Adatree Response to ACCC Intermediary Discussion Paper

February 3, 2020

Executive Summary:

Adatree is an Australian RegTech founded to remove barriers for organisations participating in the Consumer Data Right (CDR) ecosystem. We believe the CDR will result in competitive consumer outcomes and promotes ethical behaviours for sharing data. Our modular platform is designed exclusively for Data Holders and Accredited Data Recipients ("ADRs"). Adatree provides all necessary technical components, hosting, and security; consequently we create an abstraction layer from the CDR standards for our clients. Our aim is to future-proof our clients' requirements by managing compliance for them.

Adatree considers itself occupying the role of an intermediary that would receive and store the CDR data on behalf of a Data Recipient, ensuring all technical compliance with all current and future standards. Our offering is flexible so that our business model is aligned to the differing needs of ADRs. We are neither a Data Holder nor an ADR as we will not be required to share data and do not intend to receive it on our behalf; we exist to enable others in the CDR ecosystem.

Adatree believes that:

- Introducing an intermediary model will ensure the success of the CDR by securely enabling more participants and thereby giving the industry confidence in the regime;
- introducing an intermediary model would encourage organisations to adopt and maximise their use of the CDR whilst minimising their costs and the barriers to entry to being an ADR;
- an intermediary model will minimise regulatory burdens as per the Regulator Performance Framework;
- intermediaries should be able to provide Managed Services for all of the technical, hosting and security aspects for ADRs because this will be an attractive offering for industry to receive CDR data, lowering the barriers to entry for participation in the CDR ecosystem. ADRs are focused on their products and services, which is their core business. The core business of an intermediary is the safety, security, and technicalities of CDR compliance;
- the ACCC should accredit different intermediary types based on the nature of the services provided, being read and write capabilities;
- any organisation receiving CDR data that is not de-identified should be subject to the same standards and rules, and there should be no exceptions for non-accredited organisations;
- the ACCC should create tiers for Data Recipients based on the storage and access to CDR data. This tiering should still ensure the upholding of the high bar of the standards but can share responsibilities between the Data Recipient and an intermediary partner; and
- screen scraping should be banned, in line with the purpose and ethics of the CDR.

Responses to Questions about Intermediaries

1. **If you intend to be an intermediary in the CDR regime, or intend to use an intermediary, please provide a description of the goods or services you intend to provide to accredited persons or to CDR consumers using an intermediary. Do you intend (or intend to use an intermediary) to only collect CDR data, or collect and use CDR data? What value or economic efficiencies do you consider that intermediaries can bring to the CDR regime and for consumers?**

By the definitions and use cases presented in the Consultation Paper, Adatree would seek to be an intermediary in the CDR regime.

Adatree is a technology company focused on the management of regulatory processes (RegTech) that was founded as a direct result of the Australian Consumer Data Right (CDR) legislation. Adatree's vision is a world where data is democratised and competition is the driver of better consumer outcomes. We will deliver on this by removing barriers to entry for the data sharing ecosystem through our modular SaaS offering.

Adatree is the only provider of an Open Banking platform for both Data Holders and Data Recipients. Our modular platform provides all technical components to become part of the CDR ecosystem. Technical readiness is only one part of overall CDR readiness, so we also help organisations with business and customer readiness through consulting services, program management and all aspects of preparation. Our CDR platform is future-proofed to the CDR standards and rules, and our components are available on a modular basis so that an organisation can leverage existing infrastructure or capabilities that meet the CDR standard.

Adatree believes that leveraging a highly scrutinised, high quality utility model is more efficient than each ADR building it themselves having to address each security and audit consideration individually. This decreases the risk of any incorrect build or tests, longer time to market and the opportunity cost of focusing on customer offerings. CDR compliance and conformance should be the expertise of Adatree so the Data Holders and ADRs can dedicate their time, effort and resources on meaningful consumer outcomes

Adatree has taken the steps to build a CDR Data Recipient platform which encapsulates these requirements on behalf of the ADR, allowing them to retrieve the data in a 'pass-through' model where Adatree does not store the CDR consumer data but enables the ADR to meet all of the requirements. This includes data exchanges, integrations between the CDR registry and each individual Data Holders, the established consent framework, user experience conformance, and information security requirements for storing and utilising data. This is also completed according to the CDR standards, which incorporates parts of the OIDC and FAPI technical standards, as well as some CDR specific elements

The below table outlines the technical components that Adatree offers to DHs and ADRs.

ADATREE PROVIDES ALL TECHNICAL COMPONENTS DATA HOLDERS AND DATA RECIPIENTS NEED

Technical Requirements	Data Holders	Data Recipients
API Gateway	✓	✓
FAPI-conformant Identity Provider (IDP), built to the CDR standards	✓	✓
Consent Dashboard Web Application to manage, view and revoke consent	✓	✓
Consent Management API This ensures consent data is immutable, auditable, and verifiable, which is critical for consent reporting. This is specifically built to the CDR standard and purposes, and works with either the Adatree consent dashboard or one built by the DH or ADR.	✓	✓
Customer CDR Notifications through various channels	✓	✓
CDR APIs: InfoSec, Admin, Banking	✓	✓
Product Information API	✓	n/a
Human Readable Consumer Data Request	✓	n/a
Dynamic Client Registration	n/a	✓
CDR Metadata Cache	✓	✓
Test environments and plans	✓	✓

ADATREE

The below table outlines how Adatree helps ADRs leverage CDR data and ensures business readiness.

ADATREE PROVIDES COMPONENTS TO HELP ORGANISATIONS COMPETE AND COMPLY

Audience	Modules and Components
Data Recipients	Account Switching, including switching of payments, direct debits and payee lists
	Customer onboarding
	Identification of customers, which decreases time, cost and effort and improves customer experiences
	Initiation of payments, account servicing requests, account opening
	Integrations to key customer value-add partners
	Centralised consent dashboard. This is driven by our business model as we provide services for both DHs and ADRs and can be an intersection between the consent models.
Data Recipients and Data Holders	Consulting for business and customer readiness aligned to the Rules
	Consulting for technical data mapping, CDR boundaries and application of Standards

ADATREE

Benefits of using a CDR intermediary

Ultimately benefits of using an intermediary will extend to the end consumer as our platform will increase participation in the CDR regime, and businesses can focus on competitive, innovative, and customer-focused uses of CDR data.

Adatree's CDR platform benefits customers (banks, fintechs, tech companies, energy companies, etc.) and drives productive outcomes by:

- delivering on their CDR obligations and removing regulatory burdens efficiently;
- being a cost-effective alternative to building and maintaining CDR technical components;
- adapting to all ongoing regulatory changes, which future-proofs their CDR compliance. As an intermediary, we realise that change is the only constant, and adapting to these changes will be the top priority of our business. This helps alleviate backwards compatibility issues for the ACCC, Data61, the DSB, ADRs and DHs by allowing the standard to move forward;
- helping them leverage CDR data; and
- accelerating their journey to being part of the ecosystem, and therefore time to market with compelling consumer offerings.

Providing an intermediary offering will allow entry to the CDR ecosystem for many organisations. This includes startups and organisations with innovative uses for the CDR data. Organisations like these want to focus on using CDR data, create competitive and delightful customer offerings, and decrease consumer inertia. Adatree focuses on compliance and obligations so organisations can focus on their customers and experiences. The intermediary model will incubate the new participants to the CDR ecosystem by providing an efficient means to balance between compliance and competitive offerings.

Similar to how the introduction of the RADI licensing regime has made the barriers to entry in banking more manageable, the intermediary model will lower barriers to participation in the CDR. In banking, this has resulted in more competitive and compelling consumer offers, which should be mirrored in the CDR.

2. How should intermediaries be provided for in the rules? In your response please provide your views on whether the rules should adopt either an outsourcing model or an accreditation model, or both and, if so, and in what circumstances each model should apply.

Defined Terms:

Intermediaries should be defined as organisations that help facilitate the flow of CDR data. The definition should not limit what capabilities or services they provide, as there will be many different business models of intermediaries.

Storage of CDR Data should be defined as the environment where the CDR data is hosted, regardless of whether on-premise or in cloud.

Read Access to CDR Data should be defined as the ability to consume CDR data but not publish any updates to other organisations.

Write Access should be defined as the ability to publish changes on behalf of the consumer. This applies to multiple uses of updates, including but not limited to initiating payments, applying for products, updating CDR data or any other updates to other organisations. Write Access will be addressed in the upcoming Farrell review.

Accredited Data Recipient should be defined as an organisation meeting all Standards, Rules, and required certifications for accreditation by the ACCC to receive CDR data. They meet all customer, business and technical readiness obligations, and the CDR data is stored in their own environments with appropriate security protocols.

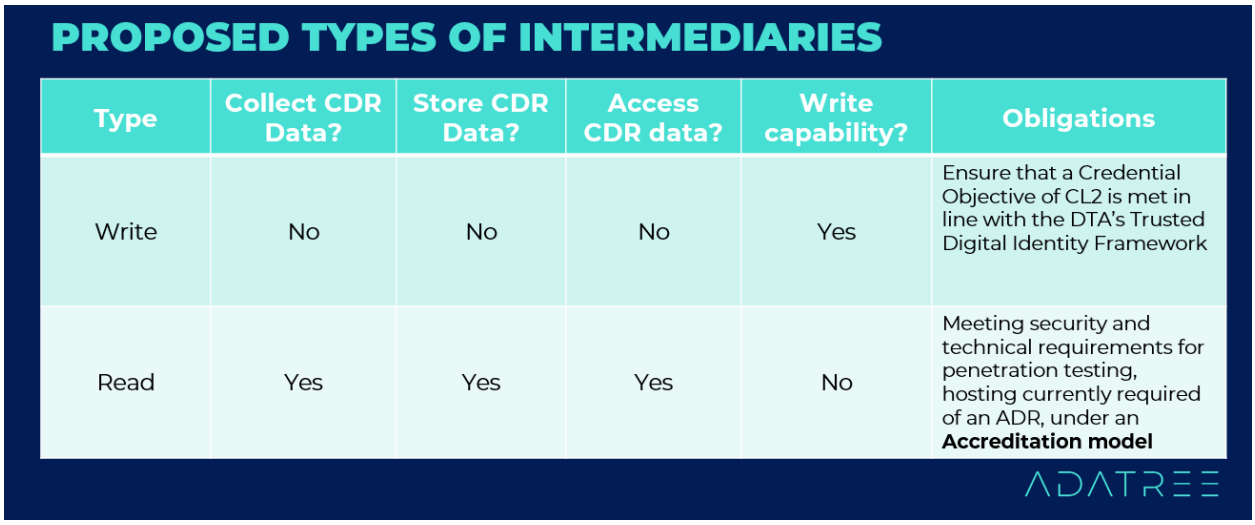
Partnered Accredited Data Recipient should be defined as an organisation using an intermediary partner to meet all of the Standards, Rules, and required certifications for accreditation by the ACCC. All customer, business and technical readiness obligations are met, but they are met with divided responsibility between themselves and an accredited intermediary. The CDR data is stored in the environment of an intermediary with required security protocols.

Intermediary models in the Rules

There should be tiering of accreditation and obligations depending on the nature of the services and data accessed. Adatree believes that all intermediaries of any type should be accredited.

Although this increases barriers to entry for intermediaries, they have greater responsibilities in the ecosystem. This also increases the certainty for the industry working with intermediaries as partners. This should ultimately expedite the procurement process of working with an intermediary and accelerate participation in the CDR. Outsourcing model agreements should not be used because it would put more work and effort onto each ADR or PADR client, resulting in a less efficient process.

Table 1: Proposed Types of Intermediaries



PROPOSED TYPES OF INTERMEDIARIES

Type	Collect CDR Data?	Store CDR Data?	Access CDR data?	Write capability?	Obligations
Write	No	No	No	Yes	Ensure that a Credential Objective of CL2 is met in line with the DTA's Trusted Digital Identity Framework
Read	Yes	Yes	Yes	No	Meeting security and technical requirements for penetration testing, hosting currently required of an ADR, under an **Accreditation model**

ADATREE

Intermediaries cannot use CDR data for their own commercial purposes. If an organisation wants to use or leverage CDR data for their own commercial purposes then they must be considered an ADR. An intermediary should not be permitted to utilise or onsell insights, trends, etc. in relation to CDR data. The exception of this is if they have express consumer consent to do so as an ADR. This upholds the ethical principles outlined in the first Farrell report.

Intermediaries should be considered to be a Managed Service, where the technical requirements outlined in Schedule 2 of the Rules are managed by the intermediary. This will uphold and maintain the standards and rules required for an organisation accessing CDR data, but will delegate responsibility to this type of intermediary instead of the ADR.

It is imperative that an intermediary model does not lead to any organisations receiving CDR data that is not de-identified without meeting the full ADR obligations, either themselves or through an intermediary.

Screen scraping has allowed organisations to collect, store and use consumer data without a consumer knowing where their data is, where it is located, if it is being sold, the frequency of access and whether the organisation is leveraging the data beyond the uses presented to the consumer. The CDR brings a higher standard for organisations that access and store consumer data. Despite this being a higher barrier of entry for organisations to receive CDR data, Adatree argues that the barriers for organisations receiving consumer data through screen scraping have been way too low at the disadvantage of the consumer. This can no longer continue, and screen scraping should be banned in Australia, as it has been in the UK.

3. What obligations should apply to intermediaries? For example, you may wish to provide comment on:

a. if intermediaries are regulated under an accreditation model, the criteria for accreditation and whether they should be the same or different to the criteria that apply to the current 'unrestricted' level, and the extent to which intermediaries should be responsible for complying with the existing rules or data standards;

b. if intermediaries are regulated under an outsourcing model, the extent to which contractual obligations should be regulated between accredited persons and intermediaries;

c. if the obligations should differ depending on the nature of the service being provided by the intermediary.

Obligations should absolutely differ depending on the nature of the service provided by intermediary, largely about the storage, access, and usage of the CDR data. These obligations are noted above in *Table 1: Proposed Types of Intermediaries*. Detail in *Table 2: Proposed Tiering for Recipients*, found in the response to Question 6, is also relevant to this question.

If an organisation is going to store CDR data, they must meet the ADR obligations themselves. A PADR cannot store CDR data and must use an accredited partner to meet the standards. This is to ensure information security principles are adhered to, and the CDR data meets the principles outlined for the consumers, including deletion, de-identification, and other measures outlined in the Rules.

For intermediaries that facilitate 'View' access to PADRs, the CDR data must be:

- Neither stored by the intermediary nor the PADR;
- not pooled with any other consumer data collected by a different PADR; and
- inaccessible by the intermediary.

For intermediaries that store CDR data on behalf of PADRs, the storage of CDR must be:

- stored by the intermediary on behalf of a specific PADR;
- not pooled with any other consumer data collected by a different PADR; and
- inaccessible by the intermediary.

For example, Fintech A is a PADR with a budgeting app and Fintech B is a PADR with a loan comparison platform. Both are utilising Adatree as an accredited intermediary, Camilla utilises both Fintech A and Fintech B, and she consents to sharing her CDR data with them, each having different purposes, sharing duration and types of data. Adatree must keep Fintech A and Fintech B's data shared by Camilla separate. Adatree cannot pool all of Camilla's CDR and share freely with the PADRs but can only share the CDR data with Fintech A & B in line with the consent specifications.

Intermediaries that store CDR data should be subject to the data at rest security obligations as a Data Holder as well as including, but not limited to, audit security, CDR data storage and boundaries, deletion, de-identification and other data security and consumer protection measures, as outlined in the Rules and Data Standards. System availability obligations should also be in line with Data Holder CDR conformance.

4. How should the use of intermediaries be made transparent to consumers? For example, you may wish to comment on requirements relating to consumer notification and consent.

Consumers should only be made aware of the end organisation with access to the identifiable CDR data, where the consent was originally granted. The intermediary (regardless of type) is not granted the CDR data. For example, if Fintech A accesses CDR data through Adatree, an intermediary, Fintech A will host the consent dashboard. Consent is not granted to Adatree, only to Fintech A. Adatree only facilitates and enables the sharing of CDR data.

In our Open Banking research, we spoke with a Data Recipient in the UK that used an intermediary for the technical components. During customer testing for designs and user flows, the intermediary branding and name was presented to the customer, which resulted in ~90% of customers not going through with the consent granting, questioning who the party was and their purpose in the process. They ended up not presenting the name of the intermediary but presented only the Data Recipient name to the customer.

In the Rules, it notes that the ADR has to have an accreditation number (section 4.11 (3) (b)). It has been discussed in the Data61 Customer Experience Working Groups that an ADR could have a badge or logo signifying accreditation. This concept could apply to a different logo for ADRs and PADRs, giving security and certainty to consumers that the organisation is officially accredited as part of the CDR ecosystem.

Consumers assume that other vendors are involved in any service, from CRMs to cloud storage providers. When data is stored or accessed by those companies, it is not disclosed to the consumer. That should be extended to any intermediaries. Intermediaries should be considered an unknown implementation detail. Making the consumer aware of this will only increase the cognitive load of the consumer, as per the example above.

One gain to be made for consumer transparency would be the creation of a consent dashboard through a consent API. This would be the focal point of convenient consumer control. In the same way that you control notifications for all phone apps in a mobile phone's Settings, this is intuitive to consumers and promotes control and visibility of their consent and data sharing.

5. How should the rules permit the disclosure of CDR data between accredited persons? For example, you may wish to comment on requirements relating to

consumer consent, notification and deletion of redundant data, as well as any rules or data standards that should be met.

The same standards outlined in the Rules should be adhered to by both ADRs and PADRs. When a consumer shares their data, they still have to view the same statements and provide express consent to certain fields, regardless of whether an ADR uses an intermediary or not. They should also have the same rights for notifications and the right to delete. The PADR would be eligible to receive the de-identified information if the consumer consents to this, similar to the ADRs.

If the consumer revokes consent, this means that the PADR can no longer access the consumer data and that the intermediary has to delete or de-identify the CDR data, in line with the consumer request.

The standards should not be decreased for the consumer with the introduction of the intermediary model.

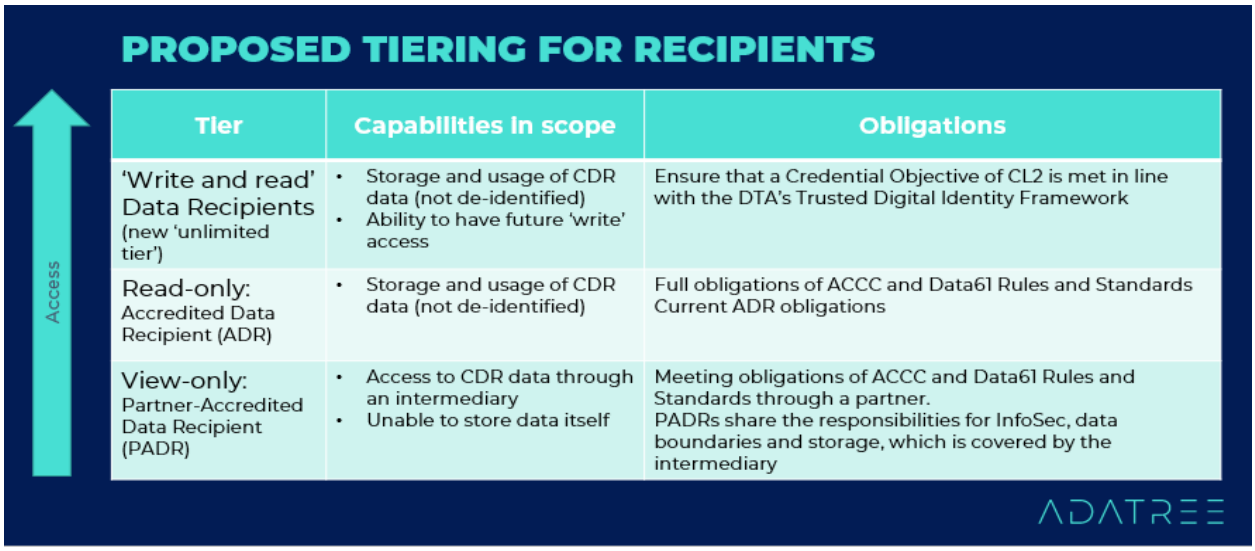
6. Should the creation of rules for intermediaries also facilitate lower tiers of accreditation? If so, how should the criteria and obligations of new tiers of accreditation differ from the current 'unrestricted' accreditation level, and what is the appropriate liability framework where an accredited intermediary is used?

As referenced above, there should be two different types of intermediaries: read and write.

There should also be different tiers of recipients, based on their use cases and capabilities. This is noted below in *Table 2: Proposed Tiering for Recipients*.

Separate tiering for intermediaries and recipients has been proposed because these two concepts can be exclusive but don't need to be. A PADR must use an intermediary, but an organisation with other tiers of recipient access can choose to build and maintain these capabilities themselves without an intermediary.

Table 2: Proposed Tiering for Recipients



Questions about permitting CDR data to be disclosed to non-accredited third parties

7. If the ACCC amends the rules to allow disclosure from accredited persons to non-accredited third parties and you intend to:

a. receive CDR data as a non-accredited third party, please explain the goods or services you intend to provide, the purposes for which you propose to receive CDR data, and how this may benefit consumers;

b. be an accredited person who discloses CDR data to non-accredited third parties, please explain the intended goods or services you intend to provide and how they may benefit consumers.

Adatree intends to be an accredited person (Intermediary of 'Read' type and 'Write' type when available, as per above). This would allow Adatree to receive and store the CDR data on behalf of a PADR, ensuring all technical compliance with all current and future standards. There should be **no** disclosure to non-accredited third parties. The introduction of the PADR tier will continue to uphold existing standards while decreasing barriers to entry.

Our goods and services for Partnered-Accredited Data Recipients (PADR) includes:

- providing all of the technical components noted above on behalf of a PADR;
- ensuring all of the requirements are met in Schedule 2 of the ACCC CDR Rules: these would be met by Adatree on behalf of the PADR;

- storage and access of the CDR data on behalf of the PADR aligned to the CDR data boundary rules;
- processes to delete the CDR data as required. This is included in our Consent API module with metadata stored after any personally identifiable information (PII) data has been deleted.
- ensuring that consent is immutable, auditable and verifiable as an audit trail for deletion and de-identification compliance;
- processes to de-identify the CDR data as required;
- sending of notifications on behalf of the PADR; and
- consulting for business readiness, including complaints handling, reporting, policies and internal processes.

8. What types of non-accredited third parties should be permitted to receive CDR data? Why is it appropriate for those types of third parties to be able to receive CDR data without being accredited?

It is not appropriate to share CDR data with non-accredited third parties. Some suggestions have been raised publicly about some professions, including lawyers and accountants, receiving the CDR data without being an ADR. If there is an exception made to decrease standards for organisations, this will encourage lobbying of other professions to decrease their barriers of entry too. An appropriate intermediary model should bring all organisations, regardless of size, systems or industry, into the CDR ecosystem effectively.

9. What privacy and consumer protections should apply where CDR data will be disclosed by an accredited person to a non-accredited third party?

The same privacy and consumer protections apply to ADRs and PADRs, being the ability to grant, manage, view and revoke, ability to delete or de-identify, send CDR notifications, etc.

10. What degree of transparency for CDR consumers should be required where an accredited person discloses CDR data to a non-accredited third party? For example, are there particular consent and notification obligations that should apply?

See response to question 4.