block data sharing in relation to a secondary user's authorisation, how this should be presented on consumer dashboards.

[4] CDR Rules 2020, r 4A.13(1)(d).
[5] https://cdr-support.zendesk.com/hc/en-us/articles/5465006047375-Ceasing-Secondary-User-Sharing.

- what information should be included on the account holder's and secondary user's consumer dashboards to reflect the status of an authorisation which has been given by a secondary user and 'blocked' by the account holder.

Consultation questions

1.1 Would these proposals help resolve the difficulties faced by the CDR community in implementing secondary user data sharing blocking requirements?

1.2 Would the proposals create any new implementation issues that require consideration?

1.3 If amendments are made so that the current requirement for data holders to provide functionality for account holders to prevent secondary user data sharing in relation to a particular accredited person is no longer mandatory, should the rules still allow this to be offered as an optional functionality?

1.4 Are any other supporting amendments required to facilitate appropriate dashboard functionality and notifications?

1.5 What, if any, data standards would be necessary to support the changes?

1.6 Are there any factors Treasury should consider about the timing of any changes?

2. Nominated representatives

A data holder must provide, for each eligible CDR consumer that is not an individual, and for each partnership that relates to a partnership account with the data holder, a service that can be used to:

- nominate one or more individuals 18 years of age or older (nominated representatives) who are able to give, amend and manage authorisations to disclose CDR data for the purposes of these rules on behalf of the CDR consumer.
- revoke such a nomination.[6]

The nominated representative appointment mechanism is designed to enable non-individuals (for example, businesses and partnerships) to nominate who can authorise the sharing of their CDR data.

Process for appointing a nominated representative

The requirements for data holders to offer a nominated representative appointment process are principle-based rather than prescriptive. This was intended to allow data holders to leverage existing processes for individuals' appointments to business accounts. It also acknowledged the diversity of these consumers, and the complexity of their arrangements with data holders.

Stakeholders have submitted that current processes for appointing a nominated representative can be confusing for holders of business accounts. To the extent they discourage business consumers from using the CDR, they also reinforce the continued use of existing data sharing channels like screen scraping.

[6] CDR Rules 2020, r 1.13(1)(c).

As an alternative, stakeholders have submitted that account administrators who already have unlimited permissions should not be required to go through an additional process with their data holder to be appointed as a nominated representative for CDR data sharing.

Visibility of authorisations given by nominated representatives

Treasury has also received feedback from stakeholders suggesting that, where a CDR consumer appoints a nominated representative, or nominated representatives, to manage authorisations, it is possible that different people will give authorisations on behalf of that CDR consumer (if, for example, the original nominated representative is later replaced). Stakeholders have expressed concern that this will affect visibility of authorisations over time, together with visibility of related consents given to ADRs or CDR representatives.

Proposed approach

Process for appointing a nominated representative

Treasury is considering possible amendments to the CDR Rules to require that data holders implement a process for appointing a nominated representative that a reasonable person would consider quick, easy to find, easy to understand and easy to use.

Treasury is also seeking stakeholder feedback on whether:

- data holders should be required to provide an online mechanism for appointing nominated representatives (although CDR consumers could continue to use any paper-based nomination services offered by the data holder).
- account administrators of non-individual and partnership accounts should be deemed by the rules to be nominated representatives in relation to those accounts, unless the consumer has indicated they do not agree to this or the nomination has been revoked. The CDR Rules would continue to allow the nomination to be revoked at any time.[7]

Additional dashboard requirements for data holders

To address the issues raised above about ongoing visibility of authorisations given by nominated representatives, as well as visibility of related consents given to ADRs or CDR representatives, Treasury is seeking stakeholder feedback on whether it would be desirable to:

- where an authorisation has been given, amended or withdrawn by a nominated representative, require data holders to identify the nominated representative that gave, amended or withdrew the authorisation on the consumer's dashboard. This may better enable business consumers to keep track of authorisations given on their behalf.
- require data holders to include a note on each CDR consumer dashboard that the dashboard does not display consents given to ADRs or CDR representatives, that such consents must be managed through the relevant ADR dashboard(s) and that they may continue to be active after the relevant authorisation has expired.

[7] CDR Rules 2020, r 1.13(1)(c).

- There would be no requirement to include details of any consents in this note, given that data holders do not have this information. The purpose of the note would be to alert consumers to the fact that their data holder dashboard does not give them visibility of consents given to ADRs or CDR representatives.

Consultation questions

2.1 Do stakeholders consider the proposed approach to modify the CDR Rules to require the data holder's nominated representative appointment process to be quick, easy to find, easy to understand and easy to use a desirable change?

2.2 Should data holders be required to provide an online mechanism for appointing nominated representatives?

2.3 Should the rules automatically require any account administrators of a non-individual or partnership account be a nominated representative in relation to the account (unless the consumer has indicated they do not agree to this or the nomination has been revoked)?

2.4 Should data holders be required to identify the nominated representative who gave an authorisation in the consumer dashboard?

2.5 Should data holders be required to include a note on each consumer dashboard, stating that the data holder dashboard does not display consents given to ADRs or CDR representatives?

3. Avoidance of harm

As a general rule, data holders are required to share data when they receive a valid request from an accredited person. However, a data holder is exempt from this requirement in some circumstances, including where it considers refusal to share data is necessary to prevent physical, psychological or financial harm or abuse.[8] In these circumstances, the data holder's options are limited to either sharing data in full compliance with the rules, or not sharing data at all. Data holders are not, for example, able to share data without having to comply with the requirements to provide notifications or records.

There is a more comprehensive *avoidance of harm* provision that applies to joint accounts, which provides that a data holder is not liable for a failure to comply with its obligations if it considers that the relevant act or omission is necessary in order to prevent physical, psychological or financial harm or abuse to any person.[9] This allows the data holder to share data at the request of a joint account holder who may, for example, be seeking to use CDR data in preparation for leaving an abusive relationship, without complying with notification requirements that would alert the perpetrator to the request.

However, this avoidance of harm provision is limited to data holder obligations in relation to joint accounts, so it does not apply to the data holder's obligation to provide certain records to a CDR consumer.[10] Under these obligations, data holders are required to provide any of the holders of a joint account with records relating to the sharing of CDR data from

[8] CDR Rules 2020, r 4.7.
[9] CDR Rules 2020, r 4A.15.
[10] CDR Rules 2020, r 9.5.

that account, if requested. As a result, it is possible that information would be disclosed to an account holder in the form of data holder records, that would have otherwise been withheld to prevent harm to another account holder.

These settings create two issues:

- data holders have more flexibility to choose how to comply with their obligations to prevent harm in the context of joint accounts than they have in other data sharing contexts.
- flexibility to avoid harm or abuse, even for joint accounts, can be undermined by obligations that do not relate directly to data requests, such as obligations to provide records to consumers.

To address these issues, stakeholders have suggested that an avoidance of harm provision, similar to that available for joint accounts, should be applied to all data sharing requests. Stakeholders have also suggested that avoidance of harm provisions should be expanded so that data holders are not required to comply with obligations to provide records to CDR consumers where they consider such non-compliance necessary to prevent harm or abuse.

Proposed approach

Treasury is considering rule amendments to:

- expand the avoidance of harm provisions currently applicable to joint accounts so that data holders are not required to comply with obligations to provide records under rule 9.5 to one account holder where this might cause harm to another account holder.
- make similar avoidance of harm mechanisms available to data holders responding to requests that relate to accounts other than joint accounts where they consider compliance would result in physical, psychological or financial harm or abuse to any person, such as secondary users and third parties.

Consultation questions

3.1 Are there other circumstances, not set out above, where a data holder's obligations to comply with the CDR Rules could cause harm to a joint account holder, secondary user or third party in which the proposed avoidance of harm protections may not result in the intended outcome?

3.2 Is there a risk the proposed changes could significantly impact data sharing under the CDR? If so, is there a different approach that could be taken?

4. CDR representative arrangements

The CDR representative model, introduced in 2021, enables unaccredited persons (CDR representatives), to provide goods and services to consumers using CDR data under the supervision of a person with unrestricted accreditation.[11]

[11]The *Corporations Act 2001* (the Corporations Act) provides a precedent for representative style arrangements, allowing Australian Financial Services licensees to appoint 'authorised representatives' to provide specified financial services on its behalf. See Division 5 of Part 7.6 of the Corporations Act, including ss 916A, 916B and 916F.

The CDR representative model relies on a contractual arrangement known as the 'CDR representative arrangement' between an accredited person with unrestricted accreditation (CDR representative principal) and an unaccredited person (CDR representative). The CDR Rules set out mandatory terms that must be included in a CDR representative arrangement, including terms imposing obligations on CDR representatives which largely align with certain conditions imposed on accredited persons.[12] The CDR representative principal must ensure that their CDR representative complies with the mandatory terms of their arrangement. Failure to do so may result in enforcement action.[13]

In addition, the CDR Rules require ADRs to hold adequate insurance, or comparable guarantee, in light of the risk of CDR consumers not being properly compensated for any loss that might reasonably be expected to arise from a breach of obligations related to the management of CDR data.[14] For CDR representative principals and OSP principals, this insurance obligation extends to the management of CDR data held by their CDR representatives (as well as any direct or indirect OSPs engaged by the ADR or their CDR representatives).

The CDR representative model has driven a substantial increase in participation in the CDR. As the CDR matures, Treasury considers it desirable to ensure the model is operating as intended by strengthening and clarifying the requirements on principals and CDR representatives. To support compliance with existing obligations under the CDR Rules, Treasury is also considering amendments that would expand CDR regulators' auditing and intervention capabilities, with the intention of strengthening consumer protections.

Proposed approach

Treasury is considering amendments to the CDR Rules to strengthen and clarify the requirements on principals and CDR representatives.

ACCC powers to intervene to protect consumers

Treasury is considering amendments to the CDR Rules to allow the ACCC to intervene to:

- prevent CDR data from being shared by a principal with their CDR representative
- remove a CDR representative from the Register of Accredited Persons (the register)

where it reasonably believes this is necessary to protect consumers.

The proposed changes would allow the ACCC to intervene at any point in the life of the arrangement, including prior to the CDR representative's details being entered on the register or after data sharing has commenced.

Adequate insurance

To clarify and strengthen current insurance obligations, Treasury is considering amendments to:

[12] CDR Rules 2020, r 1.10AA.
[13] CDR Rules 2020, rr 1.16A(2) and 9.8.
[14] CDR Rules 2020, r 5.12(2)(b).

- clarify that, where an ADR's CDR representatives and OSPs have their own comparable insurance, this may be relevant to an assessment of whether the ADR has met the insurance requirements. This could ensure there is flexibility as to which entity holds the necessary insurance.
- Strengthen the ACCC's ability to monitor insurance arrangements by requiring ADRs to keep records of how they have complied with their insurance requirements, including evidence of insurance that covers their CDR representative and OSP arrangements.
- make ADRs subject to a civil penalty provision if they fail to hold adequate insurance, including coverage of any CDR representatives or OSPs.

Auditing, record-keeping and reporting

Treasury is considering amendments to strengthen auditing powers in relation to CDR representatives.[15] In particular, the change could support the ACCC and the Office of the Australian Information Commissioner (OAIC) to monitor compliance in relation to their CDR representative principal under the CDR Rules.[16]

If introduced, for example, CDR representative principals may be subject to a civil penalty provision if their CDR representative fails to comply with a written notice from the ACCC or the Information Commissioner requesting the CDR representative to produce copies of certain records, including information from those records.

Treasury is also considering whether any additional record-keeping or reporting requirements for CDR representative principals are needed. For example, Treasury is considering whether principals should be required to keep records about and/or report on:

- a CDR representative's compliance with information security obligations.
- their cyber security practices.

'Fit and proper person' assessment

Treasury is considering amendments to require accredited persons to consider the fitness and propriety of prospective CDR representatives. This requirement would only apply to CDR representative arrangements entered into after the relevant rules are made.

Accredited persons could be required to assess their prospective CDR representatives against objective criteria. These criteria could be wholly or partially based on the existing criteria for accreditation applicants.[17] For example, the accredited person could be required to ensure that prospective CDR representatives have not been convicted of a serious criminal offence or an offence of dishonesty within the last 10 years.

If made, this change could be supported by the proposed changes to allow the ACCC to intervene in CDR representative arrangements where it reasonably believes this is necessary to protect consumers.

Treasury is also considering whether, if this requirement is introduced, CDR representative principals should be subject to a civil penalty provision if they fail to comply.

[15] CDR Rules 2020, r 9.6.
[16] CDR Rules 2020, r 9.6.
[17] CDR Rules 2020, r 1.9 sets out the fit and proper person criteria accreditation applicants are assessed against.

Consultation questions

4.1 What impact would the proposed changes have on the attractiveness of the representative model as a pathway to CDR participation? Would they give rise to any unintended consequences?

4.2 Would the proposed changes benefit CDR consumers and increase confidence in the CDR?

4.3 Are there other measures that would better ensure proactive oversight over CDR representatives by principals without creating unnecessary regulatory burden?

4.4 Treasury is considering new record keeping or reporting requirements for CDR representative principals. Would it be preferrable to only create new record keeping requirements, rather than adding to CDR representative principals' reporting obligations?

4.5 To what extent should the criteria used to assess the fitness and propriety of accreditation applicants be considered by an accredited person when assessing the fitness and propriety of a prospective CDR representative? Would alternative criteria be preferable?

4.6 Should any equivalent changes also be made to the rules about CDR outsourcing arrangements and outsourced service providers (where relevant)?

5. Obligation to handle all CDR data received from a principal as service data

The CDR Rules allow ADRs to become principals in CDR outsourcing arrangements and CDR representative arrangements. A CDR outsourcing arrangement permits OSPs to assist an ADR or CDR representative to provide services to CDR consumers, while a CDR representative arrangement allows an unaccredited person to provide their own services to CDR consumers but under the supervision of their principal ADR. Both OSPs and CDR representatives have a range of contractual obligations for protecting the CDR data they receive as service data for the purpose of the arrangement with their principals.[18]

CDR data may be disclosed by an ADR to a trusted adviser of a CDR consumer under a trusted adviser disclosure consent, or to a specified person under an insight disclosure consent or business consumer disclosure consent.[19] While a trusted adviser needs to belong to a class of the regulated professions (for example, accountants or solicitors), [20] trusted advisers and specified persons do not need to be accredited to receive data from an ADR. Unlike CDR representatives and OSPs, the CDR Rules do not place any requirements on how CDR data must be handled by trusted advisers and specified persons once it has been received from the ADR.

[18] CDR Rules 2020, rr 1.10 and 1.10AA. These provisions set out the contractual terms that must be included in CDR outsourcing and CDR representative arrangements, including requirements in relation to the protection, use and disclosure of service data. 'Service data' is defined by the CDR Rules to mean CDR data disclosed to, or collected by, the CDR representative or OSP for the purposes of a relevant CDR representative or outsourcing arrangement.
[19] CDR Rules 2020, r 1.10A. Business consumer disclosure consents can be offered by ADRs from 1 December 2023 or, if relevant data standards are made earlier, from the day those standards are made.
[20] CDR Rules 2020, r 1.10C.

Stakeholder feedback indicates the rules would benefit from greater clarity about the data security requirements for OSPs and CDR representatives who fall within a class of persons who can be a trusted adviser under the CDR Rules. For example, stakeholders have suggested there is a lack of clarity about whether a registered accountant could apply the less rigorous obligations that apply to trusted advisers to all CDR data they receive, instead of the more rigorous requirements that apply under their CDR representative or arrangement.

Proposed approach

Treasury is considering amendments to clarify that an OSP or CDR representative who receives CDR data from an ADR who is their principal must, in all cases, comply with their obligations under the relevant agreement in respect of that data as though it were service data received for the purposes of their OSP or CDR representative arrangement, and apply CDR protections to it.

This would mean that if an OSP or CDR representative received data under a trusted adviser or insight disclosure consent from an entity who is their ADR principal, the OSP or CDR representative would need to treat the data as service data. However, if the same entity received this data from an ADR with whom they have no OSP or CDR representative arrangement, they would not have to treat it as service data (in other words, their obligations in relation to that data would be the same as any other recipient of CDR data under a trusted adviser disclosure consent or an insight disclosure consent).

Consultation questions

5.1 Would the proposed amendment clarify expectations for OSPs and CDR representatives who are also able to receive data under a disclosure consent?

5.2 Would the proposed amendment have any unintended consequences for ADRs, CDR representatives, outsourced service providers or CDR consumers?

6. Consent continuity for CDR representatives and affiliates granted unrestricted accreditation

As the CDR matures, Treasury expects CDR representatives and affiliates will seek unrestricted accreditation, meaning they will no longer be operating under the supervision of an unrestricted ADR and will be able to collect CDR data directly from a data holder. In both cases, this would require the entity to demonstrate enhanced capabilities for consumer protection and information security in order to meet their accreditation requirements. They would also be subject to civil penalties for non-compliance with their obligations under the Act and the CDR Rules. In these circumstances, Treasury considers it desirable to ensure any consents given by consumers to a CDR representative or affiliate who is subsequently granted unrestricted accreditation can continue to operate with minimal disruption to the consumer.

Proposed approach

Treasury proposes to amend the CDR Rules to ensure that, in the event a CDR representative or an affiliate is granted unrestricted accreditation, there will be minimal disruption to any active consents, but that CDR consumers are appropriately notified of the change. For example, it may be desirable for the entity moving to unrestricted accreditation to notify

CDR consumers with active consents about the change in accreditation status, explain any consequences, and remind them that they can withdraw their consents at any time. Where an active consent continues after the CDR representative or affiliate is granted unrestricted accreditation, it may also be desirable for historical information relevant to that consent to continue to be available to the consumer.

The proposed amendments would not extend to circumstances where a CDR representative becomes an affiliate, given that affiliates must still rely on an unrestricted ADR to manage the collection of CDR data from a data holder on their behalf. Treasury welcomes feedback from stakeholders about whether the proposed amendments are desirable, if any limitations or consumer notifications should apply and whether excluding circumstances where a CDR representative becomes an affiliate could have any unintended consequences.

Consultation questions

6.1 If amendments are made to ensure there are minimal disruptions to active consents where a CDR representative or affiliate is granted unrestricted accreditation, should affected CDR consumers be notified of the change to their service provider's accreditation status? If so, what information should these notifications include, and when should they be given?

6.2 If the proposed amendments are made, a CDR representative who is granted unrestricted accreditation would become responsible for maintaining consumer dashboards. Where an active consent continues after the CDR representative is granted unrestricted accreditation, should historical information relevant to that consent continue to be available to the consumer?

6.2.1 Should consumers be notified, and given the opportunity to withdraw consent, prior to the CDR representative or affiliate gaining unrestricted accreditation?

6.2.2 What information should be provided to the consumer about ongoing collection and handling of CDR data, and which party should be responsible for handling historical information in relation to a consent which pre-dates the CDR representative or affiliate gaining unrestricted accreditation?

6.3 How should the data holder dashboard reflect the fact that the relevant authorisation relates to an entity with a changed accreditation level, and no longer relates to the sponsor or CDR representative principal?

6.4 Are there other matters that would need to be addressed in the rules if the proposed amendments were made?

Issues for Feedback – Energy

7. Authorisations granted by nominated representatives in the energy sector

In the energy sector the implementation dates for consumer data sharing are phased by the size of the retailer (being the three initial retailers first, then all other 'larger retailers' with more than 10,000 small customers) and the type of consumer data request (being non-complex or complex requests).

The CDR Rules define complex requests to mean a consumer data request that:

- is made on behalf of a large consumer; or
- is made on behalf of a secondary user; or
- relates to a joint account or a partnership account.

Consumer data requests made by CDR consumers who use a nominated representative are not included in the complex request definition. As a consequence, larger retailers will have to provide nominated representative functionality when they first begin sharing consumer data on the 1 November 2023 tranche 3 compliance date.

Proposed approach

In response to stakeholder feedback Treasury proposes broadening the definition of complex request to include consumer data requests made by CDR consumers who use a nominated representative to provide authorisations. This would mean larger energy retailer data sharing obligations to support nominated representatives for all CDR consumers would shift from 1 November 2023 to 1 May 2024, giving them additional time to build for such requests.

Consultation questions

7.1 Do you support a deferral of larger energy retailers' obligations to support nominated representatives?

8. Trial products for the energy sector

The *Competition and Consumer (Consumer Data Right) Amendment Rules (No 1) 2023* removes data sharing obligations for certain 'trial products' in the banking sector, based on the product's period of offering and number of customers. For banking, a 'trial product' is a 'pilot' or 'trial' product that is offered for a period of no more than six-months and is offered to no more than 1,000 customers. A product ceases to be a trial product if it continues to be offered after the end of the six-month trial period or is supplied to more than 1,000 customers.

The intention is for the trial product rules to address possible disincentives under the CDR for data holders to introduce innovative new products, particularly for smaller data holders, which do not have the scale to pilot products internally. The rules enable data holders to test the viability and scalability of their offerings without being subject to CDR data sharing obligations.

Currently, the trial product rules only apply to the banking sector. Stakeholder feedback on the trial product rules supported extending this exemption to trial products to the energy sector, but with an energy-specific definition of a trial product to reflect energy products' unique features.

Proposed approach

Treasury proposes introducing rules for energy trial products that reflect the specific needs of the energy sector. We note that energy products differ from banking products and therefore seek stakeholder feedback on how trial products could be defined and whether they should be subject to certain thresholds (such as the period of time the product is offered for and a limit on the number of customers it is offered to).

Consultation questions

8.1 Do you support extending the trial product exemption to the energy sector?

8.2 If the trial product exemption is extended to the energy sector, what is an appropriate sector-specific threshold for defining such trial products? Should a threshold be quantitative (e.g. a numerical threshold) or qualitative (e.g. focused on the purpose of a product)?

9. Insight disclosures for the energy sector

Amendments to the CDR Rules in 2021 introduced the concept of a 'CDR insight', which allows CDR consumers to consent to their data being disclosed to specified unaccredited persons for a range of prescribed purposes that are considered low risk. Currently, the specified purposes for which an insight disclosure consent could be given are to verify the consumer's identity, account balance, or details of credits to or debits from the consumer's accounts.

Treasury has received stakeholder feedback that insight disclosures should be expanded to include additional energy-specific insights. For example, an insight disclosure consent could be given to verify or demonstrate a consumer's energy usage. Stakeholders have suggested that energy data may be less sensitive than banking data and that energy-specific insights could provide more detail than insights using banking data.

Proposed approach

Treasury is considering whether to expand insight disclosures to include energy-specific insights and is seeking stakeholder feedback on whether insights could be developed to be sector-agnostic, sector-specific or a combination of both. For example, insights to verify a consumer's identity could remain sector-agnostic while an insight about or related to off-peak energy usage could be added to the energy Schedule.

Consultation questions

9.1 How should energy-specific use insights be defined? What use cases could be enabled through energy-specific insights?

9.2 Should a sector-agnostic model for insight disclosures be established? If so, what kinds of sector-agnostic insights should be considered?

9.3 What are the potential privacy impacts associated with additional energy-specific insights?

10. Historical metering data liability

Under the CDR Rules, energy retailers are required to disclose Australian Energy Market Operator (AEMO) metering data for a period that pre-dates the current retailer's relationship with the consumer (referred to as 'historical metering data').[21] For example, this would occur where a consumer has switched energy retailer but has not moved house. Including historical metering data as part of the CDR allows consumers access to their energy usage data over a longer duration.

From 1 November 2023, the Market Settlements and Transfer Solution (MSATS) procedures made under the National Electricity Rules (NER) will require retailers to notify AEMO when the account holder changes. AEMO will then set a 'customer change' flag to determine the metering data that relates to the CDR consumer and which an energy retailer can then on-disclose to an ADR. The DSB is now consulting on technical and CX standards that will use the new MSATS procedures to enable sharing of historical metering data.[22]

Under the MSATS procedures, a retailer may unintentionally disclose incorrect metering data if the customer change flag has not been set correctly. This could result in the retailer inadvertently disclosing energy consumption data unrelated to the CDR consumer. This could occur if, for example, a retailer incorrectly records a customer as an 'in-situ' customer when they open the consumer's account.

Proposed approach

Treasury proposes to amend the CDR Rules so that a data holder acting in good faith would not be liable under the CDR framework where they on-share incorrect metering data provided to them by AEMO. The retailer would not be acting in good faith if it has reason to believe the disclosure would include metering data unrelated to the CDR consumer making the request.

Consultation questions

10.1 Do you support a proposed rule amendment to provide that a retailer or ADR acting in good faith would not be liable where they make an inadvertent disclosure of metering data within the CDR framework?

[21] CDR Rules 2020, Sch 4, cl 3.2.
[22] DSB, Decision Proposal 314 –Last Consumer Change Date (Phase 1).

Issues for future consideration

Treasury is considering other proposals for operational enhancements to the CDR Rules, which may be consulted on in future design papers. Treasury welcomes any preliminary comments from stakeholders in relation to the following issues:

- whether the rules around consumer eligibility in relation to a data holder are fit-for-purpose where data holders operate multiple brands.[23]
- when an authorised deposit-taking institution (ADI) or energy retailer who has collected CDR data as an ADR should be able to hold that data as a data holder (rather than as an ADR).
- how the rules about corrections under privacy safeguards 11 and 13 should be clarified, and whether associated changes to the data standards could support these corrections to be made effectively and efficiently.
- whether consumer dashboard retention obligations for data holders and ADRs should be clarified in the CDR Rules.
- whether changes to the CDR Rules are needed to better facilitate management of consents and authorisations where there are multiple nominated representatives involved, or where a business consumer's nominated representatives change over time.

[23] Feedback was provided in relation to ACCC regulatory guidance on Consumer eligibility across data holder brands in the banking sector. Data holders have indicated there may be technical complexities associated with identifying consumers across different brands, as well as with sharing data from closed accounts in circumstances where a consumer has open eligible accounts with one brand, and only closed accounts with a different brand of the same data holder.