Our Ref: 3171

12 October 2018

Data Action Pty Ltd
ACN 008 102 690
Level 3, 55 Currie Street
Adelaide SA 5000
T 08 **8201 1000**
E info@da.com.au
W da.com.au

To Whom It May Concern

ACCC Consumer Data Rights Rules

Thank you for the opportunity to register our comments and recommendations to the Consumer Data Right Rules.

About Data Action

Data Action (DA) was formed in 1986 by 4 credit unions to be their outsourced provider of core banking. Since then we have grown substantially in both number of clients and range of products and we now provide core banking, digital products and integration with other third-party providers, enabling the mutual sector to be a credible 'fifth pillar'.

We support the move towards open banking and are committed to enabling our 16 ADI clients to be compliant with Open Banking rules.

The mutual banking industry is distinguished from the big banks in that mutual banks are owned by their customers and place customer outcomes above all else, including profits. The mutuals are cognisant of the increased competition from the big banks that Open Banking will expose them to, however they see the Consumer Data Right as enormously beneficial to their customers. As such the following DA clients are writing to Treasury to request that they be brought into scope to be active data providers on 1st July 2019 alongside the "Big 4":

- Bank Australia
- P&N Bank

We wish to register our comments and recommendations to the Consumer Data Right Rules Framework via the document attached.

DATA ACTION RESPONSE

1. General obligations and structure of the rules framework

1.b – *At a consumer's direction, a data holder will be obliged to share a consumer's data with the consumer themselves (see section 10)*

We have no objection in principle to this, but it has technical and process implications.

The clarification of this in section 10 suggests that consumers can directly access this data – perhaps as Excel or CSV downloads - which is straightforward for consumers to interact with.

However, section 10.b states that consumers can use the APIs directly.

The number of consumers sufficiently technically skilled to consume an API – a machine interface to their data – can only be expected to be a small minority of actual consumers.

Nor can it be argued that this would stimulate competition, since for any technology that sprung out of this process to spread further would require ACCC accreditation in order to access any other consumer's data via Open Banking APIs.

When combined with the fact that developing and maintaining this functionality will be a sizeable piece of technical work for ADIs to complete, we recommend that section 10.b be excluded from the rules under cost/benefit considerations.

2. CDR Consumer – who may take advantage of the CDR?

3.1 Former customers

The ACCC also acknowledges that there are some issues to be resolved in enabling this, including the authentication process for former customers and the timeframe over which customers may seek to exercise the CDR once they cease to be a customer.

The ACCC does not consider resolution of these issues to be critical for the first version of the rules. The ACCC therefore proposes that the first version of the rules will not enable former customers to exercise the CDR. However, the ACCC considers it desirable that former customers are brought within scope as soon as possible, and seeks stakeholder views on what would be a reasonable timeframe for requiring data holders to share the data of former customers under the CDR regime.

We believe that including former customers in the rules is technically possible through the processes outlined below, however given the increased workload and lesser currency of data, that this be afforded a lower priority:

- We suggest there would be an in-branch or call-centre process to re-activate a past customer, with appropriate identity checks.
- Former customers would need somewhere to manage their permissions. Applications like Internet Banking would need to be modified to recognise a former customer and present a limited view.

- We would expect rules to clarify when a former customer's right to CDR data would end. Under Open Banking, there would be no transaction history left after 7 years, so it would seem to follow that former customers could request that their data be shared up to this time, with the same grandfather clause of 1st January 2017.
- We believe this could be achieved within 12 months, but requires significant work for data providers, and the output will be of much less value given that the data is intrinsically not current.

3.2 Offline customers

Methods by which consumers without online banking accounts can access Open Banking will be brought within scope in a subsequent version of the rules. The ACCC seeks stakeholder views on what would be a reasonable timeframe for requiring banks to share data of their offline consumers under the CDR.

We believe everyone should have access to the CDR and that a process as described below could be achieved within the initial scope:

1. An option would be created for the consumer to side-step the Internet Banking credential prompt, triggering a flow to the data provider's Customer Relationship Management (CRM) processes.
2. A staff member would then contact the consumer over the phone, confirm their identity, and issue a one-time password (OTP), that could be provided to complete the authorisation.
3. Rules would need to be defined for:
    A. appropriate identification
    B. the lifetime of the OTP
    C. banks to recover costs for this labour-intensive activity, e.g., via a card payment

4.2 Phased implementation

The wording of the Farrell report indicated that though the Big 4 ADIs must go live by July 1st 2019, other ADIs could go live at that time. The ACCC Rules Framework seems to rule out the possibility that other ADIs might go live alongside the Big 4.

Data Action raised this concern at an ACCC round table discussion and it was clear that the ACCC was not aware of why an ADI might want to be regulated earlier than required.

Mutual banks are owned by their customers and as such they have a very different philosophy to the Big 4 banks – they place customer outcomes above profits. The mutual banks see the Consumer Data Right, and Open Banking in particular, as complementing their existing services to deliver outcomes for their

customers. As such the following Data Action ADI clients are writing to Treasury to request that they be included within the scope of the initial launch of Open Banking alongside the Big 4 banks:

- Bank Australia
- P&N Bank

As a service provider Data Action will support our clients' compliance with the rules should the Treasury and ACCC agree to allow them take part from 1 July 2019.

5.3.1. Customer data

The ACCC proposes to make rules to the effect that customer data will include, at a minimum … payee lists/direct debit authorisations on the account(s)

A direct debit is an instruction by the consumer to allow future requests from a payee to withdraw from the account. We see this as semantically equivalent to future-dated transfer requests, or recurring transfer requests.

Note, these are not transfers themselves but, like direct debits, are customer-created instructions that express how money will be transferred in the future.

Data 61 has deemed these out-of-scope based on the ACCC CDR Rules Framework, since they are not explicitly within the scope of section 5.3.1. Both future-dated transfer requests, and recurring transfer requests are within the scope of the UK standards. We would like the ACCC to clarify whether these data items should be in scope.

Including them would make it easier for consumers to migrate the banking services from one ADI to another, by having the receiving ADI replicate their outgoing payment instructions, thus increasing competition between ADIs. It would also enrich financial planning products.

Similarly, we would expect to be able to retrieve a list of New Payment Platform (NPP) PayIDs related to an account. In future versions, once the read-only restriction is dropped, we would expect Open Banking to include an API endpoint to request that an NPP PayID be made portable. There is no equivalent to NPP in the UK standards.

5.3.2 Transaction data

The ACCC is considering whether the metadata associated with each transaction should be included as part of the transaction data to be shared in the first version of the rules.

We have no objection in principle to this, however data providers may not have this data in an accessible form. We recommend that metadata should be optional.

7. The Register

The Accreditation Registrar may keep the Register in any electronic format and the Register may contain such information as the Registrar considers appropriate, provided that the Register identifies all entities that hold accreditation under section 56CE(1) of the draft legislation and, where different levels of accreditation exist, the person's level of accreditation

1. The term electronic format is loose. The Register needs to be in a machine-readable format. The former term leaves open the possibility that interacting with the Register is a manual process, and it must be automatic.
2. The Register must contain some form of digital signature technology so that data providers can verify that a request from a particular source has indeed originated from an accredited data recipient.
3. Data Providers will need to be able to read the Register periodically and cache the results. There will be a time after which this cached copy becomes 'stale' thus, we recommend that the ACCC makes rules to define the time limit for how long a data consumer can expect to wait between being added to the Register and having all data providers allow access. We would recommend a value between 1 hour and 1 day.

8.1.1 Joint accounts and complex authorisations

We support the notion that if an individual has full authority on an account, then they can share CDR data access with the same authority. In a joint account situation, how authorised individuals are notified about the activity of other authorised individuals is a matter for each ADI to determine and should not be within the scope of the ACCC rules.

We would expect other authorised individuals to be able to review and revoke the access.

In the case where multiple signatures are required to transact on the account, we would expect multiple authorisations prior to sharing data under Open Banking.

8.3.1. Nature of the consent to be provided

The ACCC proposes to make rules to the effect that the consent request from the accredited data recipient include . . . if the accredited data recipient uses or proposes to use any outsourced service providers to assist in providing the service to the consumer the name of those third-party service providers

The term any outsourced service providers is broad.

Data Action provides outsourced development and hosting services to many Australian ADIs, but we do not own the data in those systems. The ADI owns the data and solely derives value from the data. We

believe that it would confuse and unduly concern a consumer to see Data Action named on the disclosure statement alongside their ADI.

Surveys of the UK population post-open banking suggest that the majority would never share their banking data outside of the bank. We need to be careful that this provision is not seen to strike fear into consumers and unnecessarily discourage data sharing.

For example, in the normal course of business, a bank would not disclose all outsourcing arrangements to customers. These relationships are largely technical in nature and are subject to change with the needs of the business.

We think the intent here is to ensure that the data consumer should disclose any other party who they may transfer ownership of the data to, or who may gain insights from their personal data, during the lifetime of the grant.

There are other provisions being discussed by the ACCC: Privacy Safeguard #6 and #11 preventing disclosure of data without valid consent in accordance with the rules; and destroying/de-identifying redundant data. These safeguards ought to clarify that the consumer remains the owner of the data being shared.

We recommend that the term *any outsourced service providers* be clarified accordingly.

The ACCC proposes to make rules to the effect that the consent request from the accredited data recipient include . . . the period for which the accredited data recipient will hold the data

Since many of the consumers of Open Banking data will be ADIs, we expect clarification on whether there be a maximum period that ADIs should hold the data they have received as a data consumer. Under Anti-money Laundering (AML) law, ADIs currently hold transactional data for a 7-year period and identity verification data for 7 years after all services to the consumer have ceased. Our question is that if CDR data is brought into the ADI and used as the basis for a financial decision (e.g., lending, or identification), should the CDR data that was the source of the decision be retained as long as the outcome of the financial decision itself, or 7 years, or a different duration?

9.6. Granularity of authorisation

Fine-grained authorisations may enable more nuanced services to be provided to consumers. More fine-grained authorisations would also be consistent with a data minimisation principle, helping to ensure that only the most relevant data is shared with an accredited data recipient. However, the ACCC understands that there may be technical challenges associated with delivering 'fine-grained' authorisations, at least for the time being. It is therefore appropriate that the level of granularity of authorisation be addressed through the standards development process.

The ACCC consequently proposes to make a rule that the Data Standards Body, as part of the standards development process, continue to pursue delivery of more finely-grained authorisations. The initial degree of granularity of authorisation in the technical standards is thus a matter for the Data Standards Body, but with an expectation that more finely-grained authorisation will be developed over time. It may also be the case that in the short-term some service providers offer 'intermediary' services where they collect data pursuant to a coarse-grained authorisation, and then provide data to another accredited data recipient at a finer degree of granularity.

We can see no technical reason not to have fine-grained authorisations from the start of Open Banking. The issue being debated on the Data61 forum is the trade-off between:

1. A simple user experience with coarse-grained authorisations
2. A complex user experience with fine-grained authorisations

When this matter is decided, permissions would not become more fine-grained over time. So the ACCC expectation that "more finely-grained authorisation will be developed over time" is misplaced.

We recommend that hierarchical permissions be offered from the outset to capture the best of both worlds. So that where user experience is a priority over control, coarse-grained permissions could be used. But where a use case exists for a fine-grained permission, this is available and should be preferred.

9.9. Revocation of authorisation

Other proposed rules in relation to the revocation of authorisations provided to data holders include:

i. if a consumer revokes an authorisation via the data holder, the data holder must notify the accredited data recipient and any intermediary

We recommend that the mechanism for notifying the data recipient and any intermediary should be defined. If this is not standardised, then this process cannot be automated effectively. Ideally, data recipients must provide an API endpoint to be notified.

12.1.1. To a specified entity as directed by the consumer

The ACCC proposes to make rules requiring accredited data recipients to transfer data to a non-accredited entity if directed by a consumer and with their specific express consent. This is a situation where CDR data has been shared by a data holder with an accredited recipient, and the consumer is now directing that accredited recipient to share the data with a non-accredited recipient. The ACCC is not proposing to make rules that would permit the sharing of CDR data from a data holder to a non-accredited recipient.

The ACCC ought to specify the mechanism by which a data recipient should transfer data to an unaccredited 3rd party. The absence of specificity here will mean that this process is ad-hoc and manual, and therefore expensive to support for the data recipient sending the data and the non-accredited entity receiving the data.

As an example, an ADI can become an accredited data recipient (in addition to being a data provider). If the ADI is holding CDR data that it has received as a data recipient on behalf of a consumer, 12.1.1 implies that the consumer can indicate that the ADI share that CDR data with a non-accredited entity at the consumer's direction.

In this scenario, the ADI has no direct relationship with the non-accredited entity, nor will the ACCC Register mediate the exchange.

Unless this provision can be brought explicitly into the broader API framework of the other provisions, we recommend that this provision be removed as impractical.

12.1.2. To an outsourced service provider of the data recipient for a specified use

The ACCC proposes to allow an accredited data recipient to disclose CDR data to an outsourced service provider, even though the outsourced provider may not be accredited, with appropriate additional protections in place including the requirement that these arrangements are disclosed to consumers during the consent process and other obligations relating to outsourcing (see paragraph 6.8).

Similar concern as above under 8.3.1.

In general – Notifications

The term 'Notification' is used frequently in the framework. Please clarify the mechanisms that would be considered 'Notification'. For example:

- A message visible inside an Internet dashboard the next time the consumer logs in.
- An SMS, push, or e-mail message sent within 'x' minutes of the event, where a phone number, email address, or native app has been registered.
- A monthly digest of activity via e-Mail.
- What notification would be appropriate for a person with only a mailing address? Should the ADI write to them?

Please feel free to contact us if you would like to discuss our contribution to your consultation process.

Yours sincerely

Brett Miller
Chief Technology Officer
Data Action Pty Ltd