# ACCC CDR Amendment No. 3 consultation summary

quill peak

David Giddy.

V1.1 – 6 Oct 20

# Key changes

Amendment No. 3 proposes more than 20 individual changes to the CDR Rules. This document provides a high level summary of the key changes that will be of interest to many CDR participants. This reader is assumed to be already familiar with the CDR as it exists today.

1. Introduction of new classes of restricted Accredited Data Recipients
2. Permitting transfer of CDR data between accredited persons
3. Allowing ADRs to disclose CDR data to non-accredited persons with a customer's consent
4. Allowing ADRs to provide insights to anyone with a customer's consent
5. Extending data sharing to companies and business partnerships
6. Extending data sharing authorization to others authorized to operate on an account
7. Changes to the Joint Account Management Service
8. Allowing consents to be amended
9. Separating consent for collection from consent for use
10. Changes to the way data is made redundant
11. Improvements to Data Holder dashboards
12. Allowing consumers to consent to their data being used for research
13. Formalising guidance around Product Reference Data for white-label products

Note: This document simplifies many of the proposals. Participants should refer to the consultation document here for details before submitting a response to the ACCC.

# 1 Introduction of new classes of restricted Accredited Data Recipients

The ACCC is proposing 3 new classes of restricted ADRs that would effectively extend the recently approved CAP model

## Limited Data model

The concept here is to limit the shared data to less sensitive data

- For banking, this could be:
  - Bank account data
    - Balance, identifiers, product information
    - Does not include: transaction data
  - Basic customer data
    - Name, occupation, business numbers, industry code
    - Does not include DOB
  - Payees - all stored payee data
  - Regular payments - All regular payment information

## Data Enclave model

The concept is to create a secure environment within another unrestricted ADR that could host activities for restricted ADRs

- Principal could host their applications in the environment
- Provider could collect data and provide analytics for the principal
- Principal could not download local copies of the data or otherwise access the data outside the environment

## Affiliate model

The concept is to partner with an unrestricted ADR who could sponsor the restricted ADR in respect of their compliance with particularly the data security obligations, thus avoiding audit costs

- Sponsor would need to attest to the ACCC that the affiliate meets the accreditation criteria
- ACCC would conduct a targeted audit programme towards this class of ADRs

In all three models, the restricted ADRs would still need to comply with most of the obligations. It is fundamentally the data security compliance certification that is proposed to be relaxed (often the most expensive part of becoming an ADR) – self assessment and attestation would replace formal ASAE3150 audits

# 2 Permitting transfer of CDR data between accredited persons

This effectively extends the ADR to ADR sharing between a Principal and a Provider under the CAP arrangements to allow more flexible data sharing amongst ADRs

- Proposal is to permit ADRs to share data (with a customer's consent) with another ADR for the purpose of providing a service to the consumer
- The rule would allow both unrestricted and restricted ADRs to share data, but a restricted ADR could only receive data from another ADR that it could have received itself
- An example given was of an ADR providing a comparison service for a consumer then recommending another ADRs service and passing on the customers data in order for the customer to acquire that service

3

# Allowing ADRs to disclose CDR data to non-accredited persons with a customer's consent

This is fundamentally about enabling customers to share data with trusted advisors

- Proposal is to permit ADRs to disclose CDR data to non-accredited persons with a customer's consent, where those persons are from a specified class
- The specified classes are expected to include:
  - accountants
  - lawyers
  - tax agents
  - BAS agents
  - financial advisors
  - financial counsellors
  - Mortgage brokers
- Generally the thinking is that the classes would need to be subject to some form of professional regulation that has similar privacy obligations or "best interests" duty
- It is up for discussion whether those classes should include all holders of an AFSL or an ACL
- It's also up for discussion whether customer's would need to be also receiving a service from the ADR, or whether they can be simply a conduit for the data

# 4 Allowing ADRs to provide insights to anyone with a customer's consent

This could avoid the need for some use cases to actually become ADRs

- "Insights" are essentially derived data from the raw CDR data
- Examples given are
  - Income and expense verification
  - Verification of payments
  - Outcomes of responsible lending assessments
- Part of the definition of an "insight" that is proposed is that the insight, when decoupled from a customer identifier would not allow identification of the customer

# 5 Extending data sharing to companies and business partnerships

This has always been the intent and is now proposed to be enacted

- To date, whilst business has not been excluded from data sharing, in practice it's only been sole traders and partnerships operating with a simple joint bank account who have been able to actually share data
- The proposal is to extend data sharing to bodies corporate (and likely trusts) and also partnerships generally
- To enable this they propose a concept of one or more "nominated representatives" who would be permitted to authorize data sharing on behalf of the entity
- There would be a single dashboard for the entity that would be visible to all the nominated representatives
- Partnerships would be treated similarly to bodies corporate and also need to specify nominated representatives
- This is a high priority for the ACCC, so is likely to be implemented, however no target date has been set as yet

6

# Extending data sharing authorization to others authorized to operate on an account

This is really a consistency clean up action

- To date, only account owners have been able to authorise data sharing
- This proposal extends data sharing authorization privileges to others with account authorisation
- The account owner would need to approve this through a “secondary user instruction”
- The account owner would maintain control over the account and any secondary user instructions
- An example given is second card holders on credit card accounts

# 7 Changes to the Joint Account Management Service

This is mainly about improving the customer experience for joint accounts

- To date, account owners have had to set up a preferences around how joint account authorisations work outside the context of a data sharing establishment and potentially through an offline process
- These amendments would require Data Holders to implement an online preference selection mechanism and also enable preferences to be set during the process of establishing the first data sharing arrangement
- Another amendment is to further support vulnerable customers through enabling them to operate data sharing on a joint account as if they were the sole account owner
- Recognising that there are a few cases with more than two joint account holders, the rules now cater to joint accounts with three or more account holders
- The final amendment in this area is to enable either joint account holder to withdraw consent for data sharing independent of the preference on “one to authorise” or “two to authorise”

# 8 Allowing consents to be amended

This will improve the customer experience around making changes to existing consents

- In the current rules, if a consumer wants to change the parameters of a consent, they need to revoke the consent and share the data again with a new consent
- In this proposal, the rules will authorise the amendment of consents by consumers
- This is intended to be quite flexible as there are many potential consent amendments that are possible
- The technical implementation, however, will not change with consent amendments being translated into consent revocation and new consent creation calls on the data holder APIs

# 9 Separating *consent for collection* from *consent for use*

This changes the semantics of how consents work in a significant way

- To date, a consent is for both an ADR to *collect* data and *make use* of it in the authorised manner
- This proposal is to separate *consent to collect* from *consent to use* data
- The benefit here is to simplify data management for ADRs and allow more granular control over consents by customers
- Example given:

> 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.

- This consent model also supports the changes to the data redundancy model (see next slide)

# Changes to the way data is made redundant

This changes the way data becomes redundant and thus simplifies data management for the ADR

- To date, data automatically becomes redundant when a consent is revoked or expires
- With the proposed separated consent model, data will become redundant only when the *consent to use* is revoked or expires
- This will simplify data management for ADRs considerably as they will no longer need to track the source of each element of data when there are multiple data holders involved (e.g an account aggregation app)
- The rules would require the ADR to notify the customer if a *consent to collect* is withdrawn that they also need to revoke their *consent to use* if they wish the ADR to cease using the data as well

# 11 Improvements to Data Holder dashboards

This is an improvement in the ability of the consumer to understand who a consent is for

- Today, if a business entity has a trading or product name that is different from their accredited entity name, then it can be confusing for the customer to recognise who a consent is for on a Data Holder dashboard
- This proposal will require Data Holders to display additional information (either from the CDR Register, or from additional meta-data provided by the ADR) in the customer dashboard to make it clear who a consent is for
- This is essentially trying to avoid the problem that exists today with card merchants having different trading names from their business names and customers being unable to identify who a transaction is from

# 12 Allowing consumers to consent to their data being used for research

This allows ADRs to request consent to use CDR data for research purposes

- Today, CDR data is only permitted to be used in provision of goods and services to a customer
- This proposal will allow consumers to consent to their data being used for research purposes as disclosed by the ADR
- Generally it is expected that the ADR would need to offer the consumer a benefit to gain their consent

13

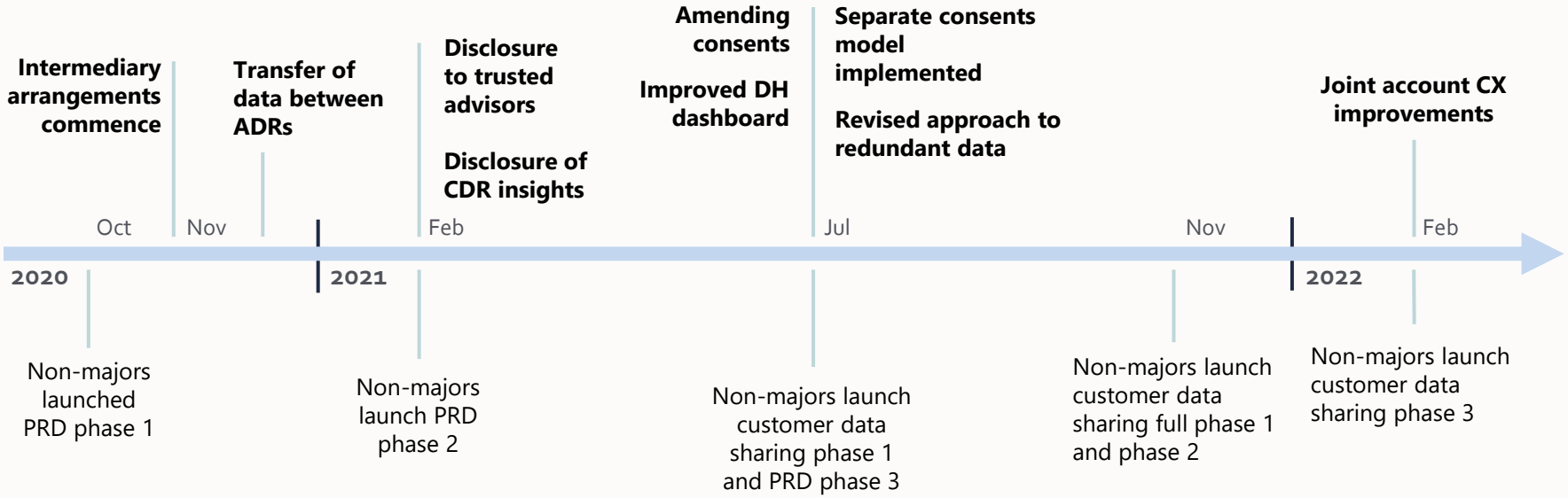
# Formalising guidance around Product Reference Data for white-label products

This is the formalisation of the previously issued guidance paper issued by the ACCC for white-label products in the context of PRD sharing

- The ACCC previously provided guidance on who was responsible for sharing PRD data in the context of a white-labelled product created by one Data Holder and marketed and branded by another
- The main clarification is that where there are two Data Holders involved, then the Data Holder with the contractual relationship with the customer is responsible for responding to product data requests
- The proposal does not address the case of consumer data requests in the white-label scenario – the position on this is still under development

# Timeline

The ACCC has issued a draft compliance timeline for most of the proposed amendments. Here are the proposed dates for the items discussed in this summary.




There are no proposed dates as yet for the following items:

- Limited data/Data enclave/Affiliate accreditation
- Data sharing by business entities and partnerships

**PRD** – Product Reference Data

# OUR COMPANY

Quill Peak Consulting is a boutique consulting firm specialising in Open Banking and the Consumer Data Right.

Principal: David Giddy
E: david@quillpeak.com.au
P: 0417 541 304