CDR Rules Framework Submission

Section 2 The ACCC proposes that in the first version of the rules, data sharing will not be subject to fees.

Please give clarity and certainty around this statement, such as –

- Stating that there are no restrictions on Data Recipients charging consumers for data sharing content or for enhanced services that rely on data sharing content.
- Stating that there are no setup fees that might be charged by a Data Holder to a Data Recipient for API integration testing or administrative once-off fees that the Data Holder might impose (or if it is intended, then this should be scoped).
- Re-stating that the Data Holder cannot charge a fee for the supply of data sharing content.
- Stating that there are no fees chargeable by a Data Holder to a Data Recipient when any consumer authorisation changes or concludes.
- Give guidance on how fees might change in subsequent versions of this rule set!

Section 5.3 Data Sets and 9.6. Granularity of authorisation

This section defines a number of data sets that will be made available -

- Consumer Data
- Transaction Data
- Product Data
- Meta Data

Our business is only interested in the transaction data. Our preference would be that selection of the specific data sets form part of the consent and authorisation process so that only the specific data sets are disclosed. As a security and privacy principle, we only want to receive the minimum amount of consumer data that is required to provide our service.

Section 12.1.3. To an intermediary through whom the data passes on its way to the data recipient

".. allow smaller accredited data recipients to qualify for a lower level of accreditation by relying on the stronger security and privacy protections provided by an intermediary accredited to a higher level.."

We believe that the statement above is inappropriately worded. All Data Recipients need to be able to demonstrate that the security and privacy protections of a particular data set are being met. However, we do agree that if a superior Data Recipient acting as an intermediary is part of the solution, then some of the requirements may be able to be attributed to the superior data recipient. This is consistent with the later statement -

".. This model may also allow for CDR data to be processed within the environment of the intermediary, and for the accredited data recipient to obtain insights from the data without ever 'seeing' or storing the data ."

Section 6 Accreditation – The applicant will need to provide:

We do not agree that the requirements for a 'business plan' and 'business continuity arrangements' are relevant to the accreditation of a Data Recipient where the data sets are only in the downwards direction from the Data Holder towards the Data Recipient. Should, later versions of the rules, permit operation on data sets in the upward direction from the Data Recipient to the Data Holder, or if the Data Recipient wants to be an intermediary, then such requirements may be appropriate. However, we suggest this additional requirement would only be for a specific category of Data Recipient.

We are not in favour of the word 'tier'. This has a suggestion of CDR flow from Data Holder to Data Recipient that implies intermediaries. We would prefer the use of 'categories' or 'classes' of Data Recipients. It may be that one 'category/class' of Data Recipient is in a 'tiered' arrangement or it may be that 'tiering' is just an optional attribute of a particular 'category/class' of Data Recipient.

There is no discussion in the framework regarding the fees for accreditation and we ask that guidance is given in subsequent versions of this rule set. We are assuming that accreditation is likely to be a 'user pay' model, and fees are likely to be similar to AFSL application fees since much of the suggested accreditation seems to reflect the AFSL requirements.

We consider the suggested accreditation evidence for risk management as being too subjective. We recommend that the objective evidence should be –

- Submission of relevant Privacy policy and procedural documentation.
- Submission of relevant Security policy and procedural documentation.
- Copy of the CDR policy as available to a CDR consumer.
- Copies/images of consent screens to be used by a CDR consumer.
- Submission of specific documentation that responds to the rules in regard to each CDR Safeguard.

And that the pass/fail criteria is an assessment that the documentation is consistent with the expectations of a person skilled in the art of privacy and security for entities wanting to be Data Recipients.

Section 9.5. the ACCC proposes to make a rule that will limit the period of authorisations to 90 days

Whilst we agree that a consent should be time bound, limiting the authorisation to 90 days will not work well with our consumers. Our consumers will not be individuals, they will be small bodies corporate with no employees and regulated by volunteer committees that meet infrequently. Many of our clients maintain bank accounts that have complex authorisations. The time frames of business plans, strategies, decisions and actions of an individual are very different to those of a bodies corporate. Bodies corporate work on an annual cycle. Our business will require regular (daily, weekly) retrieval of banking transactions for the bodies corporate that we service. All our service contracts with our body corporate clients are one year. We request that the period of both consent and authorisation be one year for all CDR consumers. However, if that is unacceptable, we request that the period of consent and authorisation be 90 days for a bank account that is in the name of an individual(s) and one year for bank accounts of data consumers that are not individuals.

14.3 Obligations on accredited data recipients - A quarterly report detailing this complaints information will be required to be provided to both the ACCC and the OAIC.

We submit that a quarterly report is not consistent with the general intention of government reducing red tape. We recommend that yearly reporting is appropriate. We suggest, that where it is appropriate, Data Recipients could be directed to report quarterly when certain thresholds are reached. This approach is consistent with the ATO where reporting cycles are set at intervals that are appropriate for that business.

16. Data Standards Body

We request that some guidance is given with regard to how an API of the Data recipient will be accredited. Section 6 gives great detail in regard to the administrative accreditation of a Data Recipient. However, this CDR framework is silent on the technical accreditation process of the client API developed by a Data Recipient that will need to interface to the Data Holder (Are we correct to assume there is no requirement to have an API approved for use?). Can you please fill the void, at least at a high level, assuming greater detail may be in the Data Standard?

Conclusion

In general, we are comfortable with the proposed CDR Framework with the exception of the 90 day authorisation limit. Unless that can be extended to 1 year for consumers who are not individuals, we forecast that our clients will struggle to renew the authorisation quarterly in which case our proposed service will be unworkable.